Comparative Study of Data Hiding in Encrypted Image using lossless and lossy Compression

1. Dr. Vivek Sharma

Head, Deptt. of CSE (UG & PG)

VNS Institute of Technology, Bhopal

2. Mr. Hariom C. Agnihotri.

VNS Institute of Technology, Bhopal

Research Scholar

ABSTRACT:

We propose an information hiding technique which based on pixels' block. We used pixels contractive relation to hide the information that we want to embed. The characteristic of our method is that to use pixels contractive relation to assist lossy compression process in reducing the image size. There exists many hiding techniques, but most of the techniques cannot tolerate the destruction of lossy compression. Compression will speed up the transmission of the image with the hiding data.We achieve something others cannot do, to implement compression into the transmission of images in order to speed up the process. Data hiding is the process of hiding piece of information into a cover media such as image, video, audio, etc. Various data hiding algorithm has been proposed for different applications, for example, it can be used for covert communication, image authentication, copyright, copy control in DVD, traitor tracing, data integrity, etc. Among these data hiding techniques, robust lossless data hiding has received increasing interest. Robust data hiding is the ability to extract the secret data correctly after compression or any other incidental alteration has been applied to the stego-image. In lossless data hiding the original image is recovered after extraction of data from the stego image. It has been successfully applied to many images, including aerial, texture, miscellaneous, standard images and medical images. Specifically, it has been successfully applied to authenticate lossless compressed JPEG2000 images, followed by possible transcoding. It is expected that this new robust lossless data hiding algorithm can be readily applied in the medical field, law enforcement, remote sensing and other areas, where the recovery of original images is desired. With the fast progression of data exchange in electronic way, information security is becoming more important in data storage and transmission. While storing and transmitting multimedia data are not easy and they need large storage devices and high bandwidth network systems. Compression and encryption technologies are important to the efficient solving of network bandwidth and security issues. This paper focus on dual approach of compression and security where compression is achieved through lossless algorithm (either Huffman coding or LZW) according to size and type of image data and compressed data is encrypted using traditional DES Algorithm.

KEYWORDS:

Information Hiding, Contractive Relation, Lossy Compression, Image processing, data hiding, robust image hiding,LOSSLESS COMPRESSION

1. Introduction

Recently, more and more people communicate with each other by surfing on the Internet. However, it is not very secure when we transmit information through Internet. Everyone can peek, copy even alter our information easily in this wide open environment. Thus, we don't want to transmit the important information without any protection in the public network unless a secure channel is provided for the transmission. The cryptography technique can protect our message content from a peeper. But the cryptography technique will cause our message content to be meaningless random codes. It is easy to guess something important in the transmitted information even the receiver do not know what is inside. They may cut, hack or break these meaningless random codes. Therefore, we need information hiding technique to help us to solve the problem of transmitting important data in an absolute secure channel. Thus, it is not only difficult to decrypt the data, but also difficult for attackers to detect the hidden data.

Data hiding, in more general term, is a process to hide data into cover media such as images, audio clips or video streams. It can be used as a way to transport information secretly or to protect the integrality of the cover medium itself. Here, we mainly focus on data hiding into images. Data hiding techniques are applicable for covert communication, ownership of digital image, image authentication, copyrights, data integrity, fraud detection, self correcting images, Fingerprinting, copy control in DVD, etc. Applications of the data hiding techniques could be divided into two groups depending on the relationship between the embedded message and the cover image. The first group is formed by steganographic applications in which the message has no relationship to the cover image and the only role the cover image plays is the one of a decoy to mask the very presence of communication. The content of the cover image has no value to the sender or the decoder. Its main purpose is to mask the secret embedded message. In this typical example of a steganographic application for covert communication, the receiver has no interest in the original cover image before the message was embedded. Thus, there is no need for distortionfree data embedding techniques for such applications.

Internet based communications are evolving at a tremendous rate. The Internet has facilitated the development of a worldwide 'Virtual Community' free from the constraints of time and geography. Due to the internet there is no distance between a person located in one place and experts around the globe. Through electronic mail / voice mail / video mail it is possible to solicit the opinion of experts. Moreover, Telemedicine is becoming popular in the specialties of radiology, pathology, critical care and psychiatry, where data is in the form of image. The internet has become a hostile environment with both wired and wireless channels offering no inherent assurance of confidentiality. It is required to ensure confidentiality and security for transmitting certain multimedia data over the internet. Encryption of data has become an important way to protect data resources especially on the Internet, intranets and extranets. The another challenge in multimedia applications is the transport services to both discrete media such as text and digital images and continuous media such as audio and video with limited bandwidth and huge data size. With the huge demand for bandwidth due to the large data transmitted in multimedia applications, it becomes necessary to apply compression algorithms on transmitted data. So the best way of fast and secure transmission is by using compression as well as encryption of multimedia data.

