INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 3 (2018) PAGES 3581 - 3585
RECEIVED : 15.04.2018 PUBLISHED : 20.05.2018

May 20, 2018

A Hybrid approach for image steganography with compression to enhance security and accuracy

[1]Kalaimathi.A, PG Scholar, Computer Science Engineering, Bharathidasan Engineering College, Natrampalli, Vellore, Tamil Nadu.

[2]R.Anbarasan, Asst Professor, Computer Science Engineering, , Bharathidasan Engineering College, Natrampalli, Vellore, Tamil Nadu.

[3]A.Sudhakar,HOD, Computer Science Engineering, , Bharathidasan Engineering College Natrampalli, Vellore, Tamil Nadu.

Abstract:

Security of secret data has been a major issue of concern from ancient time. Steganography and cryptography are the two techniques which are used to reduce the security threat. Cryptography is an art of converting secret message in other than human readable form. Steganography is a technique of hiding the secret message and transmission of confidential data through public channel like Internet. These techniques are required to protect the data over the network. An Advance approach the image security along with compression and encryption used to a high quality of secret message and data. Image compression is used to minimize the amount of memory and fast transmission over internet to represent an image or data. And encryption is used to protect the data over the noise and different attacks. In this thesis, proposed an algorithm steganography and EZW compression technique to provide hiding the large amount of secret data with Chaos encryption used to securely transfer image to receiver side. And also discuss 2-level DWT using steganography to reduce the variation of recovered image. This technique used to a securely data transfer from narrow band and unsecure channel.

Keywords: EZW compression, chaos based encryption, 2 –level DWT, Information Hiding, Security.

1. INTRODUCTION

In today’s world, transmission of the information over the channel is not secure for example patient records, military information, banking data and other sensitive information. In order to protect this sensitive information it is coded within the image, audio or text files which is decodable only with the help of a particular key. Steganography is used to hide a secret message within a cover image, thereby yielding a stego image such that even the trace of the presence of secret message cannot be detected. In the modern steganography, steganography meaning evolved into withholding information on a digital media file, the media can include images, sound or video. In steganography main component is image compression. Image compression used minimizing the size, reduce transmission time. But this technique some challenge with image communication is to maintain the image quality during the communication. Sometimes, because of low speed transmission or signal distortion, the quality of image can be affected. But some applications are sensitive to image quality; because of this there is requirement to maintain the quality of image. The main goals of algorithms is to provide a robust security against any type of intrusion and also the algorithm need to be as simple as possible in terms of ease of implementation, cost of implementation, complexity and its durability or sustainability against the different kinds of intrusions. And also used to a high quality of reconstruct image to used some techniques. An Advance approach the image security along with compression and encryption used to a high quality of secret message and data. Image compression is used to minimize the amount of memory needed to represent an image. Transmitting or storing an image is major problem in current scenario. Steganography is a technique of hiding a message in a host image without any perceptual distortion of the host image. The main terminologies used in the steganography systems are: the cover message, secret message, secret key and embedding algorithm. The cover message is the carrier of the message such as image, video, audio, text, or some other digital media. The secret message is the information which is needed to be hidden in the suitable digital media. The secret key is usually used to embed the message depending on the hiding algorithms. The embedding algorithm is the way or the idea that usually use to embed the secret information in the cover message.

