Enhancing Security using Digital Image Processing

Hemkesh V Kumar, Jeevan Nagaraj, Manoj S Hegde
(01FB14ECS083, 01FB14ECS088, 01FB14ECS114)
Team Alekhya
Department of Computer Science and Engineering, PES University

ABSTRACT

In this paper, we address the problem of enhancing security of a secret image and secret message that is to be sent over a network, by digitally processing it. We require that the secret image and secret message to be sent to the recipient in such a way that no one else suspects the existence of them. A cover image is used as a decoy in this technique in which the secret image as well as the secret message are embedded.

On the sender's side, the secret image is encrypted using AES Algorithm. In this encrypted secret image, the secret message is hidden using LSB Based Image Steganography. Furthermore, the encrypted secret image with the secret text is hidden in the cover image, using LSB Based Image Steganography. The stego image thus obtained is split into 16 parts, indexed and sent to the receiver.

On the receiver side, these sub images are fetched one by one and merged based on their index. The encrypted image is obtained from the merged image. Next, we extract the secret text from the LSBs of this encrypted image. Additionally, decryption is performed to extract the original secret image from the encrypted secret image. Thus, the receiver obtains the secret image and the secret message from the cover image.

1. INTRODUCTION

Quite often, we communicate exceedingly confidential information over a communication network that we want only the recipient to know. How do we protect such information from malicious attacks? Techniques like steganography, encryption and cryptography can be used to keep our data confidential. [5] But, a combination of these techniques would help us keep our data highly confidential. In this paper, we address the problem of security breaches using digital image processing.

The paper that we used for reference was 'Enhancing Security using Image Processing' by Rahul Kumar, Ajit Pratap Singh, Arun Kumar Shukla, Rishabh Shukla. This research paper was published in International Journal of Innovative Research in Science, Engineering and Technology in April 2015.

2. REVIEW OF PAPER CHOSEN

The chosen paper illustrates the requirement of security while transferring images using any electronic modes. [1] This could be achieved using image steganography and stitching. The paper also mentions about the existing techniques like watermarking and visual cryptography. Watermark is a sequence of characters embedded in a document to uniquely identify its originator. Visual cryptography deals with encrypting information in images so that it can be decrypted by human eye if an appropriate key image is used. [2]

The paper proposes a system where the entire workflow is broken down into four phases. Initially the secret image is broken into multiple parts.

- **Encryption phase** – In this phase AES algorithm is used to encrypt the secret message.
- **Embedding phase** – Cipher text is hidden inside the image using LSB based image steganography algorithm.
- **Hiding phase** – Kekre's Median Codebook Algorithm is used for image steganography. Image is segmented into parts and each part converted into vectors in this step. Part of secret image is hidden behind the cover image using steganography and the resulting image is sent across to the receiver's end.
- **Stitching phase** - K-nearest neighbour supervised algorithm is used. SIFT features are extracted from all sub images. KNN is found for each feature using k-d tree. RANSAC is used to find geometrically consistent feature matches. Later connected components of image matches are found out.

The paper states that it would become difficult for the intruder to decode all the parts of the images, as they are encrypted and out of order.

3. CRITIQUE

The secret message is encrypted using AES algorithm while the secret image is normally hidden using LSB based image steganography. This makes things easier for a malicious third party user to use methods such as brute force to extract the secret image from the stego image during the transmission of the image over a communication network. Hence, in our implementation, we encrypted the secret image using AES algorithm and hid the secret text using LSB based image steganography in this encrypted image.

The paper proposes using Panorama Image Stitching to stitch the images sent in parts. This requires all image blocks to have overlapping content. Stitching the images using panoramic stitching would result in an image which has its constituent bits modified, thus leading to loss in information in terms of the secret image as well as the secret message.

4. PROBLEM STATEMENT

We know that email service providers sell our data to third party companies for their usage and profits. In today's scenario, security is a major concern while transmitting any information over the network. Security provided by the network is insufficient with the increasing rates of cybercrimes. Therefore, we need employ other techniques to carefully send our data over the network. In this project, we explore a number of security techniques that can be combined together to ensure higher levels of security to our data.

