Security using image processing

Jyotika Kapur

Student Of K.J. Somaiya College Of Engineering(Vidyavihar, Mumbai-76)
jyotikakapur18@gmail.com

Akshay. J. Baregar
(Assistant author)

Student Of K.J. Somaiya College Of Engineering (Vidyavihar, Mumbai-76)
baregar1611@gmail.com

Abstract

Using image stitching and image steganography security can be provided to any image which has to be sent over the network or transferred using any electronic mode. There is a message and a secret image that has to be sent. The secret image is divided into parts.The first phase is the Encrypting Phase, which deals with the process of converting the actual secret message into ciphertext using the AES algorithm. In the second phase which is the Embedding Phase, the cipher text is embedded into any part of the secret image that is to be sent. Third phase is the Hiding Phase, where steganography is performed on the output image of Embedding Phase and other parts of the image where the parts are camouflaged by another image using least significant bit replacement. These individual parts are sent to the concerned receiver. At the receivers end decryption of Hiding phase and Embedding Phase takes place respectively. The parts obtained are stitched together using k nearest method. Using SIFT features the quality of the image is improved.

Keywords

Cryptography, image steganography, image stitching.

1 Introduction

In today's world of growing technology security is of utmost concern. With the increase in cyber crime, providing only network security is not sufficient. Security provided to images like blue print of company projects , secret images of concern to the army or of company's interest, using image steganography and stitching is beneficial. As the text message is encrypted using AES algorithm and embedded in a part of the image the text message is difficult to find. More over since the secret image is broken down into parts and then sent to the receiver. This makes it difficult for the trespasers to get access to all the parts of the images at once. Thus increasing the security to a much needed higher level. This makes it becomes highly difficult for the the intruder to detect the and decode the document. There is no limitation on the image format that can be used right from bmp to a giff image can be used. It can be grey scale or coloured images.
The size of the message needs to be of only 140 characters.

2 Literature survey:

Current picture of the world says that everything that can be thought off can be done with the help of the internet. Right from shopping for clothes to buying a house. The transactions are all done using personal information, credit card numbers etc. With the amount of internet users hiking up

day by day , everything that is transmitted over the internet is under threat by some malicious mischief of another person. In order to provide security to the data that is being send across the system network security is not enough. With the growing technology the hackers have also kept themselves updated with technology and ways to hack it.

In order to provide security the only way would be not letting the hackers know about the presence of important information in your transaction.

Many techniques have been developed to do so like digital watermarking, visual cryptography were used before image steganography. Researchers have also developed techniques that embed data or another image within the image.

There are various methods for data hiding[4] like the spatial domain, frequency domain, compressed data domain.

In spatial domain: in this the image pixels in the spatial domain are arranged in order to incorporate the data to be embedded This technique is simple to implement. It offering a high hiding capacity. The quality of the image in which the data embedding is done can be easily controlled.

Frequency domain data hiding [2,5]: In this method images are first converted into frequency domain, and then data is embedding is done by modifying the transformed coefficients of the frequency domain.

Compressed domain data hiding [2,5]. Since the data is transmitted over the network is always in the compressed form. This information is used in for embedding the data in compressed domain where the compressed data coefficients are manipulated to embed data.

Next was visual cryptography in which encryption could be done as a mechanical operation without the use of any computer. Cryptography protects the contents of the message whereas steganography protects both messages and the communicating parties. This is a visual secret sharing scheme, where an image was broken up into n parts a person with access to all n shares could decrypt the image, while any n-1 shares revealed no information about the original image

The methods for automatic image alignment and stitching fall into two categories direct and feature based[1]

Direct methods have the advantage that they use all the image data and thus provide very accurate registration, but to its disadvantage they require a close initialisation.

Feature based registration on the other hand does not require initialisation, but traditional feature matching methods lack the invariance properties needed to enable reliable matching of arbitrary panoramic image sequence

Image stitching was done in the gradient domain using RANSAC parameters and linear blending. But it provided only 70-80% efficiency. So to improve the efficiency, invariant features were used like gain compensation, multi-blending etc. Also panoramic image stitching techniques have been implemented. Thus, by combining image steganography and image stitching algorithms, double security can be provided to any application.

