ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

Enhancing Security using Image Processing

Rahul Kumar[1], Ajit Pratap Singh[2], Arun Kumar Shukla[3], Rishabh Shukla[4]

M.Tech student, Sam Higginbottom Institute of Agriculture Technology and Sciences, Allahabad, India[1,2,4].

Asst.Professor, Sam Higginbottom Institute of Agriculture Technology and Sciences, Allahabad, India[3].

ABSTRACT: Image which has to be sent over the network or transferred using any electronic mode can be secured by the use of image steganography and stitching. There is a secret image and message that has to be sent over the network. The secret image is divided into two phases. The first phase is the Encryption phase, which deals with the process of transforming the plain text (actual secret message) into cipher text using the AES algorithm. The Second phase is the Embedding phase, which deals with the process of embedding the cipher text into any part of secret image that is to be sent. The third phase is the hiding phase, which deals with performing steganography on the output of Embedding Phase. Hiding Phase and Embedding Phase get decrypted at the receiving end. K-Nearest method is used to stitch the parts obtained.

KEYWORDS: Cryptography, image steganography, image stitching.

I. INTRODUCTION

In present time security is major concern while transmitting any message over a network. Network security is not sufficient as cyber crime is increasing therefore other method is used for providing security. Security provided to image using image steganography and stitching is beneficial.AES algorithm is used to encrypt text message and embedded in a part of the image the text message is difficult to find. Image is divided into parts and then sent to the receiver. This makes it difficult to get access to all the parts of the image at once therefore it become highly difficult for the intruder to decode the document. There is no limitation on the image format that can be used. The image can be gray scale or colored but the size of the message needs to be of only 140 characters.

II. LITERATURE SURVEY

In today's world the use of E-Commerce is on the hike. Right from shopping for mobiles to buying a car and house. These transactions are all done using private information like: credit card number, password etc. Internet users are growing up day to day therefore the data transmitted over the internet is under threat. Security must be provided to the data that is being sent over the network. As with emerging technology the hacker also kept themselves updated with technology and ways to hack it. In order to provide security there is only a way to hide personal information from the hackers. Many techniques have been developed like digital watermarking, visual cryptography:

A forensic watermark, also called a digital watermark, is a sequence of characters or code embedded in a digital document, image, video or computer program to uniquely identify its originator and authorized user. Forensic watermarks can be repeated at random locations within the content to make them difficult to detect and remove.

Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. The technique was proposed by Naor and Shamir in 1994. Visual Cryptography uses two transparent images. One image contains random pixels and the other image contains the secret information. It is impossible to retrieve the secret information from one of the images. Both transparent images and layers are required to reveal the information

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

The above techniques have been developed before image steganography. Researchers have also developed techniques that embed data or another image within the image. There are various method used for data hiding [4] like frequency domain, spatial domain compressed data domain. In spatial domain, we deal with images as it is. The values of the pixels of the image change with respect to scene. Whereas in frequency domain, we deal with the rate at which the pixel values are changing in spatial domain. In other word image pixel in the spatial domain are arranged in order to incorporate the data to be embedded.

Frequency domain data hiding [2, 5]: In this method images are first transformed 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.
Cryptography provides security for the message transmitted over the network whereas steganography protects both message and the communicating parties. In this images is broken into n parts a person with access to all n shares could only decrypt the image, while any n-1 shares revealed no information about the original image.
Image stitching is the process of combining multiple photographic images with overlapping fields of view to produce a segmented panorama or high-resolution image. Image stitching is done in the gradient domain using linear blending and RANSAC parameter but this provides only 70-80% efficiency. Thus, by using image steganography and image stitching algorithm together double security can be provided to any application.

Applications of the proposed system are:
1. Financial Services (Banking)
2. Defence
3. Detective agencies
4. Government sectors

III. EXISTING SYSTEM

There are various methods for information hiding in an image but there are some drawbacks like they either do not encrypt the message or use a weak algorithm in order to perform cryptography. The use of same key for encryption and decryption make it easy for the intruder to find the information. There are other cases the technique used may not be very efficient that is, the original image and the resulting image will be distinguishable by naked human eyes. For example DES algorithm: It operates on block of 64bits using a secret key that is 56bits long hence it is easy to decode it using computation. Algorithm using key of these size are easily decode by an intruder therefore it is better if one goes for algorithm using key of longer size which are difficult to decrypt and hence provide better security.

