Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 4, April -2017

IMAGE DATA HIDING OVER ENCRYPTED DOMAIN USING STEGANOGRAPHY

Alagappan RM[1] , Anandan K[2] , Mr.J.Jerin jose[3]

1,2 *UG students, Department of Computer science and Engineering, Sathyabama university*
3 Asst professor , faculty of computing, sathyabama university

Abstract— *The transmission of data across the digital world has increased the need originality of data to be sent from one place to the other place. The processing of data or other files into images via encrypted domain to increase the confidentiality has been going for many years. This paper makes you to add important text and messages or files into files like Images or audios or pdf without detonating the real quality. It can be done with the least significancy bits of these data for combining and encrypting data which are not known or used by other normal users. By using this it allows you to add the hidden messages or files in encrypted domain using steganography and embedding algorithm. This algorithm helps you to decrypt the hidden data from the master document by using only the password which is used at the time of encryption. This system gets the favour performance on secure embedding capacity at STEGANALYSIS. It helps embedding messages and files in compression domain using ZIP compression format. So that we have a variety of compression level to be used- low, normal or high .Now a days internet has lots of data which does not use any secure transactions which may lead to many interception as well and this has became an issue . To reduce this interception steganalysis is used to prevent interception and to increase confidentiality beside data hiding .*

Keywords— *steganalysis , embedding and data hiding*

1. INTRODUCTION

The processing of information using encryption and decryption domain to increase confidentiality has attracted many researchers in recent years.[1] As many users need to transfer data in cloud or some other means where it has a possibility of interception hence they started looking for the encryption of data before sending them and to get decoded by decryption algorithm using the same private key used by send when the data is decrypted [2]-[4]. As due to emerging new technology has emerged which makes way to usedata hiding in reverse in [5][6]picture encryption because of that which helps service provider to use extra data of files like images , pdf and audios added into the files not degrading the original quality of the picture ,

We propose the reversible data hiding in secure form using unique algorithm to decrypt and embedded data in images [7]-[13]. this paper makes a aim of increasing the combined data or payload in the image .in which we use to combine the bits which are selected from the stack of cipher picture using key into bits to make space for the hidden or secret data to be stored.[14]-[19]

In this method we use two unique keys by using this method we get the original data or image where we stored the hidden private data without defecting the quality and from there we can retrive our hidden data or message using the two different public and private codes .this method achieves the high combining cover data and original image recovering quality and it avoids extra room space

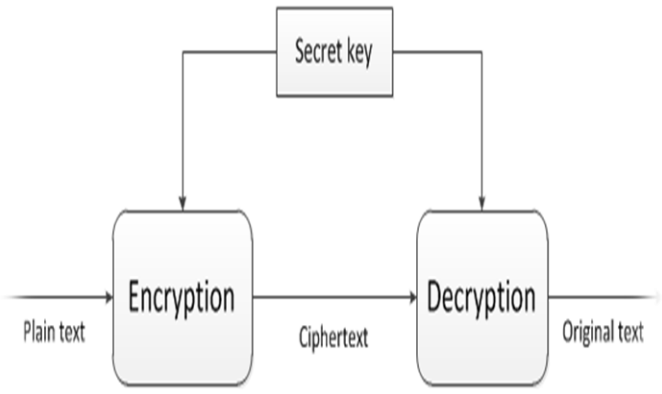

Fig 1.System Model

I. LITERATURE SURVEY:

Previously we have used a system which only hides the information in the master file and it supports only few formats of master files.[7] This system doesn't support the encryption and also compression. Here we can hide only the message and it won't supports hiding of files. The system used earlier only supports the encryption that means it just protects the file by providing a password. [8]And also the previous system supports only bytes of information to hide[9]. There is no system which supports all types of multimedia files as master file. Existing systems affects the little bit originality of master file and the overall process is little bit complex, consumes much time.