Applications of the proposed system are

1. Banking
2. Consultancies

3. Detective agencies
4. Defence forces

3 Existing system

Various systems are available for information hiding in an image, but they have some drawbacks i.e., they either do not encrypt the message or use a very weak algorithm in order to perform cryptography. They use the same key for encryption and decryption making it easy for the intruder to get access of the ingormation. In some other cases the technique used may not be very efficient that is, the original image and the resulting image will be easily distinguishable by naked human eyes. For example DES algorithm, an encryption algorithm, used keys of smaller sizes (64 bit key) hence it was easy to decode it using computations. Algorithms using keys of these sizes are easily cracked by any intruder. So it is better if one goes for algorithms using keys of larger size which are difficult to decrypt and provide better security. Where stitching is concerned, multiband blending, gain compensation, automatic straightening makes the image smooth and more realistic.

4 Proposed System

The proposed system is divided into phases for better understanding. The phases are as follows Breaking an image of size w * h into n sub-images of size x * y can be done using blkproc function in matalb.

4.1 Encrypting Phase

The message to be sent is encrypted using AES algorithm. The steps involved in performing AES are as follows[6]

AES has three approved key length: 128 bits, 192 bits, and 256 bits. This algorithm starts with a random number, in which the key and data is encrypted , which are then scrambled though four rounds of mathematical processes. The key that is used to encrypt the message must also be used to decrypt it as shown in the figure 1

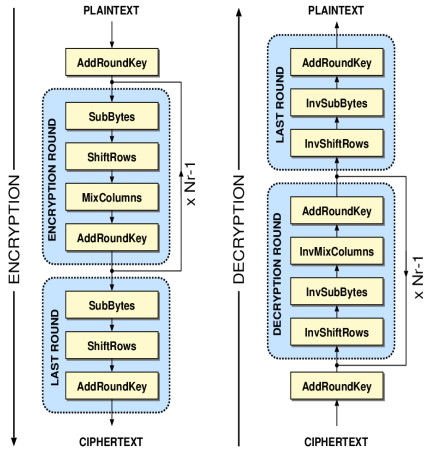


Figure 1 AES Algorithm

The four rounds are called

1. **Sub Bytes**,:- In this we rearrange the bytes of by using a lookup table which determines what each byte is replaced with.
2. **Shift Rows**:- The first row is left unchanged where as every other row is shifted cyclically by a particular offset, while. Each byte of the second row is shifted to the left, by an offset of one, bytes in the third row are shifted by an offset of two, and the fourth row by an offset of three. This is applied to all three key lengths, though there is a variance for the 256-bit block where the first row is unchanged, the second row offset by one, the third by three, and the fourth by four.
3. **Mix Columns:**- a mixing operation using an invertible linear transformation in order to combine the four bytes in each column. The four bytes are taken as input and generated as output.
4. **Add Round Key**:- a round key is derived from Rijndael's key schedule, and round key is added to each byte of the row. Each round key gets added by combining each byte of the row with the corresponding byte from the round key.

These steps are repeated again for a fifth round.

These algorithms essentially take basic data and change it into a ciphertext.

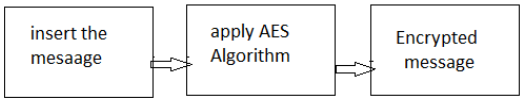


Figure2: Crypto Module

For Crypto Module the following steps are considered for encrypting the data (Refer **Figure2):**
 Insert text for encryption.
 Apply AES algorithm using 128 bit key (Key 1).
 Generate Cipher Text in hexadecimal form.

4.2 Embedding Phase

In this phase the encrypted message is embedded on to a part of the secret image
In this phase the cipher text that is given as input in the text editor is actually hidden in the cipher. Figure 4 shows the diagrammatic description.

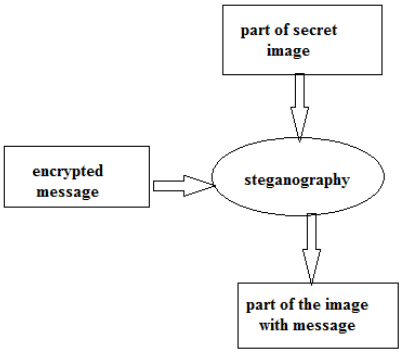


Figure 3: Embedding Phase

The LSB steganographic algorithm is used for hiding the cipher inside the image,. In this each bit of the cipher text (that has been converted

into its binary equivalent) is exchanged with the last bit of each pixel value. Similarly for each pixel the last bit is replaced with the consecutive bits of the cipher text i.e. its binary equivalent. Therefore four possibilities of swapping are

- A '0' replaced by a '0'
- A '0' replaced by a '1'
- A '1' replaced by a '0'
- A '1' replaced by a '1'

So in cases two and three, only the last bit is going to be changed. So the difference in the resulting pixel value is not going to show much difference. Hence the resulting image will resemble the original image. This technique of replacing the bits is called the LSB technique in steganography. The LSB technique together with the masking technique provides more security. Masking is nothing but replacing the bits in the pixel before, the binary equivalent of the character is binary ANDed with 254.