5. APPROACH

Image encryption and decryption was implemented using the AES algorithm. Firstly, the given image was resized to a known size (480 x 480). Then the image was divided into Nx16 blocks. The sender and receiver use a key of 128 bits. This key must be shared between the sender and the receiver in a secure manner. The key can be imagined as blocks x[0],x[1]...x[15], where each block is 8 bits long. [4]

AES Encryption is done in rounds, where we process 16 pixels in each round. The AES algorithm uses a round function that is composed of four different byte related transformations:

1. **SubBytes step:** Each value in the state matrix (original image) is replaced with a subbyte using an 8-bit substitution box (S-box). This ensures non-linearity in the cipher. The S-box is constructed by combining the inverse function with an invertible affine transformation. An 8-bit lookup table is used to replace each byte in the state S as, b[i,j]= S(a[i, j]) (Figure 3a)

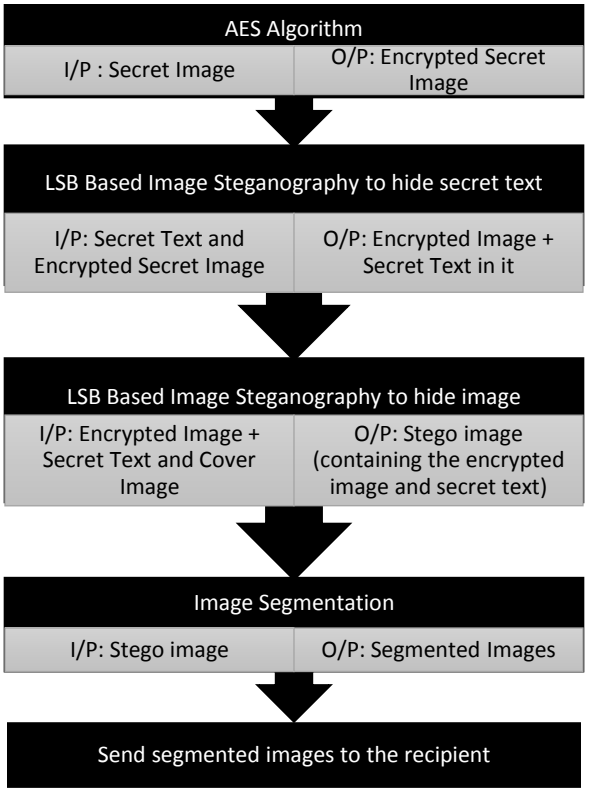


Figure 1 | **Sequence of steps performed by sender**

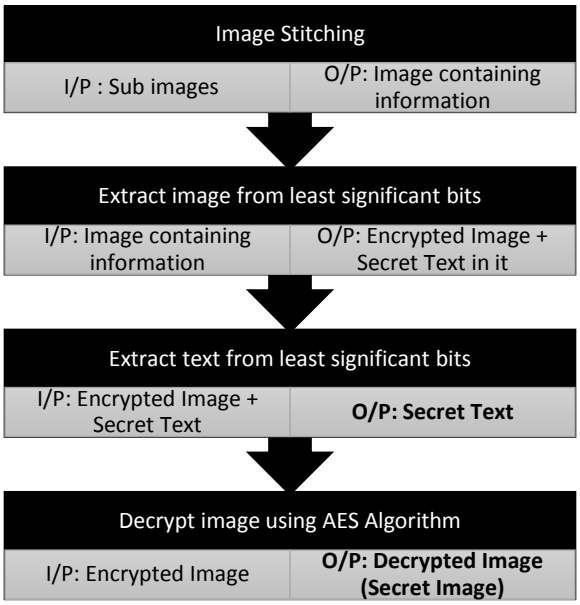
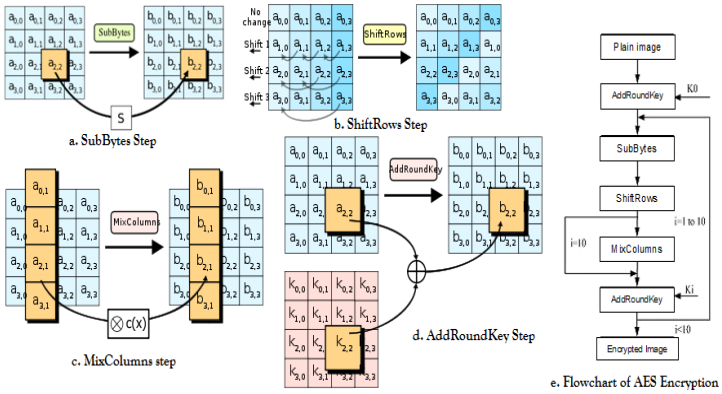
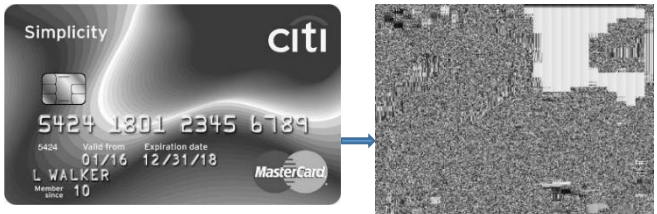