2. RELATED WORK

The Embedded Zero Wavelet (EZW) is simple and effective algorithm for image compression which has a property of coding the bits in the order of their importance. Basic concept behind EZW is the concept of zero tree structure which occurs in the Discrete Wavelet Transform (DWT) applied image due to the spatial correlation of DWT. To apply EZW on an image we need to follow 3 steps. In first step is to apply multi-level DWT on image. Second step consists of 2 passes namely Dominant pass and Sub-ordinate pass. Dominant pass start with finding a threshold and modifying the image pixel values depending on threshold. Now the image is scanned and assigned with codes positive, negative, isolated zero and zero tree respectively. In next pass, elements in subordinate list are processed in the entry order. The elements which are coded with POS and NEG are replaced by zeros in the image and the same process is repeated by making the threshold half of the previous, this process can be done up to the user defined threshold value or up to the threshold limit. In proposed technique, First pre-processing is applied on cover image. In pre-processing we applied resize of image. Then applied 2-level DWT transforms. Then added secret message using LSB embedding techniques. Then converted stego image and applied EZW compression and Chaos based encryption and converted advance stego image. Then extracting process take advance stego image applied decryption using secret key and decompress and decryption techniques. Last applied inverse transform and receive secret message and image.

3. PROPOSED SYSTEM

In today’s world, transmission of the information over the channel is not secure for example patient records and other sensitive information. In order to protect this sensitive information it is coded within the image, audio or text files which is decodable only with the help of a particular key. Steganography is used to hide a secret message within a cover image, thereby yielding a stego image such that even the trace of the presence of secret message cannot be detected. In the modern steganography, steganography meaning evolved into withholding information on a digital media file, the media can include images, sound or video. In steganography main component is image compression. Image compression usedminimizing the size, reduce transmission time. But this technique some challenge with image communication is to maintain the image quality during the communication. Sometimes, because of low speed transmission or signal distortion, the quality of image can be affected. But some applications are sensitive to image quality;

Because of this there is requirement to maintain the quality of image. Image compression is minimizing the size in bytes of a graphics file without degrading the quality of the image to an unacceptable level. The reduction in file size allows more images to be stored in a given amount of disk or memory space. Image compression also reduces the time required for images to be sent over the internet or downloaded from web pages. In DWT, wavelet filters that have floating point coefficients are used so that when data is hidden inside their coefficients any truncations of the floating point values of the pixels that should be integers may cause the loss of the hidden information. This would result in the data hiding system to fail. In case where the input data is integer as in digital images, the output data will cease to be integer which in turn doesn't allow perfect reconstruction of the input image. IWT ensures no loss of information through forward and inverse transforms. The image will be processed to get a text message hidden in the image. A text message has been obtained from the image is decompressed back to using LZW decompression technique. Text messages result from decompression was still not final results for the previous message encrypted with RSA method so that the necessary processes by using the decryption key that already exists. After the decryption process is complete we will get the actual text message.

4. ANALYSIS

In EZW, we don’t know the DWT level applied to image and number of EZW passes we cannot bring back the original image. If keys are known without the prior knowledge of level applied, number of passes and storage pattern we cannot reconstruct the image back. Also this way by having an unknown level of DWT it will be very difficult for an hacker to get back the original contents. If scramble the data it may lead to increase details in the image, which is not suitable for compression. If apply EZW on such type of scrambled image it leads to negative compression, instead of compressing the image it increase the space occupied by the image. So, to overcome this problem we are going to apply EZW first and then chaos based scrambling on the resultant data. This will save memory space and also transmission bandwidth. An robust cryptosystem is presented and implemented by combining the JPEG compression and an encryption using a modified Hill cipher method in mode by block what gives us the possibility of deciphering in a individual way blocks 8x8 pixels the compression rate is modifiable and therefore the proposed method provides an optimal use of bandwidth with a very good level of security. Implementation results of the proposed system tested on MATLAB R2014b was used and operation carried out on desktop computer having Intel i5 processor with 8GB of RAM. In results the screenshots of the intermediate results are kept which are used for generating the final result of the system. The parameter selected for result analysis of proposed system is PSNR, MSE, Compression Ratio, Embedded capacity and Execution time. Based on the parameter decided the Accuracy and robustness of this system. For result analysis we takes image is calculated to different parameters and comparison of result analysis of two classification without attack and with attack is done that different attack accuracy is near by the original accuracy from given table. Thus the as well as same to a PSNR and MSR as original image. Information security and transmission is a key factor in image processing. According to literature review and paper analysis to balance security with steganography and compression of data is primary limitation of existing system. Using proposed flow improve to security and compression for data and image. For security use hybrid model and for compression use EZW compression. Also work on different type of attacks like that Noise, Gaussian, Rotate, Salt & Pepper, Speckle, Unsharp and Blur to prove that our system is robust. Also work on different type of parameters like that PSNR, MSE, Compression Ratio, Capacity and Execution time. In future try to add some often compression for better transmission.

