ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

A Novel Approach of Steganography, Encryption and Compression Mechanism

Swati P. Mane [1], Bharati Kale [2]

ME Student, Dept. of Computer Engineering, DPCOE, Pune, India[1]

Assistant Professor, Dept. of Computer Engineering, DPCOE, Pune, India[2]

ABSTRACT: Steganography is the technique of hiding the secret data into images. The proposed system uses an efficient steganography, encryption and compression mechanism. The secret data is encrypted and concealed into image. The image signature is generated and attached with image and it sends to the network service provider (NSP). The NSP compresses the image and sends it to the receiver. The receiver decompresses it and extracts contents from image and decrypts it.

KEYWORDS: Steganography, Cryptography, LSB, Alpha Threshold, NSP, Compression.

I. INTRODUCTION

Information security is not a single technology; rather it is an approach comprised of the processes, tools and policies necessary to prevent, detect, document and counter threats to digital and non-digital information. Information security is important for maintaining the confidentiality, integrity and availability of secret data. To provide security to secret data various techniques are used such as cryptography and steganography. Cryptography is the technique of converting readable data into unreadable format. This is easy technique and provides security up to some level. Steganography has made its own place in the field of security. Steganography used in an open-systems environment such as the Internet and Far-fetched applications, privacy protection, authentication, data integrity, intellectual property rights protection. Steganography technique conceals secret data into any of the medium for example image, audio, video, text. The concealed data can be any of the form either in plain text form or encrypted form. This technique increases the security level of secret information. To hide data inside image we need to do some process on image. Basically image is made up of pixels. Image can be of any type grayscale image, color image. The operations performed on image such as storing, filtering etc. is called image processing. The encryption and compression mechanism is not able to achieve high security of data; the data is easily revealed by third party member [1].The data hiding inside audio with parity coding and phase coding makes low capacity to hide information and even it makes difficult to decode data [2]. The security based on randomization use the MSB of randomly selected pixel as indicator. It increases the capacity of hiding data but it lowers the PSNR value of image signals [3]. To increase the capacity of hiding data and confidentiality of data needs strong steganography and encryption mechanism.

To address these issues the newly efficient steganography system is proposed with encryption then compression mechanism. An efficient steganography mechanism increases the hiding capacity, integrity, confidentiality of secret data. The modified version of encryption then compression mechanism [1] adds separable encryption on image. This system helps to user firstly estimate the how much load can carry the carrier medium. Outline of proposed system is as follows.

1) A multilevel algorithm is proposed which allows maintaining integrity of data and only authorized user can access the data based on image signature.
2) Modified encryption then compression mechanism based on steganography operation requires intensive computation.
3) Compression is done on stego image without losing original data. It is performed separately without intermediate other operation.
4) Development of algorithm with imperceptible of hidden data

DOI: 10.15680/IJIRCCE.2016. 0407053

II. RELATED WORK

Steganography based on RSA algorithm and Hash LSB technique [4] suggested by Anil Kumar, Rohini Sharma, uses hash function to generate a pattern for hiding data bits into LSB of RGB value of pixel of carrier image. This ensures data is encrypted before concealing into image. This method does not provide high security; if third party gets known about hidden data he can easily modify it. Edge based image steganography [5] proposed by Saiful Islam, Mangat Modi and Phalguni Gupta uses edges in the carrier image to conceal data. The amount of data storage is based on selection of edges. The more data is stored means the proper utilization made of weaker edges. This method increases the hiding capacity of data but does not provide security, integrity and availability of secret data. Steganography with wavelet transform and random number generation [6] anticipated by Mohammad Khan and Sarvesh Rai uses carrier image to hide secret data. The secret data is first encrypted and then it stored in secret image. At encrypted side image selection and logical operations, binary converter and random number generation these operations are done. It provides the security to data but does not maintain integrity of data. R. Rejani, D. Murugan and Deepu V. Krishnan [7] used pixel pattern based steganography. This method conceals the secret data inside an image by using existing RGB values. Along with image key will also send to decrypt the message at receiver side. To provide more security the secret message and key both are encrypted by using same or different keys. The benefit of it as it can be easily shared by any method. Pramendra Kumar and Vijay Kumar Sharma [8] in their work reviewed current security and privacy issues of cryptography and steganography. Security and privacy attributes such as integrity, availability, confidentiality and imperceptibility are four most representative issues identified in their work. Also existing security defense strategies and vulnerabilities that can be exploited by attackers and relation between security issues are taken into account.

In this paper we have suggested a system to bridge above gaps by providing a unified solution for shared data in network environment, preserving integrity of data along with reducing burden of computation on user system users.

III. PROPOSED SYSTEM

Steganography provides security to secrete data. It uses different methods of hiding data inside carrier medium such as LSB, MSB, Edge, Randomization and BPCS. Here in this proposed system I am considered base paper idea and made advancements into it for provide high security to data. The ETC system only does the encryption and then compression of image. But the proposed system does the steganography of encrypted data. Following fig. shows the whole system architecture.