This already available method for this data hiding method has two different methods [11]a)vacating room after encryption and another one is b)vacating room before encryption . in 1st method that is in VRAE method the main picture is encrypted by user who is sending while sending directly and the secret data is embedded in the file by modifying some bits in the original data.[7] this embedded 1bit in each block considering each block pixels to make the decryption or interception process difficult that is the secret data in embedded in the rate of 1/n bits per pixels[9] .

we can also say the encryption and decryption occurs simultaneously that is inseparable.[10] with other idea zhang proposed the method which divides the images into multiple blocks where the data can be hidden in each block by finding least significant bit and by flipping them which makes the room for storing the secret data in it.[8][12] Decryption process is just the reversible process where it just flips the LSB bits which forms a new whole block from the original image the secret data can be recovered and extracted jointly . To overcome the defects of inseparability another method using RDH scheme was introduced for encryption of pictures .in this that class pseudo randomly produce and divides the images into many multi teams with a constant size and which makes the room for storing the data .[11] on the receiver side the total MSB are obtained by decryption. By comparing we can estimate the the bits of coset the receiver the recover the original data because in this method[13] we can extract original image easily because it happens before data recovery so it makes it easily, besides that this works likely better that the other methods .

on seeing these issues we describe a method to make high capacity data combining cover data by adding the MSB with other RDH method . As per research identifying MSB is much more easier when compare to identification of LSB planes, in other words maximum data encryption can be done by this ratio

In interaural phase technology [19] the phase modification in audio signal is studied where that paper shows that the change in basic hexadecimal numbers and base4 numbers will not effectively affect the quality of the sound signals transmitted from one device to other because it cannot be evident to any basic attacking parameters and in this proposal SNR is used to keep track on amount of sound degraded using a Fourier formula derived and it also uses the DER formula to find the data error rate in the audio transmitted

Image steganography in grey[20] and colour scale implementation has a effective effect of transmitting data with less distortion as it uses DCT enhancement (i.e)discrete cosine transform of the converted color image into the grey scale image which increase the quality of the image and which makes the decryption of covert message even when the hidden image is exposed without knowing the key, it uses RSA method to encrypt the data into the image using a key which improves the security of the image. This method two algorithm that encrypts data into image after altering the color image into grey scale and another method by before converting into grey scale .Entropy is used to measure the uncertainty between the original image and the encrypted image. Small entropy small difference ,high entropy high difference

The combined processing of neural networks and visual cryptography in image steganography has a new effect on encrypting image using key values ,where as the visual cryptography mainly concerned about the image and its decryption .[21] in decryption all the shared parts of images are arranged in original order in the stack to get the covered image where the data is hidden from the recovered image the hidden message can be retrived by using the key value which is used while encryption.

Haar Discrete Wavelet Transform method[22] used in image encryption which mainly focus on reduction of complexity and reduction of distortion of images. In this method the image to be sent is divided into four equal parts where the one part of image carries all the data of the original image and tge remaining three parts carries the secret images . and it has its own drawbacks of even a small change in image sent will affect the whole data sent

II. SYSTEM DISCRIPTION:

The proposed system has of three different parts which is encryption of image, data embedding and data extraction or image recovery . in 1st part image is encrypted with a key into a another unique image and in 2nd part data hider is used to compress the bits which is hidden data code used to generate space to store data and to encrypt using a encryption key . in 3rd part received image can be decrypted by decryption key from which l we can recover the original data and the secret data embedded in it In this system we are using AES algorithm which can be used for to encryt and decrypt as which has the very unique combination of RDH and MSB joint venture combination.

III. PROPOSED SYSTEM:

In this model we are planned to encrypt the messages and files into the master image file . in our model which supports mostly all the formats of documents like images ,audio,pdf files and also in our model it allows both encryption and

compression as well decryption of documents. It also allows to encrypt large amount of data. As well it will not degrade the original quality of the data in our system. So that the overall process is made as easy as possible . and it also uses the very powerful algorithm for encryption and decryption as it helps the model to increase the confidentiality as well as authentication .

IV. METHODS:

1)ROUND KEY GENERATOR

In round key generator key is generated in 10 pipeline stages . in this process it takes the key generated in one process or stage to the next stage till all the blocks or pipeline is filled . this round key generator is added and synchronized with encryption and decryption unit . when even a 10 vaild block in entered into the encryption or decryption unit a new key is generated and stalled .it allows to process in different stages with different keys

2)ENCRYPTION UNIT

It is constructed by combining AES primitive blocks. Since synchronous ROM is used encryption unit should be pipelined implicitly . at each stage a new key is generated and used in respective stages for encryption . this leads to tightly coupled round key generator and encryption unit . by this coupling extra time need for key generation is avoided . when a key goes out of date then it is stalled for further synchronization

