**Information Hiding using Key Dependent Improved Canny Edge Detection and RSA Algorithm**

Priyanka Mehta\(^1\) Jignesh Vania\(^2\)

\(^1\)M.E Student \(^2\)Faculty

\(^1,2\)Department of Computer Engineering

\(^1,2\)L.J.I.E.T., Ahmedabad, India

Abstract— Many potential problems have resulted from the improving Internet, such as the copy and corruption of digital information. Therefore, the information security is considered as one immediate topic. Cryptography and steganography are the most widely used techniques to defeat this threat. Steganography embeds message into a cover media and hides its existence. On the other hand, Cryptography involves converting a message text into a scrubbled cipher. Both the techniques provide some security of data, neither of them is individually secure enough for sharing information over an unsecure communication channel and are vulnerable to intruder attacks. In this paper we have proposed a secure technique of image steganography i.e. Key dependant improved canny edge detection with RSA algorithm. The proposed technique enhances the security to new level as it provides authentication module too.

**Key words:** Steganography, Cryptography, RSA encryption, improved canny edge detection, LSB, digital signature

**I. INTRODUCTION**

Steganography is the art of passing information in a manner that the very existence of the message is unknown. The goal of steganography is to avoid drawing suspicion to the transmission of a hidden message. If suspicion is raised, then this goal is defeated. It serves as a better way of securing message than cryptography which only conceals the content of the message not the existence of the message. Original message is being hidden within a carrier such that the changes so occurred in the carrier are not observable. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet.

Fig. 1: Work flow of Steganography

In steganography the secret information is hidden inside a carrier file such that the change in appearance of the carrier file should not be apparent to normal human eye. It is often confused with cryptography because the two are similar in the way that they both are used to protect secret information.

The difference between the two is that steganography involves hiding information so it appears that no information is hidden at all. If a person or process views the file where information is hidden, he or she will have no idea that there is hidden information, therefore the person will not attempt to decrypt the information. Where as in case of cryptography the confidential information is encrypted by a key and sent on the channel. A person or a process by seeing this can notice that something is under communication, but he/she cannot steal the information unless he knows the key. But in steganography the person or process who sees it will not even suspect that some secret information is on transit. Steganography can be achieved in three ways by using three types of carriers.[2]

**II. EVOLUTION OF STEGANOGRAPHY**

For understanding the term steganography, its predecessor i.e. cryptography, has to understand first. Cryptography has followed man through many stages of evolution. Cryptography can be found as far back as 1900 B.C. in ancient Egyptian scribe using non-standard hieroglyphics in an inscription. From 500 – 600 B.C. Hebrew scribes used ATBASH, a reversed alphabet simple solution cipher. From 50 - 60 B.C. Julius Caesar used a simple substitution with the normal alphabet in government communications. [1] Cryptography continued through history with many variations. Today cryptography has evolved as quantum cryptography. Quantum cryptography combines physics and cryptography to produce a new cryptosystem that cannot be defeated without the sender and receiver having the knowledge of the attempted and failed intrusion. Through the long history of cryptography, steganography was developed and flourished on its own.

Steganography comes from the Greek steganos (covered or secret) and -graphy (writing or drawing). Steganography can be defined as the hiding of information by embedding messages within other, seemingly harmless messages, graphics or sounds. During times of war, steganography is used usually. Invisible Inks were used in the American Revolutionary War by both the British and American forces. Invisible ink was used to write information on pieces of paper so that the paper appeared to the average person as just being blank pieces of paper. Liquids such as milk, vinegar and fruit juices were used, because when each one of these substances is heated it becomes dark and become visible to the human eye [3]. A thorough history of steganography can be found in the followed content of this paper.

**III. CLASSIFICATION OF STEGANOGRAPHY**

For decades people strove to develop innovative methods for secret communication. Classification of information hiding can be depicted as follows:

1. ** overt methods:**
   - Visible methods
   - Infrared
   - Ultraviolet

2. **covert methods:**
   - Audio
   - Video
   - Radio

3. **steganography methods:**
   - Visible
   - Invisible

4. **cryptographic methods:**
   - Symmetric key
   - Asymmetric key

5. **mimicry methods:**
   - Scribbled cipher
   - Scribbled message
   - Scribbled cipher

The difference between the two is that steganography involves hiding information so it appears that no information is hidden at all. If a person or process views the file where information is hidden, he or she will have no idea that there is hidden information, therefore the person will not attempt to decrypt the information. Where as in case of cryptography the confidential information is encrypted by a key and sent on the channel. A person or a process by seeing this can notice that something is under communication, but he/she cannot steal the information unless he knows the key. But in steganography the person or process who sees it will not even suspect that some secret information is on transit. Steganography can be achieved in three ways by using three types of carriers.[2]
Steganography is cryptography. But it is the hiding of message that are information can be transmitted without alerting eavesdroppers.