4.3 Hiding Phase

In this phase image steganography is performed. The technique used for image steganography is Kekre's Median Codebook Generation Algorithm (KNCG) [2] is explained as follows.
In this algorithm image is segmented into parts and these parts are converted into vectors of size k.

The Figure 4 below represents matrix T of size M x k. It consist of M number of image training vectors of dimension k. Each row of the matrix acts like the image training vector of dimension k.

$$T = \begin{pmatrix} x_{11} & x_{12} & \dots x_{1K} \\ x_{21} & x_{22} & \dots x_{2K} \\ x_{M1} & x_{M2} & \dots x_{MK} \end{pmatrix}$$

Figure 4: Training Matrix

The training vectors are arranged with respect to the first column of the matrix T shown in the figure 4 and the entire matrix is considered as one single cluster. Then choose the median of the matrix T and put it into the codebook, and set the size of the codebook to one. Split the matrix into two equal parts. Each of the part is then ordered again with respect to the second column of the matrix T . Now two clusters obtained, both consisting of exactly same number of training vectors. Calculated median of both the parts and write it to the codebook. Thus it consists of two code vectors. The parts again are partitioned to half . Each of the above four parts obtained are arranged with respect to the third column of the matrix T. In this way four clusters we obtain and in the same manner four codevectors are obtained. The above process is looped till we get the codebook of desired size. It is observed that Quick sort algorithm takes least time to generate the codebook and thus it is used. The diagrammatic representation of the hiding phase is shown in figure 5.

+

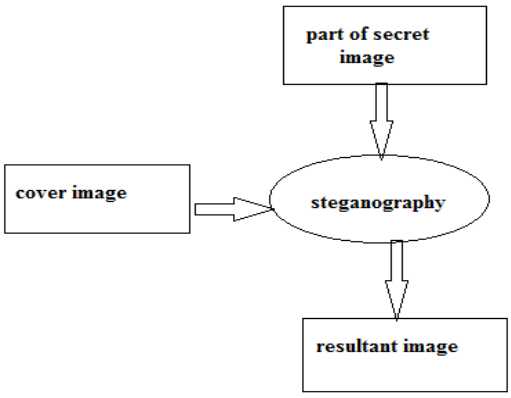


Figure 5 Hiding Phase

4.4 Stiching Phase

K-Nearest Neighbour or KNN algorithm is part of supervised learning, it is also a non parametric technique, which means that no assumption is made about the parameters in this algorithm..[1] the working is based on finding the minimum distance from the query instance to the training samples to determine the K-nearest neighbours to the query instance. After we find the k nearest neighbours simple majority of these K-nearest neighbours is taken to be the prediction of the query instance.

ü An arbitrary instance is represented by $(a_1(x), a_2(x), a_3(x),.., a_n(x))$
o $a_i(x)$ denotes features
ü Euclidean distance between two instances
$d(x_i, x_j)$=sqrt (sum for r=1 to n $(a_r(x_i) - a_r(x_j))^2$)

figure 7 shows the working of automatic panorama stitching algorithm

Algorithm: Automatic Panorama Stitching

- **Input:** n unordered images
- I. Extract SIFT features from all n images
- II. For each feature find nearest- k -neighbours using a k-d tree
- III. For each image:
- (i) Select m candidate matching images that have
- the most feature matches to this image
- (ii) Use RANSAC to find geometrically consistent feature matches to solve for the homography between pairs of images
- (iii) Using a probabilistic model verify image matches
- IV. Find connected components of image matches
- V. For each connected component:
- (i) Perform bundle adjustment to solve for the rotation
- _1, _2, _3 and focal length f of all cameras
- (ii) Render panorama using multi-band blending
- **Output:** Panoramic image(s)

5 RESULT AND EVALUATION

5.1 Result Evaluation For Kmcg

Figure 7 shows the results of avg mse versus hiding capacity for various codebook generation techniques by taking average of MSEs for 1 bit, 2 bits, 3 bits, 4 bits and variable bits using cover image[2,4,5]

