A Survey on Data Hiding in Encrypted Images

Diptee D. Lad¹, Sindhu M. R.²
G. H. Raisoni College of Engineering Pune, Savitribai Phule Pune University

Abstract: Data hiding is the very sensible issue in today’s life. From last few year’s some researchers work on the data hiding techniques. So, in this paper we are including some techniques which are already implemented. We are using cryptographic and steganographic technique for hiding the data. Cryptography is the information hiding technique; there are multiple algorithms for cryptography. Here we are introducing AES (Advanced Encryption Standard) algorithm for encryption and decryption. Steganography hides the data using different image wrapper. In this paper we are including BPCS (Bit-Plane Complexity Segmentation) steganography technique.

Keywords: LSB, BPCS, AES, image decryption, image encryption

1. Introduction

Cryptography and Steganography are the two different things. Cryptography hides the data using number of algorithms. Encryption means converting plaintext into ciphertext and decryption means converting ciphertext into plaintext. Mainly there are two types of cryptographic technique Symmetric and Asymmetric. This paper survey on symmetric and asymmetric algorithm. For symmetric type AES algorithm is used and for asymmetric technique RSA algorithm is used. AES algorithm uses single key for encryption and decryption. It is more beneficial than the asymmetric key because symmetric key uses fewer bits for encryption. Asymmetric key uses more bits than symmetric key because it uses more maths power. Asymmetric key uses more processing time than symmetric key. Asymmetric algorithm uses two independent keys for encryption and decryption. At sender side public key is used for encryption and for receiver side private key is used for decryption.

1.2 Decryption

Decryption is the reverse process of encryption. It is the process of decoding the data which is in encoding format. An authorized user can only decode data because decryption requires a private or public key. To make the data confidential, data is encrypted using a particular cryptographic algorithm. To decrypt the cipher text receiver should have to use similar algorithm and then only receiver gets original data.

1.3 Cryptography

Cryptography is technique for protecting information in computer systems. This technique writing a secret code. It includes the protocols, algorithms and to securely prevent or delay unauthorized access to sensitive information in a communication. Cryptosystems are not only mathematical process and computer programs, but also it include the human behavior, for choosing hard-to-guess passwords, switched off unused systems, and not spreading sensitive information with outsiders.

Objectives of Cryptosystem
1. Privacy: Only an authorized people able to extract the contents of the message.
2. Integrity: The information cannot be altered in communication.
3. Non-Repudiation: Prove that the sender really send this message to the receiver.
5. Access control: Identify that who is authorized receiver.
1.4 Steganography

Steganography is the hiding message into another message. The aim of the steganography is to protect a message from a third party. Steganography hides the message with its existence of secret communication. Steganography work with hidden data so only the sender and the receiver knows the secure data. In this a technique secret data is hidden into dummy image. All other remaining techniques have limited data hiding capacity. This method includes hiding messages within images, combining a message within random data, wrapping pictures with the message within video file. Network Steganography is used in telecommunication networks. Cryptographic methods secure the content of a message. The first application of hash algorithm in cryptography is message purity. The hash value provides a digital fingerprint of a message's contents, which identifies that the message has not been altered by an intruder. The inputs to a hash function are typically called messages, and the outputs are often called as message digests. Hash function H accepts messages of any length, and outputs a fixed length digest of one - bit. H returns 0 as the message digest if the input has an even number of characters, and returns 1 if the output has an odd number of characters.

Comparison between cryptographic technique

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Symmetric key</th>
<th>Asymmetric key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Definition</td>
<td>Symmetric Encryption uses a single secret key that needs to be shared for decryption.</td>
<td>Asymmetric encryption uses a public key and a private key to encrypt and decrypt data in communication.</td>
</tr>
<tr>
<td>Key distribution</td>
<td>Eliminate need to spread key over network.</td>
<td>Problem of the asymmetric key is to share the key over network.</td>
</tr>
<tr>
<td>Speed</td>
<td>Symmetric encryption algorithms can be relatively low complexity allows for easy implementation in hardware.</td>
<td>Compared to symmetric encryption, asymmetric encryption imposes a high computational burden, and tends to be much slower.</td>
</tr>
</tbody>
</table>

2. Types of Cryptography

A. Symmetric key cryptography

In this type of cryptography same key is used for encryption and decryption. This key is spread over the secure line. One constraint is that key must be known to the sender and receiver.

