International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161
©2014 INPRESSCO®, All Rights Reserved
Available at http://inpressco.com/category/ijcet

Research Article

A Hybrid Approach for Secure Data Communication using Reversible Data Hiding and Image Encryption

Sowmyashree[Ȧ*] and R.R.Sedamkar[Ȧ]

[Ȧ]Computer Engineering Department, Thakur College of Engineering and Technology, University of Mumbai, India

Accepted 16 Nov 2014, Available online 20 Dec 2014, **Vol.4, No.6 (Dec 2014)**

Abstract

The present scenarios of sending confidential information over the network are not considered to be very secure. During transmission they are vulnerable to many kinds of security integrity attacks. In this paper, a unique approach for secure data communication is proposed which is a combination of Reversible Data Hiding and Image Encryption techniques. In this approach confidential data is embedded in the image and image is encrypted before transmission. At the receiver end, image is decrypted and hidden data is extracted and original image is recovered. By doing this more security could be provided to the transmission of confidential data. By using more enhanced Algorithms for Reversible Data Hiding and Encryption it will be difficult for an intruder to access the secret data. Most of the work emphases on data hiding in encrypted images whereas, here focus is on data hiding in images and then providing security by means of image encryption. Reversible data hiding helps in preserving the quality of the image after data extraction. A block pixel frequency based histogram shifting algorithm is used for data embedding. This algorithm embeds good payload of data preserving high quality of the image. Hash Image Encryption Algorithm is used to encrypt the stego-image which gives lower correlation and higher entropy indicating high level of security. Many state of art data security and data hiding algorithms have been developed for secure data communication but lacking in security and integrity with modern challenges which we have overcome here with combine approach of data hiding and image encryption. The proposed method improves security and integrity of sensitive data.

Keywords: *Reversible data hiding, Image encryption, stego-image, image Entropy, Correlation, Histogram Analysis*

1. Introduction

Digital media like image, audio and video are used to transfer confidential information during communication. Reversible data hiding technique can be used to hide confidential data in the image preserving image quality after extraction of secret data from the image. This technique helps to keep the presence of data secret. An image having secret data can be protected against security and integrity attacks by applying image encryption. Many works have been developed on reversible data hiding and Image encryption for securing the data which is travelling across the network.

1.1 Reversible Data Hiding

Reversible data hiding algorithm, can reform the original image without any distortion or loss from the marked image after the extraction of embedded data. The reversible data hiding technique is classified as embedding in the spatial domain or in the frequency domain. Embedding secret data in the spatial domain can be studied by using Difference Expansion (J. Tian, 2003) Histogram (E. Varsaki *et al* 2007; Che-Wei Lee *et al*, 2010) and Vector Quantization (Chin-Chen Chang *et al*, 2006) etc. While embedding data in the frequency domain is learned using Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT) (K. Ramandeep, 2012) In general, embedding in spatial domain results in higher payload hiding capacity and embedding in frequency domain results in more robustness. Reversible data hiding is needed in some applications where even any degradation of the original cover is not acceptable, such as military, medical and law forensics. Many reversible data hiding techniques have been developed so far.

Z. Ni. et. al (Z. Ni *et al* 2006) proposed a novel method for reversible data hiding. This algorithm can recover the original image from the marked image after extraction of hidden data. Histogram of original image is generated. This algorithm makes use of the peak points and zero points of the image histogram and performs modification of the pixel grayscale values to embed the secret data into the image. After generating the histogram of original image, the peak and zero (minimum) points will be found out. Then the whole image is scanned in a serial order. The grayscale values by 1 which is equivalent to shifting the range of histogram towards right hand side by one unit. PSNR higher than 48 dB can be achieved and it has low

*Corresponding author **Sowmyashree** is a M.E. Student and **Dr. R.R.Sedamkar** is working as Professor & Dean (Academics) computational complexity and short execution time. The drawback of this algorithm is the frequency of peak-pixel value in the histogram are limited. Therefore capacity to hide data is limited.

H.L.Yeh (H. L. Yeh, 2007) proposed Prediction-Based Reversible Data Hiding. This algorithm is to make the predictive coding of the original image pixel value by histogram. This method has high capacity and distortions are quite invisible and always offer a constant PSNR 48.0dB. But prediction error values are limited and frequency of prediction errors is limited.

Kuo *et al*. (Kuo *et al*,2008) presented a reversible data hiding technique which is based on the block division to hide the data in the image. Original image is divided into many equal blocks and then the histogram is generated for each of these blocks. Maximum and minimum points of histogram are calculated and histogram shifting method used to embed the data.

Ching *et al* (Ching *et.al*, 2011) Proposed high capacity reversible data hiding based on pixel frequency of blocks. This method divides the image into 3×3 sized blocks. Frequency of pixels in each block is explored and used as predictive values. Because the neighbouring pixels of blocks have the similar characteristics and the differences of prediction pixels are approximately. Thus, the peak values of prediction difference histogram are increased greatly, and the embedding capacity can be effectively enlarged on the cover image. As a result, the stego-image not only has good PSNR values of image quality, but also has reversible characteristics for data hiding. But I this approach it is not specified how to choose pixel with maximum frequency when two or more pixels are having same frequency value which is maximum. So the proposed work explores an appropriate calculation (Sowmyashree *et al*, 2014) of maximum frequency pixel value with inverse scanning order (R. Rajkumar *et al*, 2012) of the image. This method significantly improves PSNR values for high payload data.