IV. PROPOSED SYSTEM

The proposed system is broken down into phases. The phases are as follows Breaking an image of size Q*R into n sub-images of size X*Y can be done using blkproc function in matalb.

4.1Encrypting Phases

AES algorithm is used to encrypt the message. The steps involved in performing AES are as follows[6]
The AES has three fixed 128-bit block ciphers with cryptographic key sizes of 128 bits, 192 bits and 256 bits. Key size is unlimited, whereas the block size maximum is 256 bits. Advance Encryption Standard is a symmetric cipher uses an algorithm that starts with a random number, in which both the key and data are encrypted and then are scrambled through four rounds of mathematical processes and the key that is used to encrypt the message must also be used to decrypt as shown in the figure 1.The AES algorithm organizes the data block in a four-row and row-major ordered matrix. In both encryption and decryption, the AES uses a round function.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

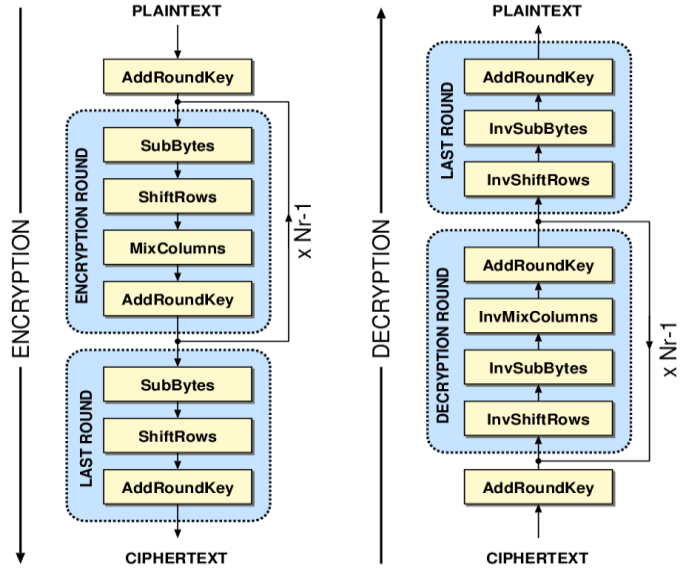
International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

The four rounds are called:

1. Sub Bytes: a non linear substitution step where each byte is replaced with another according to a lookup table.
2. Shift Rows: a transposition step where each row of the state is shifted cyclically a certain number of steps.
3. Mix column: a mixing operation which operates on the columns of the state, combining the four bytes in each column.
4. Add Round key: each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule.



These steps are repeated again for a fifth round.
These algorithms essentially take basic data and change it into a cipher text.

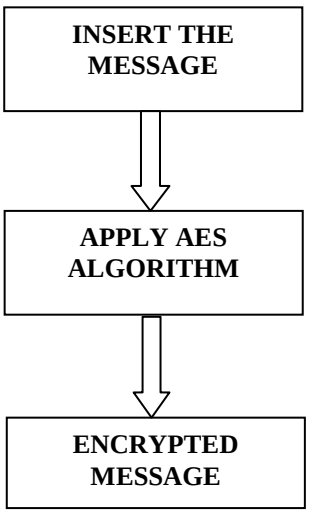


Figure 2: Crypto Module

For Crypto Module the following steps are followed for encrypting the data (Refer Figure 2):

1. Insert text for Encryption.
2. Apply AES algorithm using 128bit key.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

3. Generate Cipher Text (Hexadecimal form).

4.2 Embedding Phase

In Embedding phase the encrypted message is embedded on to a part of the secret image therefore cipher text that is given as input in the text editor is hidden in the cipher. Hiding cipher text inside the image is done using LSB Steganographic algorithm. In this each bit of the cipher text is exchanged with last bit of each pixel Value. For each Pixel the last bit is replaced with the consecutive bits of the cipher text 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'

The last bit is going to be changed in case 2 and 3 therefore the difference in the resulting pixel value is not going to show much difference and hence the resulting image will resemble the original image. This technique of replacing the bits is called LSB technique in steganography. The use of masking technique along with LSB for provides more security.