The extensively used technique today is hiding of secret messages in a digital image. This steganography technique exploits the weakness of the human visual system (HVS). HVS cannot detect the variation in luminance of color vectors at collection of color pixels. The individual pixels can be represented by their optical higher frequency side of the visual spectrum. A picture can be represented by a characteristics like 'brightness', 'chroma' etc. Each of these characteristics can be digitally expressed in terms of 1s and 0s. For example: a 24-bit bitmap will have 8 bits, representing each of the three color values (red, green, and blue) at each pixel. If we consider just the blue there will be 2 different values of blue. The difference between 11111111 and 11111110 in the value for blue intensity is likely to be undetectable by the human eye. Hence, if the terminal recipient of the data is nothing but human visual system (HVS) then the Least Significant Bit (LSB) can be used for something else other than color information.

There are various techniques to achieve steganography like Least Significant Bit Insertion, Masking & Filtering and Algorithms & Transformations. [29] Each of these techniques can be applied, with varying degrees of success, to different image files. Least Significant Bit Insertion is a common, simple approach to embedding information in a cover file.

There are three basic parameters for evaluation of different steganography techniques.

1) Imperceptibility: It is the ability of steganography method to avoid detection of hidden message through human visual system (HVS) and statistical analysis. It can be measured through peak signal to noise ratio (PSNR) [7].
2) Capacity: It is number of bits of message that are hidden into a stego image.
3) Robustness: It is ability of the steganography technique to retain the hidden message after many image related operations. These operations are compression, cropping, rotation and filtering etc.

IV. APPLICATIONS

There are many applications for digital steganography of images, including copyright protection, feature tagging, and secret communications [26].

A. Copyright Protection:
A secret copyright notice or watermark can be embedded inside an image to identify it as intellectual property [27]. This is the watermarking scenario where the message is the watermark [27].

B. Feature Tagging:
Captions, annotations, time stamps, and other descriptive elements can be embedded inside an image, such as the names of individuals in a photo or locations in a map. The number of times an image has been viewed can be embedded for “pay-per-view” applications.

C. Secret Communications:
In many situations, transmitting a cryptographic message draws unwanted attention. The use of cryptographic technology may be restricted or forbidden by law. However, the use steganography does not advertise covert communication and therefore avoids scrutiny of the sender, message, and recipient. A trade secret, blueprint, or other sensitive information can be transmitted without alerting potential attackers or eavesdroppers.

V. STEGANOGRAPHY BLENDED WITH CRYPTOGRAPHY

There are many aspects to security and many applications. One essential aspect for secure communications which is needed with steganography is cryptography. But it is important to note that while cryptography is necessary for secure communications, it is not by itself sufficient. There are some specific security requirements[30] for cryptography, including Authentication, Privacy/confidentiality, and Integrity Non-repudiation. The three types of algorithms are described:
(i) Secret Key Cryptography (SKC):Uses a single key for both encryption and decryption
(ii)Public Key Cryptography (PKC): Uses one key for encryption and another for decryption.
(iii) Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information.

Steganography is the other technique for secured communication. It encompasses methods of transmitting secret messages through innocuous cover carriers in such a manner that the very existence of the embedded messages is undetectable. Information can be hidden in images [21], audio, video, text, or some other digitally representative code. Steganography systems can be grouped by the type of covers [30] used (graphics, sound, text, executables) or by the techniques used to modify the covers
- Substitution system
- Transform domain techniques
- Spread spectrum techniques
- Statistical method
- Distortion techniques
- Cover generation methods

K Boopathybagan[22] proposed in order to provide strong security, we use two levels of data encryption. When the data encryption is done, using steganographic techniques the cipher text is hidden inside the image. The message will be first encrypted using the Playfair cipher which is also known as playfair square. The first ciphertext will again be encrypted using Advanced Encryption Standard technique.

Vanita M. Mane [23] used and hybrid encryption algorithm, DES algorithm for data transmission because of its higher efficiency in block encryption, and RSA algorithm for the encryption of the key of the DES because of its management advantages in key cipher. Under the dual protection with the DES algorithm and the RSA algorithm, the data transmission will be more secure. The proposed system works to hide data which should not be loss single digit.

Anil Kumar [24] presented the problem statement consisting of embedding the secret message in the LSB of each RGB pixels value of the cover image. Before embedding, the secret message is to be converted to cipher text using RSA algorithm to enhance security.

Ayasha Siddiqua [25] considered a digital color image consists of different pixels. In binary notation, it is represented by a stream of 8 bits. Therefore in total, 24 bits are required to denote a pixel. Thus an image is an array of many bytes each representing a single color information lying in a pixel. In the proposed method, a group of three sequential bytes from such an array is used to embed a bit of the entire message. This proposed work gives more security but provides less capacity for embedding information.

