Secured Image Transmission using Hybrid Approach with Compression

Prachi Raviraj Mendhekar, Pramod Borole

Department of Electrical Engineering

Veermata Jijabai Technological Institute, Mumbai

Abstract— Now-a-days secured communication is very essential as all communications are possibly done over the internet. So we need to Trans-receive more confidential data with the more security. To provide more security we encrypt our secret image and hide encrypted image into target image so it will provide more security. And by compressing we can we can reduce the image size so it will become easy to transmit secured image over the network. In this paper by using the improved LSB technique encrypted message can be hidded into the target image. The encryption of the secret image is done by using steam cipher. So by using the hybrid combination of cryptography and steganography we provide security to our image transmission. Compression is done by using hybrid approach of DCT and DWT algorithm.

Key words: The PSNR (Peak Signal To Noise Ratio), MSE (Mean Square Error) Calculation Are Performed

I. INTRODUCTION

On internet multimedia data is more used, so before transmitting data it is desire to secure it. When sender transmits the data to the receiver, there may be intruder between them. So he can capture the data, view it and may alter it. This type of distortion is not acceptable for the military, medical purposes. For that we secure our data by convert it into another form so no one can understand what the exact message is. But by using statistic test and crypt-analyses test intruder can detect the data and capture the data. To provide more security with hiding the message we hide existence of message i.e. invisible communication called steganography. Combination of cryptography and steganography increases each other strength.

Several researchers worked in the respective field like Manu Devi and Nidhi Sharma et al. (2014) in paper “Im proved Detection of Least Significant Bit Steganography Algorithms in Color and Gray Scale Images” have describe the image security by using Improved LSB based steganography technique i.e.1-3-4 LSB algorithm, so that human eye cannot predict and detect the existence of any secret data inside the target image. This shows the better embedding payload capacity of 1-3-4 LSB algorithm over simple LSB technique.

E. Elharar, Adrian Stern, Ofer Hadar, “A Hybrid Compression Method for Integral Images Using Discrete Wavelet Transform and Discrete Cosine Transform”. In this paper proposed systems experimental results shows better compression ratio, less MSE and high PSNR can be obtained using hybrid combination than the standalone JPEG based DCT and DWT transform.

Belmeguenai Aissa, Deruiche Nadir Mansouri khaled (2012) “Security Analysis of Image Cryptography using Stream cipher Algorithm with nonlinear filtering function “. In this paper new encryption algorithm introduced by which more security is possible by using stream cipher encryption algorithm with nonlinear filtering function. And for satisfy-ing cryptography criteria Boolean function used. Experi-mental results show highly key sensitivity, good resistance again brute force, Berlekamp-Massey Attack and algebraic attack [3].

Alok Kumar Singh, G.S. Tripathi (2014), “A Comparative Study Of DCT, DWT & Hybrid(DCT-DWT) Transform”, proposed comparative study of three transform systems namely as DCT (Discrete cosine transform), DWT (Discrete wavelet transform) and hybrid DCT and DWT transform. Results show better performance of hybrid DCT and DWT transform in terms of peak signal to noise ratio (PSNR), MSE and compression ratio [5].

II. CRYPTOGRAPHY

In cryptography by keeping the message confidential security can be provided. By replacing original message into other for, so that no one can understand the exact original message. For the encryption, key is needed which is use at the time of decryption. At the encryption side plaintext and key gives cipher text.

There are two types of keys [2]: Public key cryptography and secret key cryptography

In secret key cryptography sender and receiver have same keys and it also private. If one of them key is exposed then it breaks security. So it is necessary to keep the keys very protective.

Secret key cryptography divided into block cipher and stream cipher.

In this paper stream cipher algorithm is used to encrypt the image. Stream cipher encrypt bit stream with unit of bit or bytes.

A. Stream Cipher Algorithm:

Stream cipher breaks message M into successive char-acters or bits m1, m2, m3… and encrypt each bit of M with elements of key stream i.e. k1, k2, k3… etc.

The key stream used for XORing with plaintext and results will be used to do encryption [12].

For encryption,
P: Plain text
Q: Secret bit stream
R is result of P&Q

B. Encryption Steps:

R=P X-OR Q
To decrypt encrypted data steps:
R X-OR Q=(PX-OR Q) X-OR Q=P X-OR (Q X-OR Q) = P X-OR 0=P
So, P= R X-OR Q.
III. STEGANOGRAPHY

Hidden communication is also called Steganography. In this data can hide in carriers which forms stego image so that eavesdropper not able to read the secrete data. The carriers can be audio, sound, video, text. In this way existence of message is not readable to attackers and secrete data can transmit to receiver side [6]. Digital image or painting etc. are the carrier image used for data hiding. There are many techniques used for the data hiding. In this paper we used approach of hiding image with secret message inside the target image. So that target image should be large so that image as well as secret message can be hiding inside it. To retrieve the hidden data by the intended recipient who knows the extracting algorithm to decode the stego image.

Properties of steganography are mode data hiding capacity and unidentified secret data. Here we proposed the technique more of the secret data to be hidden inside the target image with more capacity and security. After encrypt the secret image with the message it will hide into the target image by using the improved LSB algorithm. In this algorithm secrete image is hides inside the least significant bits of blue color of target image so that it gives less distortion and more efficiency. This algorithm works in spatial domain.[12]

- Steps for Improved LSB Algorithm:
  1) Selection of cover image
  2) Secret information should be embedded only in blue color component.
  3) By using pixel selection method find best area of cover image where to hide the secrete image.
  4) Use Bit replacement method.