A. System Architecture

Fig.1 shows proposed system architecture which shows how the overall operations performed by different user involved in system. The sender of system first takes covered image and secret data as input and does the channel separation and bit plane separation of image. Tithe payload estimation of LSB bits are done by using alpha threshold. Sender ensures the secret data is encrypted before hiding in image. The BPCS technique hides secret data inside image and generates stego image. Image signature is generated by using message digest algorithm and generated signature is embedded in stego image by alpha channel embedding. The finally watermarked image is generated. The NSP takes watermarked image as input and compresses it and sends it to receiver side. The receiver takes compressed image as input and decompresses it. Then it extracts the contents from stego image. The receiver checks the integrity of data by using image signature. If signature is matched then receiver decrypts the data.

DOI: 10.15680/IJIRCCE.2016. 0407053

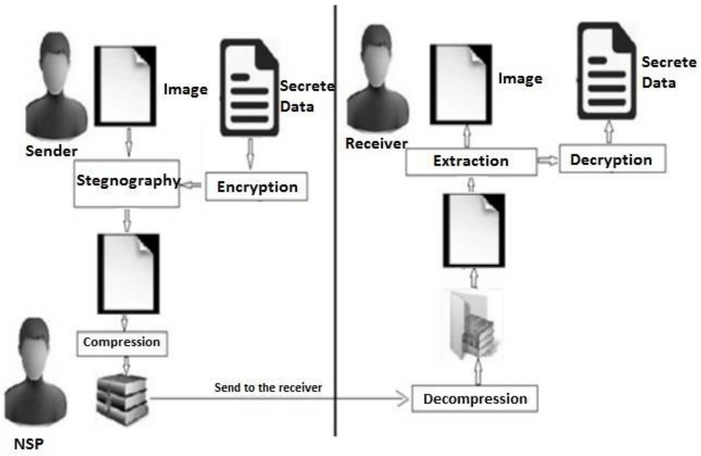


Fig1. System Architecture

B. System Flow

The following fig. shows the detailed execution of proposed system. The sender side and receiver side operations are shown how the encryption and decryption takes place.

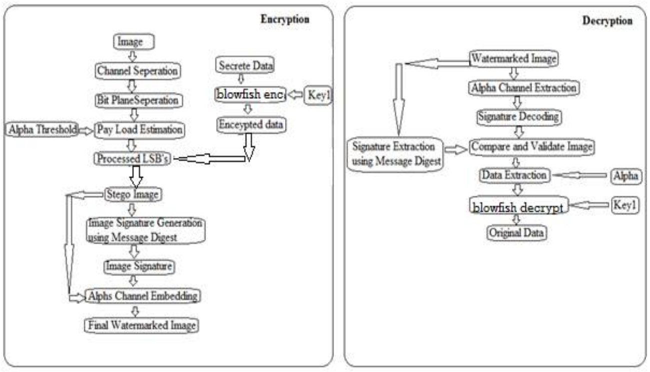


Fig2.System Flow

IV. MATHEMATICAL MODEL

Mathematical model is defined as follows:
Set-of-Inputs = {Ci, Sd, Pk}
Set-of-Outputs = {Wi, Ck, Od}
Where,
Ci = Covered image
Sd = Secret data
Pk = Encryption key
Ck = Compressed image
Wi = Watermarked image
Od = Original data

Expressions:

First system will perform system initialization phase and takes the system parameters from user including cover image, secret data and secret key as inputs.
C = *Encryption* (Sd, Pk)

The secret data must be encrypted before going to generate stego image. The encrypt function will generate cipher text data. Then LSB function will generate stego image.
Si = *Steganography* (Ci, C)
Where,
C= Cipher text and Si = Stego image.

The signature must be generated before watermarked image. The image signature function will generate signature. The signature is embedded into stego image by alpha channel embedding and finally watermarked image is generated.

Is = *Image_Signature* (Si)
Wi= *Alpha_Channel_Embedding* (Is, Si)

The network service provider takes water marked image and by using compression function compresses it. Then receiver will extract data from image and decode it.

Ck =*Compression* (wi)
Receiver = *Decryption* (Ck, Pk)

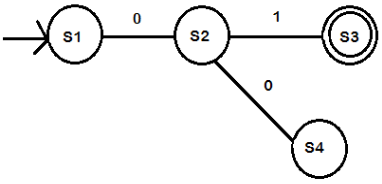


Fig3. State Transition Diagram

Where,
S1= Starting Node (Data Owner)
S2=NSP Node
S3=Receiver Node
S4=False
Success= If data is reached without modification to intended user
Failure= If data is modified by third party user

V. RESULTS

The secret file and original image needs to be taken as input. The secret file is encrypted by Blowfish algorithm. The Blowfish algorithm is symmetric cipher algorithm. It takes variable length key from 32 bits to 448 bits and it divides the data into 64 bit blocks. Following image shows the original image.