4.3 Hiding Phase

Image steganography is performed in this phase. Kekre's Median Codebook Generation Algorithm (KNCG) [2] is used for image steganography. KNCG is fastest as compared to other codebook generation algorithms. Using this algorithm image is segmented into parts and these parts are converted into vectors of size K. The Figure 4 below represent matrix T of size M*k consisting of M number of image training vectors of dimension k. Each row of the matrix is the image training vector of dimension k.

$$T = \begin{bmatrix} x_{1,1} & x_{1,2} & \cdots & x_{1,k} \\ x_{2,1} & x_{2,2} & \cdots & x_{2,k} \\ . & . & . & . \\ . & . & . & . \\ x_{M,1} & x_{M,2} & \cdots & x_{M,k} \end{bmatrix}$$

Steps for KMCG Algorithm:

1. Image is divided into the windows of size 2x2 pixels (each pixel consisting of red, green and blue components).

2. These are put in a row to get 12 values per vector. Collection of these vectors is a training set.

3. The training set is sorted with respect to first column. The Median of the first column is used to divide the training set in two parts and the median vector is put in the codebook. Set the codebook size equal to 1.

4. Further each part is then separately sorted with respect to second column to get two median values and these two median vectors are put into the codebook. Set the codebook size equal to 2.

5. The process of sorting is repeated till codebook of desire size is obtained.

Here quick sort algorithm is used. This algorithm takes least time to generate codebook and thus it is used. The diagrammatic representation of the hiding phase is shown in Figure 5.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

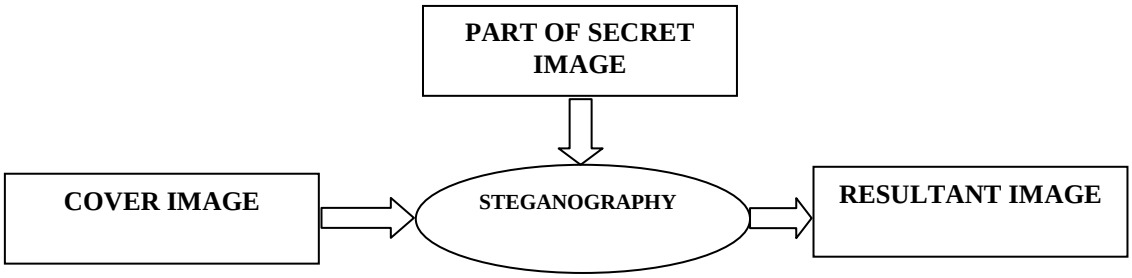


Figure 5 Hiding Phases

4.4 Stitching Phase

K-Nearest Neighbour or KNN algorithm is a supervised learning algorithm which is used for classifying object based on the closest training example in the feature space.KNN algorithm, it is also a non parametric technique which means that no assumption is made about that parameter in this algorithm.[1].The working of this algorithm is based on minimum distance from the query instance to the training sample to determining K-Nearest neighbour. After we find the K-Nearest neighbours then simple majority of these K-Nearest neighbours is taken to be the prediction of the query instance.

ü An arbitrary instance is represented by $(a_1(x), a_2(x), a_3(x), \ldots\ldots, a_n(x))$ where $(a_i(x)$ denotes features

ü Euclidean distance between two instances

d(x_i , (x_j)=sqrt (sum for r=1 to n $(a_r(x_i) - a_r(x_j))^2$)