2. The Hiding and Extraction Method

In this section, we will introduce our hiding and extraction method. Our method develops with block gray scale pixels value contrastive relation and cannot be destroyed after lossy compression and decompression process. There are two important components, cover image and hiding data, in data hiding technique.

3. DOMAINS FOR DATA HIDING

Information hiding scheme using digital image as a cover media are performed into three domains:

A. Spatial Domain

In spatial domain, more redundant spaces are available to embed a secret message. In addition, less time is needed for embedding and extracting procedures. However, spatial domain-based data embedding schemes are vulnerable to common attacks.

B. Transformed Domain

In transformed domain, a transformation such as discrete cosine transform (DCT) or discrete wavelet transform (DWT) is first performed on a cover medium to obtain frequency coefficients. A secret message is then embedded into significant coefficients to achieve the robustness. Nevertheless, the embedding capacity of transformed domain based data embedding schemes is low because a transformed medium has only a few significant coefficients. Besides, extra time is needed for transformation operations.

C. Compressed Domain

In compressed domain, a cover medium is first compressed by using a compression technique such as the vector quantization (VQ) compression method to obtain compression codes. Then, a secret message is concealed into compression codes. In general, compressed domain-based data embedding schemes are robust against common attacks and they are suitable for low bandwidth transmission lines because the amount of transmitted data is significantly reduced. However, the embedding capacity of compressed domain-based schemes is low because of less redundant spaces for secret data embedding. Furthermore, additional time is required for compression and decompression processes.

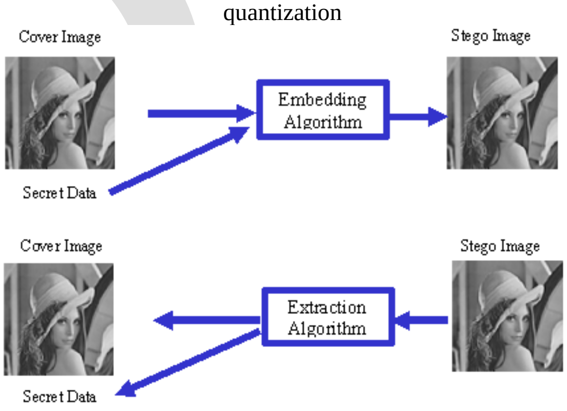


Figure.1 Image Data Hiding

1. Individual or independent compression and encryption

a) *Compression followed by Encryption (CE)*: In this sequence an intruder have less cleave to access image but encryption may again increase the size.

b) *Encryption followed by Compression (EC)*: In this sequence size is not again increased but an intruder may have more clues to access the image. In some case sequence size decreased so not efficiently compressed.

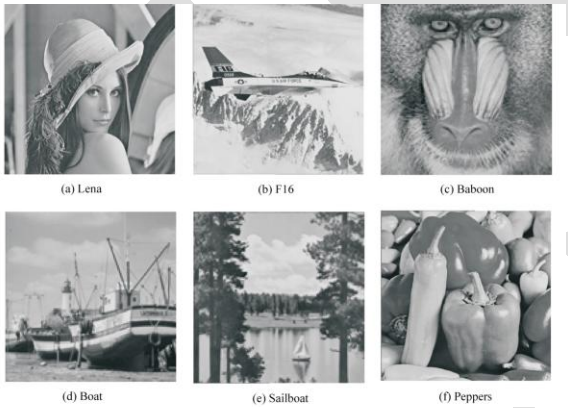
2. Joint Compression and Encryption (JCE):

This approach is recently used which may be fast as compared to previous two but procedure is complicated.

Encryption applied by different researchers by means of encrypting algorithm which encrypt the entire or partial multimedia bit sequence using a fast conventional cryptosystem . Much of the past and current research targets encrypting only a carefully selected part of the image bit stream in order to reduce the computational load, and yet keep the security level high. The encryption can be performed either using Symmetric key cryptography or by using Asymmetric key cryptography. If same key is used for encryption and decryption then it is called as Symmetric key cryptography and if the different key is used for encryption and decryption then it is called as Asymmetric key cryptography.