VI. PROBLEM FORMULATION AND WORK METHODOLOGY

The problem statement consists of hiding secret message in LSB of each pixel value of cover image. Before embedding the message has to be converted to cipher text using RSA algorithm to enhance security.

Then improved canny edge detection algorithm is applied to obtain edge image from image cover image.

![Flow chart of Sender side in proposed model](image)

In the proposed method, a group of three sequential bytes from such an array is used to embed a bit of the entire message. This proposed work gives more security but provides less capacity for embedding information.

1) Step 1: Division of cover image is done into set of blocks, having n-pixels each. P1 pixel is used to store status of other pixel. The status of each pixel Pi, is defined as “1" if it is a edge pixel. If non-edge pixel then “0". The status of pixels from P2 to Pn is stored inside P1 by LSB substitution operation. To preserve the quality of pixel P1 as well as to increase the embedding payload, based on the experimental results, we suggest assigning the values of n as 3, 4.

2) Step 2: For a non edge pixel in a block we embed ‘x‘ bits of message XOR with ‘x’ MSBs of the pixel by LSB substitution operation. To maintain the quality of the stego image, the value of x here is 1 or 2.
3) Step 3: For an edge pixel in a block, we embed ‘y’ bits of message XOR with ‘y’ MSBs of the pixel by LSB substitution. The value of ‘y’ is generated randomly for each pixel using chaotic map. To maintain the quality of stego image, the value of y is generated between 1 and 4.

And totally opposite approach is followed on receiver side. Firstly the stego image received on receiver side and edge pixels are identified.

![Flow chart of Receiver side in proposed model](image)

From the whole stego image at every pixel the message is hidden so if a pixel is edge pixel then 3 or 4 LSBs and if a pixel is a non edge pixel then 1 LSB has to be checked to fetch embedded bits of secret message.

Next step is to decrypt the message bits obtained from the stego image. After decryption the message integrity is checked by verifying the digital signature generated.

VII. PERFORMANCE ANALYSIS AND RESULTS

According to the proposed system discussed in the previous section, if “hello” is given as input to the system:

![Output of Digital signing and RSA](image)

![Lena Image: (a) Original Image (b) Edge Image (c) Stego Image](image)

The above figure shows the cover image and its edge image obtained, whose edge pixels will be used to conceal the secret message obtained in the previous step.
After getting the hidden message retrieved from the pixels of the stego image, the hidden message is decrypted and we finally get the secret message at the receiver's side.

A comparison is done for the cover images available using the available method as well as the proposed method. And we get the following comparison out of it. And also for the same comparison graphs are plotted to illustrate the mentioned values of MSE and PSNR value on basis of which the comparison is done.

<table>
<thead>
<tr>
<th>Cover Image</th>
<th>MSE</th>
<th>PSNR(in db)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baboon</td>
<td>0.001820</td>
<td>75.531019</td>
</tr>
<tr>
<td>Lena</td>
<td>0.002365</td>
<td>74.392286</td>
</tr>
<tr>
<td>Lotus</td>
<td>0.153054</td>
<td>56.282360</td>
</tr>
<tr>
<td>Peppers</td>
<td>0.055897</td>
<td>60.656937</td>
</tr>
<tr>
<td>Tiger</td>
<td>0.031993</td>
<td>63.080246</td>
</tr>
</tbody>
</table>

Table 1: Comparison of proposed system with existing system

Fig. 7: Retrieved hidden message

Fig. 8: MSE of Key dependent algo vs. Proposed System

Fig. 9: PSNR value of Key dependent algo vs. Proposed System

VIII. CONCLUSION AND FUTURE WORK

Cryptography and steganography are the key techniques or branches of data security which gives higher level of security. In the proposed system, cryptographic and steganographic are combined to provide two-tier security to the secret data i.e. secret message is initially signed by the sender, then is encrypted before hiding it into the cover image which gives high security to secret data. RSA algorithm is used to encrypt secret message and Canny edge detection with key dependent image steganography methods are used to conceal encrypted secret message within cover image. Since the resultant perceptual quality of the stego image is of good quality, it is almost not attracted from eavesdropper by bare eye. Finally it can be concluded that the proposed system is efficient for secret data communication obtained in concurrence with more payload capacity and good imperceptibility with authentication too.
Information Hiding using Key Dependent Improved Canny Edge Detection and RSA Algorithm

<table>
<thead>
<tr>
<th>Technique used</th>
<th>Imperceptibility</th>
<th>Capacity</th>
<th>Robustness</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Dependent Image Steganography Using Edge Detection</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>RSA Algorithm and Hash-LSB Technique</td>
<td>Medium</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>Proposed System</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>

Table 2: Comparison of proposed system with existing systems wrt parameters of Steganography and Cryptography

In future the steganography could be done with the help of fuzzy based algorithms. And also, steganographic technique can emerge with more storage capacity in less time.

REFERENCES