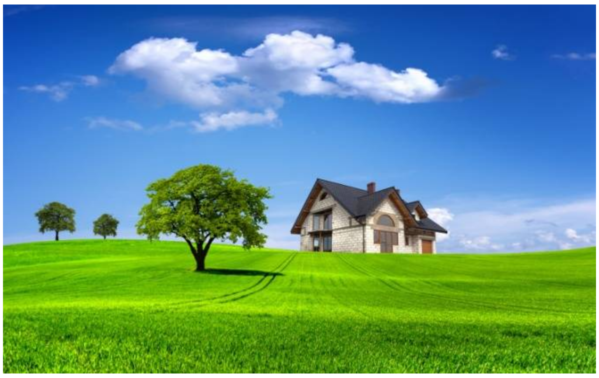
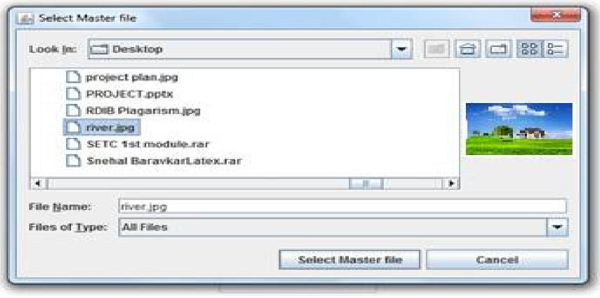


Fig4. Before Steganography

The above is the cover the image. The encrypted data file needs to be embedded into this cover image. The following fig. shows the data embedding file selection.



Select Master file

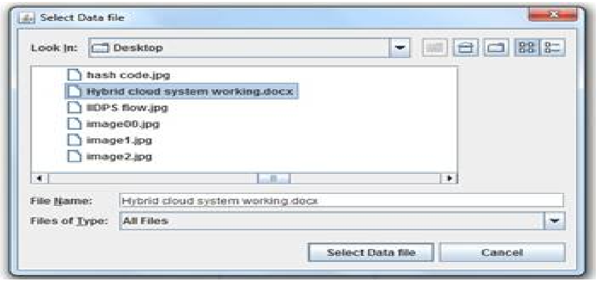
Look In: Desktop

project plan.jpg
PROJECT.pptx
RDIB Plagarism.jpg
river.jpg
SETC 1st module.rar
Snehal BaravkarLatex.rar

File Name: river.jpg
Files of Type: All Files

Fig5. Selection of Master File to Hide Data

The above master file selection selects the cover image from the system. Once the cover image selection done there needs to be select the data file to embed into cover image. The following fig. shows data file selection. The data file should have encrypted form. The encryption key is shared to receiver by email.



Select Data file

Look In: Desktop

hash code.jpg
Hybrid cloud system working.docx
IIDPS flow.jpg
image00.jpg
image1.jpg
image2.jpg

File Name: Hybrid cloud system working.docx
Files of Type: All Files

Fig6. Selection of Secret File

Once the data is successfully embedded into cover image the generated stego image and original cover image looks the same as shown in following fig.

Fig7. After Steganography

VI. CONCLUSION

An efficient steganography achieves high security by applying encryption and compression mechanism on data and image. Within proposed framework the encryption and decryption achieved via Blowfish Algorithm. The efficient steganography of image is done by using LSB technique. Highly efficient compression and decompression of water marked image has then been realized by Huffman Algorithm. It provides security and integrity of secret data through steganography of encrypted data and image signature. The proposed system also does the fast operations by doing different operation on different system; it saves time and speedup the overall performance of system.

REFERENCES

1. Jiantao Zhou, Xianming Liu, Oscar C. Au and Yuan Yan Tang, "Designing an Efficient Image Encryption-Then- Compression System via Prediction Error Clustering and Random Permutation" , Ieee Transactions Information Forensics And Security, Vol. 9, No. 1, pp.39-50, January 2014.
2. Kamalpreet Kaur DeepankarVerma , "Multi-Level Stganographic Algorithm for Audio Steganography using LSB, Parity Coding and Phase Coding Technique", International Journal of Advanced Research in Computer, Volume 4, Issue 1, pp.718-723, January 2014.
3. Namita Tiwari ,Dr. Madhu Sandilya ,Dr. Meenu Chawla , "Spatial Domain Image Steganography based on Security and Randomization" International Journal of Advanced Computer Science and Applications, Vol. 5, No. 1, pp.156-159 2014.
4. Anil Kumar, Rohini Sharma,"A Secure Image Technique Steganography Based on RSA Algorithm and Hash-LSB", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, pp.363-372, July 2013.
5. Saiful Islam, Mangat R Modi and Phalguni Gupta," Edge-based image steganography", EURASIP Journal on Information Security, pp.1-14, 2014.
6. Mohammad Sajid Khan, Sarvesh Singh Rai," Encryption Based Steganography Modern Approach for Information Security", International Journal of Computer Science and Information Technologies, Vol. 5 (3), pp.2914-2917,2014.
7. R. Rejani, D. Murugan And Deepu V. Krishnan, "Pixel Pattern Based Steganography On Images", Intact Journal On Image And Video Processing, Volume: 05, Issue: 03, pp. 991-997, February 2015.
8. Pramendra Kumar, Vijay Kumar Sharma, "Information Security Based on Steganography & Cryptography Techniques: A Review ", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 10, pp.247-250, October 2014

DOI: 10.15680/IJIRCCE.2016. 0407053