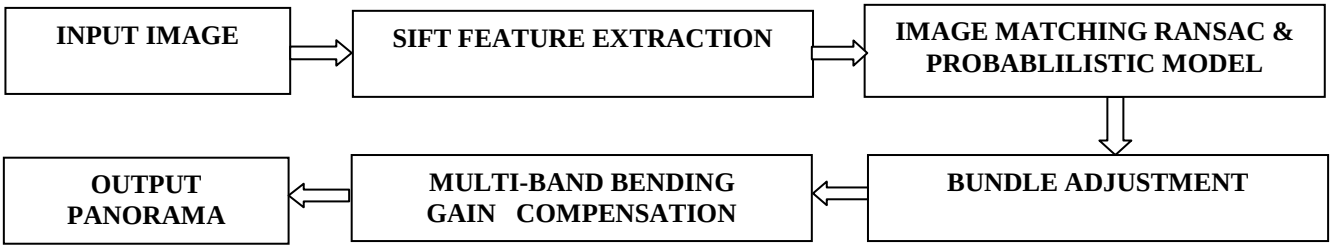


Figure 5.1

From Figure5.1 In image processing, the feature point also called key point. It is the basic concept of image processing, which is used in many technique like object recognition, image registration and corner detection. SIFT is the widely accepted and used method to detect feature points and detect the corner from the input image. After we have information of feature matching of all pictures, we can use this useful information to do image matching. In image matching step, we are going to find out which picture is neighbour of another picture, and find the correctly feature matching set we need for next step of all feature matching set.

RANSAC (RANdom Sample Cosensus) is non-deterministic algorithm estimates parameter of a mathematical model from a set of observed data which contain outliner iteratively. We show the step of RANSAC in detail as follows:

RANSAC loop:

1. Select four feature pairs (at random)
2. Compute homography H (exact)
3. Compute *inliers* where $SSD(p_i', \boldsymbol{H}\, p_{i)} < \varepsilon$
4. Keep largest set of inliers
5. Re-compute least-squares H estimate on all of the inliers

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

Algorithm: Automatic Panorama Stitching
Input: N unordered images

1. Extract SIFT features from all n images
2. Find k nearest-neighbours for each feature using a k-d tree
3. For each image:
   A. Select candidate matching images that have the most feature matches to this image
   B. Use RANSAC to find geometrically consistent feature matches to solve for the homography between pairs of images
   C. Verify image matches using a probabilistic model
4. Find connected components of image matches
5. For each connected component:
   A. Perform bundle adjustment to solve for the rotation _1,_2,_3 and focal length f of all cameras
   B. Render panorama using multi-band blending

Output: Panoramic image(s)
Figure 7 shows the working of automatic panorama stitching algorithm

V. RESULTS AND EVALUATION

5.1 Result evaluation for KMCG

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] is shown in Figure 7

Cover image

Message

after applying KMCG

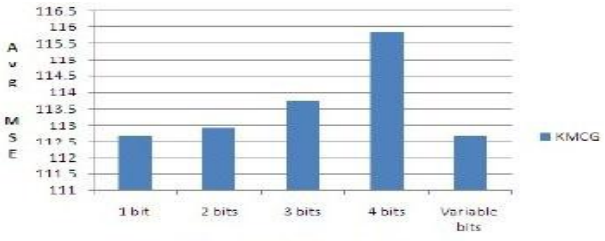


Figure: 7

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

5.1 Result evaluation of stitching

The Two input image are stitched together using SIFT features by automatic panorama algorithm.[1]

Figure (a): IMAGE 1

Fig(b): IMAGE 2

Fig(c)SIFT MATCHES 1

Fig(d): SIFT MATCHES 2

Fig(e):RANSAC INLIERS 1

Fig(f): RANSAC INLIERS 2

Fig 7: PARANOMIC IMAGE

Fig (a) and Fig (b) shows input images which are used to stitch each other for the Panorama output purpose. Fig (c) and Fig (d) shows the output of SIFT which indicates the feature points in the images. Then we apply RANSAC method which differentiates the inliers and outlier, Fig (e) and Fig (f) shows the output for RANSAC.Figure 7 Automatic Panorama Stitching

VI. CONCLUSIONS

The paper has given an idea of creating a new system which combine cryptography and image steganography which is a secured method for data transaction over an unreliable network. In this system data and image encryption are done using AES algorithm for cryptography, image steganography that can be widely used in defence and financial services.
The image which is to be send over an unreliable network are divided into parts and encrypted individually and sent over the network it become difficult for the intruder to decode all the parts of the images. Every parts of the image I camouflaged by a cover image therefore the encrypted image look same as another regular image .This help in fooling the intruder.
We can recognize multiple panoramas in unordered image sets and stitch them automatically without user input by the help of invariant local features and a probabilistic model. The output of the image is rectified and we get a smooth image.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

REFERENCES

[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.