Cover image message after applying kmcg

Figure 6 Working Of Kmcg

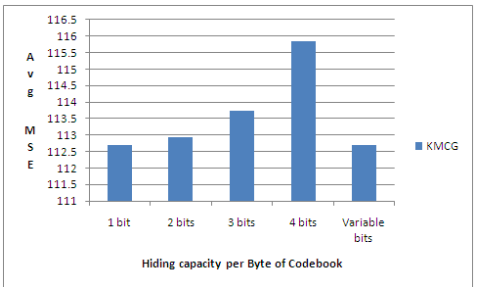


Figure 7: Plot of Hiding Capacity versus average MSE for various hiding methods 1bit, 2bits,3bits, 4bitsAnd Variable bits on KMCG.

5.2 Result evaluation of stitching :

Using Automatic Panorama Stitching algorithm two input images are stitched together using SIFT features. [1]

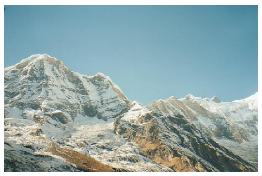
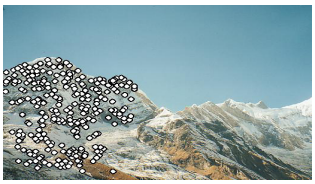


Image 1

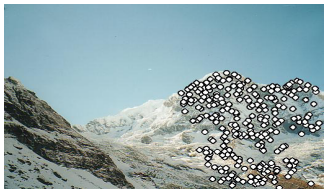
Image 2

SIFT matches 1

SIFT matches 2



RANSAC inliers 1



RANSAC inliers 2

Paranomic images

Figure 7 Automatic Panorama Stitching

6 Conclusion

This paper has presented a novel system for data and image encryption using AES algorithm for cryptography, image steganography and image stitching which can be used by banking, consultancies and detective agencies . It has put forth a new system which combines text cryptography and image Steganography which could be proven a highly secured method for data transactions in the near future.

As the image to be sent is broken down into parts and encrypted individually and sent over the network it becomes difficult of the intruder to get access of all the parts. Additionally since every part is camouflaged by a cover image, the encrypted image looks like just another regular image. Thus fooling the intruder.

With the help of invariant local features and a probabilistic model for image matching purpose in image stitching, allows us to recognise multiple panoramas in unordered image sets, and stitch them fully automatically without user input. With the help of SIFT features and RANSAC algorithm the output of the image is rectified and we get a smooth image. This image can also be used as a password to open a document of a file.

7 Reference

[1] ”Automatic Panoramic Image Stitching using Invariant Features”, Matthew Brown and David G. Lowe of Computer Science,University of British Columbia,Vancouver, Canada.

[2] ”High payload using mixed codebooks of Vector Quantization”, H. B. Kekre, Tanuja K. Sarode, ArchanaAthawale, KalpanaSagvekar

[3] ”Steganography Using Dictionary Sort on Vector Quantized Codebook”,Dr. H.B. Kekre, ArchanaAthawale, TanujaSarode, SudeepThepade&KalpanaSagvekar International Journal of Computer Science and Security (IJCSS), Volume (4): Issue (4) 392

[4] ”H.B.Kekre,ArchanaAthawale and Pallavi N.Halarnkar,”Polynomial Transformation to improve Capacity of Cover Image For Information Hiding in Multiple LSBs”,International Journal of Engineering Research and Industrial Applications(IJERIA),Ascent Publications,Volume 2,March 2009,Pune.

[5] ”H.B.Kekre,ArchanaAthawale and Pallavi N.Halarnkar,”Performance Evaluation of Pixel Value Differencing and Kekre’s Modified Algorithm for Image Hiding in Images”,ACM International Conference on Advances in Computing,Communication and Control(ICAC3)2009.

[6] ’Proposed System for data hiding using Cryptography and Steganography *Dipti Kapoor Sarmah1, Neha Bajpai2 1Department of Computer Engineering, Maharashtra Academy of Engineering,Pune, INDIA 2Department of Information Technology, Center of Development of advance computing,Noida, INDIA

AUTHORS

JYOTIKA KAPUR studying in KJ Somaiya College Of Engineering specializing in computers

AKSHAY BAREGAR studying in KJ Somaiya College Of Engineering specializing in computers.

.