Figure 2 | **Sequence of steps performed by the receiver**

2. **Shift Rows step:** The bytes in each row are shifted by a certain offset to the left that increases iteratively. The first row is left unchanged. Each byte of the second row is moved one byte to the left cyclically. Similarly, the third and fourth rows are moved by offsets of two and three accordingly. (Figure 3b)
3. **Mix Columns step:** The four blocks of each column of the state are joined using an invertible linear transformation like multiplication followed by bitwise XOR. This function takes four bytes as input and outputs four bytes. Addition is a simple XOR operation. Multiplication is modulo irreducible polynomial. Each column of the state is multiplied with a fixed polynomial c(x). (Figure 3c)
4. **Add Round Key step:** The state and sub key are combined. Using the main key, a sub key is found. The sub key is added by XORing a byte from the state with its respective byte form the sub key. (Figure 3d) [6]





Secret Image [9]

(f)

Encrypted Secret Image

Figure 3 | **AES Algorithm**

After encrypting the secret image, least significant bit based image steganography is performed to hide the secret message in the secret image. We append a null character with the secret text to denote the end-of-text. LSB based image steganography involves hiding data in the least significant bits of an image as it contains the least amount of information in an image and flipping them will not cause a significant change in the appearance of the image. [3] The secret message is converted into its ASCII representation. These ASCII values are converted into their 8-bit binary representation. The least significant bits of the pixel values of the secret image are replaced with these bits in order. Hence the secret text is successfully hidden inside the secret image.

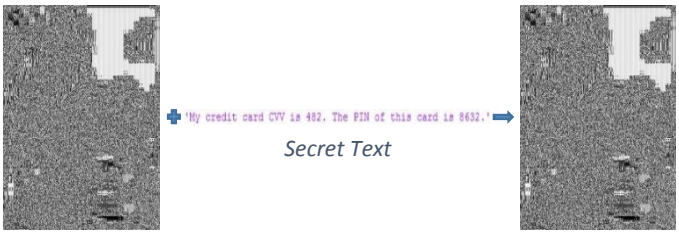


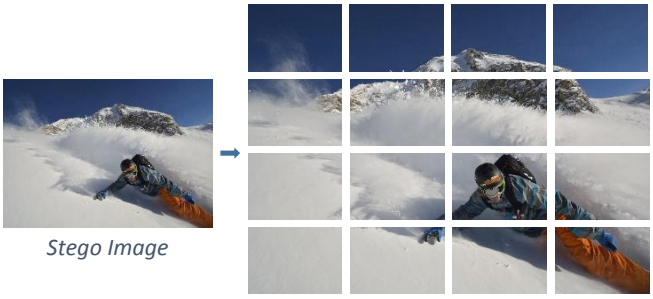
Figure 4 | **Hiding of secret key inside the encrypted secret image**

Similar to the method of LSB based image steganography that involved hiding the secret message into the secret image, the encrypted secret image containing the secret text is hidden inside the cover image using the same technique. The binary representation of the pixel values of the encrypted image with the secret text in it is hidden first in the red component, followed by the blue and the green components of the cover image. [7]

Encrypted Image *Cover Image* [8] *Stego Image*

Figure 5 | **Hiding of encrypted image containing the secret text inside the cover image**

Next, we divide the cover image with the encrypted secret image and the secret text embedded in it into multiple parts (16 to be specific). Each part is then separately sent to the recipient.



Stego Image *Segmented Images*

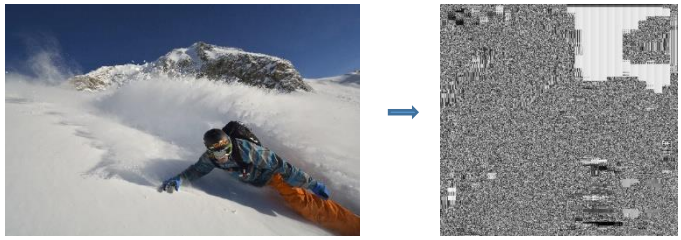
Figure 6 | **Segmentation of the stego image**

On the receiver's end, the sub images are stitched back based on their index values (0 to 15) to regain the original cover image.

Sub Images *Merged Image Containing Information*

Figure 7 | **Stitching of sub images into a single image**

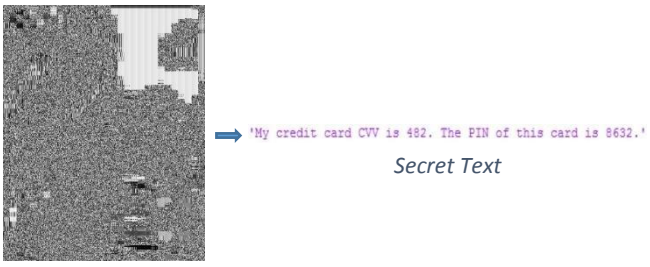
The least significant bits of the red, blue and the green components are extracted 8-bits at a time for the entire size of the secret image. Now, we obtain the encrypted secret image with the secret text embedded in it.



