Data Hiding for Optimized Security

Anagha Bhute[1] Aishwarya Kekan[2] Aniket Bhosale[3] Prof Mrunalinee Patole[4]
[1,2,3]B.E. Student [4]Professor
[1,2,3,4]Department of Computer Engineering
[1,2,3,4]RMD Sinhgad School of Engineering, Pune, India

Abstract—It is very necessary to hide the confidential important data efficiently, as there are many attacks made by the hacker to hack the secret data. The secret data can be hidden with the help of steganography. BPCS (Bit Plane Complexity Segmentation) is type of digital steganography. In Steganography secret data is hidden into an image for securing the data. All other techniques have limited data hiding capacity but with the help of technique mentioned in this paper more amount of data can be hidden in vessel image. The cryptography concept is used for locking the secret message in the cover image. We make use of Bit Plane Complexity Segmentation (BPCS) Technique, in BPCS technique the image is divided into noise-like region. The secret data is hidden into these noise-like regions of the image without any deterioration. Hence this technique is a robust secure method for data hiding.

Key words: Data Hiding, AES Encryption, Image Signature, BPCS

I. INTRODUCTION

A huge amount of data is being stored and transmitted over the internet in the form images, text, videos, audios, secret messages etc. Our daily life is somewhere related to this massive data flow over the internet. Some of these files can be confidential or personal. This type of confidential data transmission mostly takes places in sectors like banking, governmental sector, military, IT sectors etc. So, security of these files has been necessity.

Such problems can be solved by hiding data in some of the images, not only hiding it but hiding it in encrypted form and providing a secret key. Even if the hacker tries to hack the data, still the data will remain protected as key plays an important role while extracting the hidden data. So by using this system mentioned in this paper data can be protected with high security.

II. RELATED WORK

Currently we are using AES encryption and BPCS algorithm for better security. Previously the technique used was LSB technique. In LSB the data stored was not more secured because while hiding the data encryption was not done. LSB was more time consuming and the data was stored bit by bit serially, but using BPSC and AES the encrypted secret data will be stored randomly making it more secure. Our technique will store more amount of encrypted data. The encryption key will also be generated to keep data secure from hacker. So even if the hacker tries to hack he will not get the exact original data. So our system overcomes the drawbacks the previous system had.

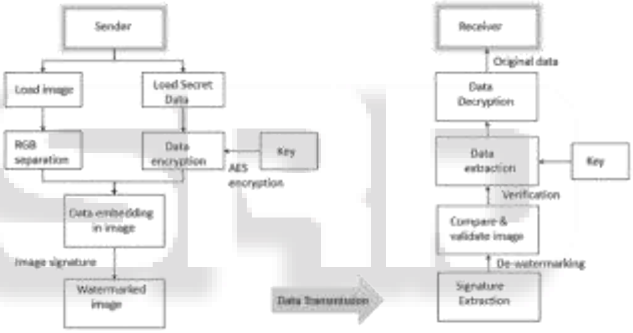
III. PROPOSED SYSTEM

A. System Introduction

To overcome the drawback of the existing system we have used AES encryption and BPCS algorithm, in this the binary image is divided into and noise-like region. The secret data is hidden into these noise-like regions of the image without affecting the quality of image. If the image is complex (i.e. full of colors. e.g. nature image) then more amount of data can be hidden. First the hiding capacity of an image is calculated, then according to capacity of the image we will encrypt our secret data in it. The user will be able to protect the secret data

B. System Architecture

The basic architecture of the system is shown in diagram below. The main aim of this system is to hide user's personal data efficiently & securely. The image and data uploaded will go under certain processes such as RGB separation, Pay load analysis, AES encryption, BPCS, watermarking etc. A secret key will be generated. At the receiver end while extracting the data AES decryption, extraction of image signature, de-steganography will takes place. The original data is then obtained.



C. System Modules

1) Load Image
2) Load Data
3) Data Encryption
4) Data Embedding
5) Image signature
6) Encryption key
7) Decryption

D. Algorithm

1) Select an image for hiding data.
2) Load the secret data.
3) Channel separation and Bit plane separation of the image will be done.
4) The payload analysis of the image will be carried out using α-threshold
5) Then the BPCS algorithm will be applied
6) At the same time the AES encryption algorithm will be applied on the secret data
7) The stego image will be marked with a certain signature.
8) Perform embedding operation to embed secret image in image.
9) A secret encryption key will be generated

10) Final image in which data is securely hidden is obtained.
11) Exactly the reverse procedure will be followed while extracting the original hidden data using AES decryption.

E. Feasibility Analysis

Our problem is P complete problem that can be proved by following points:

1) The entire data can be hidden in an image efficiently.
2) Every state is deterministic.
3) If size of data to be hidden is larger than size of image, then there is a possibility that image quality will decrease but still data can be hidden.
4) It is completely solvable problem.

F. Applications

1) Banking
2) Educational Sector
3) Military
4) Government sector

IV. System Features

1) Accurate and reliable data hiding
2) Easy for user to hide the data
3) Important data remains secure
4) Difficult for hacker to get the correct hidden data

V. Advantages

1) Any type of data can be hidden efficiently (video, speech, txt file)
2) Privacy maintained
3) Integrity
4) Non-repudiation
5) Difficult for stego analyzer to get the secret data.
6) Secret encryption key makes data hidden more secure

VI. Conclusion and Future Scope

Hence this method is very secure from network hackers due to its strong hiding algorithm used. Every time a new secret key will be generated through the same secret signal entered as the key developed is stored in the database and compared at the transmitter end. This encryption method generates a encryption secret key which provides optimized security for hiding the secret data within the image so that the data is secure and can be shared securely without any fear of hacker.

Future work can be done related to hiding more amount of data in a small image without affecting the quality of data as well as image. Several improvements could be implemented to our program to make the images with embedded data safer from detection or extraction by an unwanted user

References

[1] Eiji Kawaguchi and Richard O. Eason, "Principle and Applications of BPCS-Steganography", Kyushu Institute of Technology, Kitakyushu, Japan – University of Maine, Orono, Maine.

[2] X.Zhang," Separable Reversible Data Hiding in Encrypted Image," IEEE transactions on information Forensics and Security, Vol.7, No.2, April 2012

[3] Parag Kadam, Mangesh Nawale, Akash Kandhare and Mukesh Patil, "Separable Reversible Encrypted Data Hiding in Encrypted Image Using AES algorithm and Lossy Technique," 2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME)

[4] Rini.J, "Study on Separable Reversible Data Hiding in Encrypted Images," International Journal of Advancements in Research & Technology, Volume 2, Issue 12, December-2013 223 ISSN 2278-7763.

[5] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, “Reversible data hiding,” IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.

[6] N.Memon and P. W. Wong," A buyer-seller watermarking protocol," IEEE Trans. Image Process, vol. 10, no. 4, pp. 643–649, Apr. 2001.