3)DECRYPTION UNIT

Same like encryption in decryption is constructed by combining AES and primitive blocks but in reverse in opposite order used for encryption and it is also implicitly pipelined .in this decryption order of generation of round key I in opposite direction as of in encryption process and buffers with each stage are inserted between the round key generators so it gives the desired latency needed for propogation

V. CONCLUSION:

From the analysis we have made we found that there is a chance of the data transferred can get distorted and change in quality of the original image and loss or decrement in confidentiality but by using this application with AES algorithm using key modulation technique which we intend to produce will have the most effective output with the exact recovery of original image and also free from other malicious attacks and intrusion

And it has a advantage of difficulty of detecting the difference between the real image and the image which is encrypted and as it share the same data range its is not suspected to have been embedded and data loss is not evident able to the rotation of images

VI. REFERENCES:

[1] Erkin,, Piva, S. Katzenbeisser, et al., “Protection and retrieval of encrypted multimedia content: When cryptography meets signal processing,”
[2] Johnson, P. Ishwar, V.Prabhakaran, D. Schonberg, and K. Ramchandran, “On compressing encrypted data,” IEEE Trans. Signal Process., Oct. 2004.
[3] Liu, W. Zeng, L. Dong, and Yao, “Efficient compression of encrypted grayscale images,” IEEE Trans. Image Process., Apr. 2010.
[4] Zhang, G. Feng, Y. Ren “Scalable Coding of Encrypted Images,” IEEE Trans. Inform. Forensics Security,June 2012.
[5]. Deng,.. Bianchi,. Piva, and B. Preneel, “An efficient buyer-seller watermarking protocol based on composite signal representation,” 2009,.
[6] S. Lian, Z. Liu, Z. Ren, and H. Wang, “Commutative encryption and watermarking in video compression,” IEEE Trans. Circuits Syst. Video Technol., vol. 17, no. 6, pp. 774–778, Jun. 2007.
[7] W. Puech, M. Chaumont and O. Strauss, “A reversible data hiding method for encrypted images,” Proc. SPIE 6819, Security, Forensics, Steganography,Feb. 26, 2008,
[8] X. Zhang, “Reversible data hiding in encrypted images,” IEEE Signal Process. Apr. 2011.
[9] W. Hong, T. Chen, and H. Wu, “An improved reversible data hiding in encrypted images using side match,” IEEE Signal Process. Lett., v Apr. 2012.
[10] X. Zhang, “Separable reversible data hiding in encrypted image,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.
[11] K. Ma, W. Zhang, et al. “Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption,” IEEE Trans. Inf. Forensics Security, vol. 8, no. 3, 553-562, 2013.
[12] Qian Z, . Han X and X. Zhang, “Separable Reversible Data hiding in Encrypted Images by n-nary Histogram Modification,” 3rd International Conference on Multimedia Technology (ICMT 2013), Guangzhou, China, 2013.

[13] W. Zhang, K. Ma and N. Yu, "Reversibility improved data hiding in encrypted images," Signal Processing, vol. 94, pp. 118–127, 2014.
[14] Kalker .Tand M. Willems, "y bounds and code constructions for reversible data-hiding," in Proc. 14th Int. Conf. Digital Signal Processing
[15] Fridrich.j and M. Goljan, "Lossless data embedding for all image formats," , Jan. 2002
[16] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans Aug. 2003.
[17] Ni.Z, Shi,Y . Ansari, and S. Wei, "Reversible data hiding," IEEE Mar. 2006.
[18] D. M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," IEEE 2015
[19] Trikarsa Tirtadwipa Manunggal, Dhany Arifianto," Data protection using interaural quantified-phase steganography on stereo audio signals"IEEE region 10 conference 2016
[20] Yash Kumar Singh, Sudhanshu Sharma," Image Steganography on Gray and Color Image using DCT Enhancement and RSA with LSB Method"IEEE 2016
[21] K.S.Seethalakshmi, Usha B A,Sangeetha K N," Security Enhancement in Image Steganography Using Neural Networks and Visual Cryptography"international conference on computational system 2016
[22] Essam H. Houssein ,Mona A. S. Ali , and Aboul Ella Hassanien," An Image Steganography Algorithm using Haar Discrete Wavelet Transform with Advanced Encryption System" Proceedings of the Federated Conference on Computer Science and Information Systems 2016