Fig. 1: Improved LSB Algorithm

IV. COMPRESSION

With the growth of technology into the Digital Age, the world has found itself amid a vast amount of secret information. There are many difficulties while dealing with such enormous information. Image compression is minimizing the size in bytes of information file without degrading the quality of the image to an unacceptable level. The reduction in file size allows minimum storage space and reduces the time required for images to be sent over the Internet or downloaded from Web pages.

For efficient transmission and storage of images compression is required. There are two types of image compression:

A. Lossless versus Lossy compression:

In lossless compression, after compression, the reconstructed image is numerically identical to the original image. However lossless compression can only achieve a modest amount of compression. Lossless compression is preferred for medical imaging, military imaging, technical drawings, clip art or comics. An image reconstructed after lossy compression contains degradation relative to the original. Often this is because the compression discards more redundancy. However, lossy schemes are capable of achieving much higher compression but less image quality.[13]

B. DCT (Discrete Cosine Transform)

JPEG is primarily a lossy method of compression. JPEG discard information that the human eye cannot easily see. Slight changes in color are not perceived well by the human eye, while slight changes in intensity (light and dark) make difference.[13]

DCT separates images into parts of different frequencies. During compression less important frequencies are discarded through quantization and during decompression important frequencies are used to retrieve the image.

C. Advantage of DCT: [4]

1) It has the ability to pack most information in fewest coefficients
2) It minimizes the block like appearance called blocking artifact that results when boundaries between sub-images become visible.

2D_DCT transformation is given by the following equation:

\[ c(u,v) = D(u)D(v) \sum_{x=-1}^{N-1} \sum_{y=-1}^{N-1} f(x,y) \cos[(2x + 1)u\pi/2N] \cos[(2y + 1)v\pi/2N] \] (1)

D. DWT (Discrete Wavelet Transform):

\[ x[n] * h[n] = \sum_{k=-\infty}^{\infty} x[k] \cdot h[n - k] \] (2)

A half band low pass filter removes all frequencies that are above half of the highest frequency in the tile signal. Then the signal is passed through high pass filter.[4]

On comparing, DCT gives more compression ratio but less image quality and DWT gives good image quality but processing power is more. Hence hybrid combination of DCT and DWT gives better result than standalone DCT and DWT.

E. Mean Square Error (MSE) [13,5]:

MSE define as the average of the square of the difference between the desired response and the actual system output.

\[ MSE = \frac{1}{MN} \sum_{x=1}^{M} \sum_{y=1}^{N} [I(x,y) - I'(x,y)]^2 \] (3)

Where I(x,y) is the original image, I'(x,y) is the approximat-ed version.
Secured Image Transmission using Hybrid Approach with Compression

F. Peak Signal-To-Noise Ratio (PSNR):
It is the ratio between the maximum possible power of a signal and the power of corrupting noise. To measure of quality of reconstruction in image compression PSNR is used.

$$\text{PSNR} = 20 \times \log_{10} \left( \frac{255}{\sqrt{\text{MSE}}} \right)$$

V. PROPOSED METHODOLOGY
In this proposed paper secrete information is text and image and target image is also an image.
In embedding phase
1) Take secrete image
2) Stego image generation using stego secrete image
3) Image encryption
4) Stego image generation using target image
5) Compression
In data extracting phase, By applying reverse techniques original data can be recov-ered.

VI. EXPERIMENTAL RESULTS
Proposed work implemented Using Matlab R2013a and experimental results shown below.
Figure 4 shows the secrete image and stego secrete im-age. Where stego secrete image hided into the secrete image.

Fig. 4: Selection Of Secrete and Stego Secrete Image
After generation of stego image it encrypted using key.

Fig. 5: Encrypted Stego Image
This encrypted image now hided inside another image called stego image for more security. Now compress this stego image and send to decoder side.

Fig. 6: Compression of another Stego Image
At the receiver side decompress the compress image and by applying reverse algorithm original image can be recovered.

Fig. 7: Decompress and Original Recovered Image
Secured Image Transmission using Hybrid Approach with Compression (IJSRD/Vol. 3/Issue 04/2015/471)

<table>
<thead>
<tr>
<th>Sr. no.</th>
<th>Secrete image</th>
<th>Target image</th>
<th>PSNR</th>
<th>MSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Baboon</td>
<td>Chrysanthemum (JPG)</td>
<td>53.8448</td>
<td>30.824</td>
</tr>
<tr>
<td>2.</td>
<td>Barbara</td>
<td>Cmp (BMP)</td>
<td>56.0047</td>
<td>30.6513</td>
</tr>
<tr>
<td>3.</td>
<td>House</td>
<td>Colored chips (PNG)</td>
<td>44.3436</td>
<td>31.7412</td>
</tr>
</tbody>
</table>

Table 1: PSNR and MSE for Different Image File Format

VII. CONCLUSION

In this paper the hybrid approach of Steganography and cryptography for image security has been presented. Image steganography is done by using Improved LSB algorithm that provides better performance than simple LSB. Encryption is done by using stream cipher. And for compression hybrid approach of DCT & DWT is used which are better than the standalone DCT & DWT transforms. Recovery of original image without significant loss. To check the effectiveness of proposed system simulation results are shown and analyzed.

REFERENCES