![Symmetric key cryptography](image)

Figure 3: Symmetric key cryptography

Given message and the key is having same length as plaintext. Decryption uses the reverse process of encryption so, it requires same key as encryption.

B. Asymmetric key cryptography

Asymmetric key cryptography also referred as public key cryptography. The main difference in symmetric and asymmetric is that symmetric key does not share a private key. In asymmetric cryptography there are two types of keys public key and private key. Encryption is done through public key and decryption is done through private key. Receiver creates a both keys so receiver is responsible to distribute public key to the sender.

![Asymmetric key cryptography](image)

Figure 4: Asymmetric key cryptography

C. Hash Algorithm

Hash algorithm is also called message digest. It is not having any kind of key. The first application of hash algorithm in cryptography is message purity. The hash value provides a digital fingerprint of a message's contents, which identifies...
Figure 5: Steganography using Least significant bit

B. Bit Plane Complexity Segmentation

Bit Plane Complexity Segmentation (BPCS) technique embedding data into bitmap file. The goal of BPCS is to wrap a data into a cover image without detection by human interaction. In BPCS, the vessel image is divided into two region first is “informative region” and another one is “noise-like region”, secret data is hidden into dummy image without corruption of image quality. In LSB technique last 4 bits are hidden but in BPCS technique MSB plane with LSB plane provide a security on data. The primary goal of BPCS Steganography is to make use of as much capacity of image for data hiding without much corruption in the visual display of the original image.

In BPCS Steganography color images are mostly used for dummy data. BPCS Steganography has the large capacity of embedding data. The original BPCS algorithm divides the image into bit-planes, and there is high correlation between the bit planes. The higher the bit-plane is, the stronger the correlation between the pixels of the bit-planes is.

Advantages of BPCS stegnography
1. Information hiding is about 50-60%
2. A sharpening operation on the vessel image increases the embedding capacity
3. It is most secured technique

Comparison between LSB and BPCS

<table>
<thead>
<tr>
<th>Parameter</th>
<th>LSB</th>
<th>BPCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accuracy</td>
<td>This is the traditional technique. It has limited data hiding capacity and that can hide up to 10-15% of the vessel data amount</td>
<td>BPCS technique can hide up to 50-60% of data</td>
</tr>
<tr>
<td>Process</td>
<td>In LSB technique, hide the data with last four bits.</td>
<td>In BPCS technique, data is hidden in MSB planes with the LSB planes</td>
</tr>
</tbody>
</table>

4. Proposed System

Figure 6: Flow of Proposed system

Proposed system uses BPCS technique for embedding data. BPCS-Steganography is different from traditional approach. It has large embedding capacity. BPCS overcome the short comings of traditional stegnographic techniques. In BPCS, the vessel image is divided into informative region and noise like region and the secret data is hidden in noise blocks of vessel image without affecting on image quality.

In the proposed system text, image and audio data is hiding through the stegnography and encryption techniques. For cryptography algorithm, this system uses AES algorithm which is symmetric cryptography. Because it requires less bit for encryption.

5. Acknowledgment

I take this opportunity to thank Prof. Sindhu M.R. for her valuable guidance and for providing all the necessary facilities and her suggestions.

6. Conclusion

This paper analysis on probabilistic and homomorphic properties for ciphertext images encrypted by symmetric key and asymmetric key cryptography. By using proposed scheme we can replace ciphertext pixel values with new values for embedding additional data into BPCS plane. The
wrap data can be extracted for encrypted domain and this does not affect decryption of plaintext image.

References