Image compression algorithms are used use to reduce the amount of data required to represent a digital image and the basis of the reduction process is the removal of spatial and psychovisual redundancies. Mathematically, visual data compression typically involves transforming (encoding) a 2-D pixel array into a statistically uncorrelated data set. Two types of compression are lossless compression and lossy compression. If same image can be generated from the compressed image then it is Lossless compression otherwise it is lossy compression. This study focuses on CE pattern in which compression is followed by symmetric key encryption. Compression of multimedia data such as images achieved through two lossless algorithm Huffman coding and LZW. Therefore in this paper comparative study of two image compression algorithm and their variety of features discussed and that factors are used to choose best among them for further encryption phase.

4. Results


(a) Lena (b) F16 (c) Baboon

(d) Boat (e) Sailboat (f) Peppers

Figure 2. 512 _ 512 cover-image.

PROPOSED APPROACH AND METHODOLOGY

In this paper CE order i.e. compression is followed by encryption is applied on colour and grayscale image of different size and type. Here compression is performed by either Huffman or LZW lossless coding algorithm which is depending on user choice and contents of data. For resultant compressed data is secured by DES (Data Encryption Standard) encryption algorithm. The schematic block diagram of this proposed approach is given in

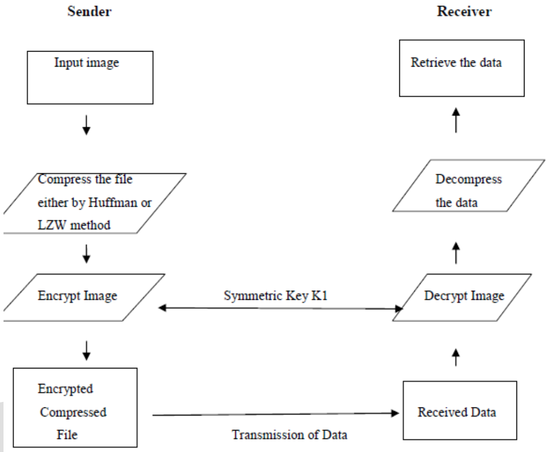


Figure 3. The schematic block diagram of proposed approach

Steps followed are as follow.

1) Browse or consider any standard grayscale or colored image which sender want to transmit securely and speedily.
2) Then sender choose any lossless algorithm either Huffman coding or LZW for compressing selected file.
3) Compressed image is encrypted by symmetric key k1 using DES algorithm and sent to receiver.
4) Receiver decrypt received data using same shared symmetric key k1.
5) Decompression of decrypted data is done either decompression algorithm of either Huffman or LZW to retrieve original transmitted data from sender.

Huffman coding:

Huffman code procedure is based on the two observations a. More frequently occurred symbols will have shorter code words than symbol that occur less frequently. b. The two symbols that occur least frequently will have the same length. The Huffman code is designed by merging the lowest probable symbols and this process is repeated until only two probabilities of two compound symbols are left and thus a code tree is generated and Huffman codes are obtained from labeling of the code tree

LZW compression:

It is a lossless ‘dictionary based’ compression algorithm. Dictionary based algorithms scan a file for sequences of data that occur more than once. These sequences are then stored in a dictionary and within the compressed file, references are put where-ever repetitive data occurred. LZW compression replaces strings of characters with single codes. The code that the LZW algorithm outputs can be of any arbitrary length, but it must have more bits in it than a single character. The first 256 codes (when using eight bit characters) are initially assigned to the standard character set. The remaining codes are assigned to strings as the algorithm proceeds.

Data Encryption Standard:

DES is the Data Encryption Standard, a United States government standard encryption algorithm for encrypting and decrypting unclassified data of the same length. It uses a symmetric key, which means that the same key is used to convert cipher text back into plaintext. The DES block size is 64 bits. JPEG images are fully compressed file format and especially used in case of lossy compression technique so while applying Huffman algorithm on JPEG image then on an average 10 to 20 % space reduction can be achieved While we get better result for following two JPEG images. Reconstructed image have same quality as compare to original because of lossless approach. On black and white or grayscale bmp images Huffman give better results. While discussing security of DES algorithm it has 64-bit key length so it is not easily affected by any attack except brute force. Time required to encrypt or decrypt image data is less so DES algorithm is fast and it achieves a good image encryption rate.