Merged Image Containing Information *Encrypted Image + Secret Text in it*

Figure 8 | **Extracting the encrypted image from the least significant bits of the stego image**

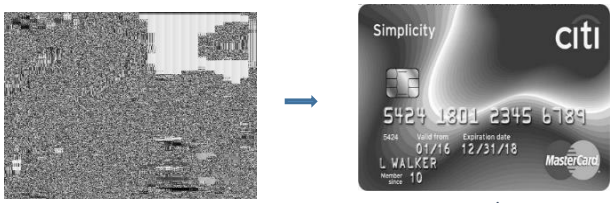
From this secret image, the least significant bits are extricated, 8 bits at once, until we hit a number representing a zero. These 8 bit binary numbers obtained are converted to their decimal representation. These decimal representations represent the ASCII values of the characters. They are then converted back to their character representation to obtain the secret message.



Encrypted Image + Secret Text in it *Secret Text*

Figure 9 | **Extracting the secret text from the encrypted image**

The process of decryption of secret image using AES is similar to the encryption process, but in reverse order. First, Add Round Key step is performed where we undo the changes made to the image on sender's side. Then Inverse Mix Columns step is performed where we apply an inverse of the polynomial function on the image. This brings back the columns of the image to its original configuration. Then we shift back the rows of the image that were jumbled on the sender's side before sending. Then inverse substitution is applied by taking the inverse of the 8-bit table lookup. On repeating the process, we obtain the secret image on the receiver's end.



Encrypted Image *Decrypted Image*

Figure 10 | **Decrypting the encrypted image using AES Algorithm**

6. CONCLUSION

Our project has put forth a new system where AES encryption is combined with steganography to provide a highly secure method of image and text transactions between the sender and the receiver. AES algorithm encrypts the secret image and LSB steganography hides the secret text. The secret image and text are hidden inside the cover image. It becomes difficult for the intruder to get access to the secret messages as the cover image sent is broken down into parts. Various applications of our proposed approach include financial services (banking), defence, detective agencies, hiding passwords and encryption keys and transporting highly private documents between international governments or within sectors.

CITATIONS

[1] Rahul Kumar, Ajit Pratap Singh, Arun Kumar Shukla, Rishabh Shukla "Enhancing Security using Image Processing" Sam Higginbottom Institute of Agriculture Technology and Sciences, Allahabad, India | International Journal of Innovative Research in Science, Engineering and Technology - Vol. 4, Issue 4, April 2015

[2] Jyotika Kapur, Akshay. J. Baregar "Security using image processing" K.J. Somaiya College of Engineering, Mumbai, India | International Journal of Managing Information Technology (IJMIT) - Vol. 5, No. 2, May 2013

[3] WIKI "Steganography"

[4] WIKI "Advanced Encryption Standard"

[5] WIKI "Cryptography"

[6] Roshni Padate, Aamna Patel "Image Encryption and Decryption using AES Algorithm" Fr. Conceicao Rodrigues College of Engineering, Mumbai, India | IJECT – Vol. 6, Issue 1, January (2015), pp. 23-29

[7] Champakamala B S, Padmini K, Radhika D K "Least Significant Bit algorithm for image steganography" Don Bosco Institute of Technology, Bangalore, India | International Journal of Advanced Computer Technology (IJACT)

[8] Nikon | Imaging Products | Still Images – Nikon D7100 "http://imaging.nikon.com/lineup/dslr/d7100/sample.htm"

[9] Credit Card – Citi Simplicity – citi.com "https://www.citi.com/credit-cards/credit-card-details/citi.action?ID=citi-simplicity-credit-card"

CONTRIBUTION OF EACH TEAM MEMBER

- **Hemkesh V Kumar**
  Coded the algorithm of image segmentation and recovery (and panoramic stitching which did not give expected results)
  Coded for the recovery of secret text from the stego image
- **Jeevan Nagaraj**
  Coded for embedding of secret image inside the cover image and for extracting the same
  Coded the embedding of secret text into the encrypted image
- **Manoj S Hegde**
  Developed the entire module of AES Encryption/Decryption

Each member of the team expressed himself, influenced the group's decisions and made strong contributions to the discussion at meetings and to the work of the group project.