The image will be processed to get a text message hidden in the image. A text message has been obtained from the image is decompressed back to using LZW decompression technique. Text messages result from decompression was still not final results for the previous message encrypted with RSA method so that the necessary processes by using the decryption key that already exists. After the decryption process is complete we will get the actual text message. An robust cryptosystem is presented and implemented by combining the JPEG compression and an encryption using a modified Hill cipher method in mode by block what gives us the possibility of deciphering in a individual way blocks 8x8 pixels the compression rate is modifiable and therefore the proposed method provides an optimal use of bandwidth with a very good level of security.

CONCLUSION

Information security and transmission is a key factor in image processing. According to literature review and paper analysis to balance security with steganography and compression of data is primary limitation of existing system. Using proposed flow try to improve security and compression for data and image. For security use hybrid model and for compression use EZW compression. In future try to add some often compression for better transmission.

REFERENCES

[1] FaiqGmira, Said Hraoui, AbderrahimSaaidi, AbderrahmaneJarrarOulidi, Khali Satori. "Securing the Architecture of the JPEG Compression by an Dynamic Encryption." IEEE Intelligent Systems and Computer Vision (ISCV), Morocco,25-26 March 2015, DOI 10.1109/ISACV.2015.7106192 Print ISBN: 978-1-4799- 7511-2.

[2] ShubhamLavania, Palash Sushil Matey, Thanikaiselvan V. "Real-Time Implementation of Steganography in Medical Images using Integer Wavelet Transform." IEEE International Conference on Computational Intelligence and Computing Research (ICCIC),TamilNadu, 18-20 Dec. 2014, DOI 10.1109/ICCIC.2014.7238344 Print ISBN: 978-1-4799-3975-6.

[3] Rina Mishra, Atish Mishra, Praveen Bhanodiya. "An Edge Based Image Steganography with Compression and Encryption." IEEE International conference on Computer, Communication and Control (IC4-2015), Indore, 10-12 Sept. 2015, DOI 10.1109/IC4.2015.7375510 Print ISBN: 978-1-4799-8165-6.

[4] Nathaniel D. Amsden, Lei Chen. "Analysis of Facebook Steganographic Capabilities." 2015 International Conference on Computing, Networking and Communications, Communications and Information Security Symposium, Huntsville, 16-19 Feb. 2015, DOI 10.1109/ICCNC.2015.7069317 Print ISBN: 978-1-4799-6959- 3, pp. 67-71.

[5] T. VenkataSainath Gupta, Ch. Naveen, V. R. Satpute, A. S. Gandhi. "Image Security using Chaos and EZW Compression." 2014 Students Conference on Engineering and Systems (SCES), 28-30 May 2014, DOI 10.1109/SCES.2014.6880108 Print ISBN: 978-1-4799-4939-7.

[6] Pcmag.com. (2016). lossy compression Definition from PC Magazine Encyclopedia. [online] Available at: http://www.pcmag.com/encyclopedia/term/46335/lossy-compression [Accessed 25 Aug. 2016].

[7] LedyaNovamizanti, GelarBudiman, IwanIwutTritoasmoro. “Designing Secured Data Using a Combination of LZW Compression, RSA Encryption, and DCT Steganography.” 2015 1st International Conference on Wireless and Telematics (ICWT), Indonesia, 17-18 Nov. 2015, DOI 10.1109/ICWT.2015.7449245 Print ISBN:978-1-4673-8434-6.