Original colored JPEG image

Reconstructed image

Original Grayscale JPEG image

Reconstructed image

5. Conclusions & Future Scope

In this paper, we proposed a new information hiding technique based on spatial domain in gray-scale image. We hide data in one block and use pixels contrastive relation. The data is easy to hide and extract and cannot be detected easily. Besides, it is compatible with JPEG lossy compression process. We can reduce the image file size and save time on transmission of images on the Internet. In addition, we can extract all of the embedded data correctly from the stego-image. People can hide important text data by this method. Therefore, our proposed method is more security and practical than the other hiding methods. utilized to embed some digital signature related data to authenticate losslessly compressed JPEG images.. The unified authentication framework provides both fragile and semi-fragile authentication. The former is for data integrity verification, while the latter for content integrity verification. Further more,

there are lossy and lossless two modules in the semi-fragile authentication. The robust lossless module. Specifically, if a losslessly compressed JPEG image data hiding scheme reported here is used for the lossless has not been altered correctly, the image will be classified as authentic and the original image can be recovered exactly. If the image is before authentication, the hidden data can be extracted compressed using JPEG losssy compression, the hidden data can be extracted correctly. Of course, the original image will not be able to be recovered. If the lossy compression is so severe that the resultant bit rate is lower than the specified minimum altered, then even the hidden data can be extracted out without error, the extracted data will render the extracted correctly, surviving bit rate, the hidden data will not beimage has been and the image will be rendered nonauthentic. If the content of the losslessly compressed altered image nonauthentic because the hidden data dismatch the altered content. The best way of fast and secure transmission is by using compression and encryption of multimedia data like images. The research works have been categorized this dual approach in the following three categories based on the order of the two process viz. CE, EC or JCE. From the above result, it is concluded that LZW compression is effective for grayscale bmp files as well as large text files. While it give effective result for 16bits or 8bits or 256 color image as compare to 24 bits image. In the proposed approach the key is required to send separately. This is a different issue of securely transmitting the secret key. Future scope of the proposed work is that we can design the mechanism to securely transmit the key so that unauthorized person should have no access to it. While currently this approach only focuses on multimedia data i.e. images but in future we will apply this approach on remaining data type e.g. audio and video and choose appropriate algorithm for encryption and compression which are suitable for them. The performance evaluation factors are Compression ratio and coding decoding time for compression and encryption respectively. But the balancing parameter for the combined process is not yet been defined.

6. References

[1] A. Razzaque, N. V. Thakur, "Image compression and encryption: an overview", International Journal of Engineering Research & Technology , Vol. 1. 5, pp. 1-7, July 2012.

[2] N. G. Bourbakis, "Image data compression-encryption using G-scan patterns", IEEE computational cybernetics and simulation , vol.2 pp. 1117-1120, Oct 1997.

[3]S. S. Maniccam, and N. G. Bourbakis, "SCAN based lossless image compression and encryption", IEEE Information intelligence and system , pp. 490-499, 1999.

[4] H. Cheng and X. Li, "Partial encryption of compress ed images and videos", IEEE Transactions On Signal Processing, Vol. 48. 8, pp. 2439-2451, August 2000.

[5] E. Celikel and M. E. Dalkilic, "Experiments on a secure compression algorithm", Proceedings of the International Conference on Information Technology : Coding and Computing , vol. 2, pp 150-152, April 2004.

[6] M. Ito, N. Ohnishi, A. Alfalou and A. Mansour, "New image encryption and compression method based on independent component analysis", IEEE information an-d communication technologies from theory to application , pp 1-6, April 2008.

[7] Y. You, H. Kim, "Endoscopy image compression and en cryption under fault tolerant ubiquitous environment" IEEE Biomedical circuit and system conference , pp. 165-168, Nov 2009.

[8] D. Maheswari, V. Radha, "Secure layer based compoun d image compression using xml compression" IEEE Computational intelligence and computing resea rch , pp 1-5, Dec 2010.

[9] A. Alfalou, C. Brosseau, N. Abdallah, M. Jridi, "Si multaneous fusion, compression, and encryption of multiple images", Optics express , Vol. 19. 24, pp 24023-24029, Nov 2011.

[10] G. H. Keat, A. Samsudin, Z. Zainol, "Enhanced perfo rmance of secure image using wavelet compression" World Academy of Science, Engineering and Technology , Universiti Sains Malaysia, pp. 633-636, 2007.

[11] N. V. Thakur, and O. G. Kakde, "Compression mechani sm for multimedia system in consideration of information security" Proceeding of International workshop on machine int elligence research, pp 87-96, 2009.