1.2 Image Encryption

Encryption is a technique to convert original data into unreadable form. Encryption techniques ensure that the information being transmitted are not prone to unauthorized access and has not been modified during the transmission. Images are widely used in the current digital world for different purposes. In order to guarantee protection of images against eavesdroppers during transmission images can be encrypted before transmission. Only intended user can decrypt the image using the key. Image encryption has an evident role in the field of information hiding by providing second level security to hidden data in the image. The values of neighboring pixels are strongly correlated in natural images. Encryption breaks this correlation increasing entropy values (Alireza *et al*, 2010). Numerous chaotic and non-chaotic algorithms for image encryption have been developed since decades.

Xiaojun Tong *et al* (Xiaojun *et al*, 2007) Image Encryption with compound chaotic sequence cipher shifting dynamically. It uses the new compound chaotic function by choosing one of the two one-dimensional chaotic functions randomly. The scheme is not sensitive to the changes of plain images. Does not work as good random number source.

Zhang (Y. Zhang, 2009) proposed an algorithm of Fractional Fourier Transform and application in digital image encryption where the fractional Fourier transform (FrFT) is applied to an image encryption and decryption. The encrypted digital image can be decrypted by someone who attempts parameter; he may get the correct decrypted image.

Mohammad Ali et. al (Mohammad Ali et. Al, 2007) proposed a non-chaotic Image Encryption Using Block-Based Transformation Algorithm. This is a combination of image transformation and a well-known encryption-decryption algorithm called Blowfish, which resulted in lower correlation and higher entropy.

A new permutation based image encryption algorithm was proposed by Hiral Rathod *et al* (Hiral Rathod *et al*, 2011) which uses combination of permutation and Hyper image encryption algorithm promising high entropy and low CPU and memory utilization. Our proposed work makes use of Hyper Image Encryption (SHA-1) algorithm for Hybrid approach of Reversible Data Hiding and Image Encryption.

2. Proposed Work

Even though reversible data hiding technique keeps the existence of data secret, the data embedded may be easily damaged by any alteration of the stego-image (E. Varsaki *et al* 2007). In this case, encryption can play an important role. We propose a hybrid approach based on data hiding and image encryption for protecting stego image against security attacks.

The proposed Hybrid Approach for Secure Data Communication using data hiding and Image Encryption is based on two technologies.

- Reversible Data Hiding
- Hyper (Hash) Image Cryptography

The proposed Reversible Data Hiding is a modification of high capacity reversible data hiding algorithm which is based on pixel frequency of blocks (Ching-Te Wang *et al*, 2011) The algorithm makes use of frequency of pixels in each 4×4 sized blocks of image to form prediction difference image. In each block, the pixel with maximum appearance frequency is considered as mode value which is used to generate prediction difference image. But there are some blocks where two or more pixels are having same maximum frequency. Our approach proposes an appropriate calculation for choosing pixel with maximum frequency when two or more pixels are having same maximum frequency value. It results in good PSNR values indicating high image quality. A non-chaotic Hyper Image encryption algorithm (Hiral Rathod *et al*, 2011) is used for encryption of the stego image which results in high entropy. Entire work consists of two parts: Sender (Part A) and Receiver (Part B)

Part A consists of

- Reversible Data Hiding(RDH)
- Hash Image Encryption

Part B consists of

- Hash Image Decryption
- Secret Data extraction and Restoration using RDH algorithm

Figure 2.1 and 2.2 shows Part A and Part B of Proposed Hybrid approach.

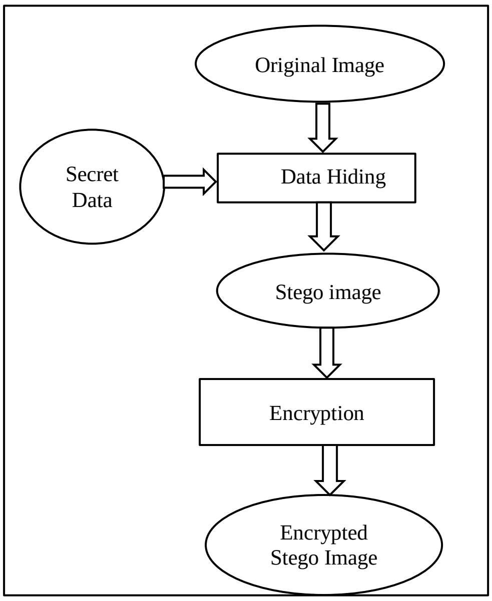


Fig.2.1 Proposed Approach (Part A)

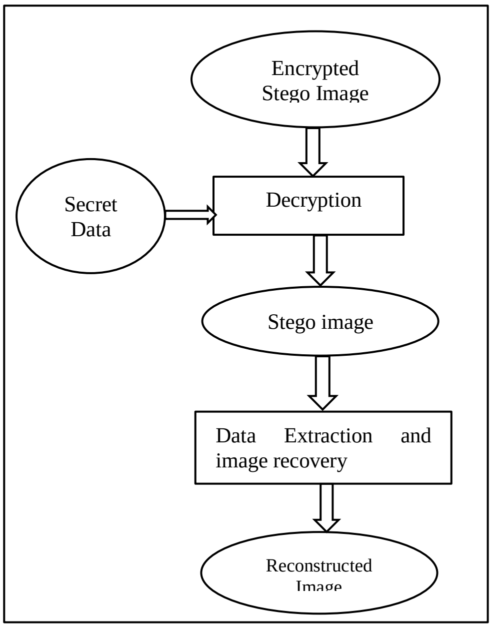


Fig. 2.2 Proposed Approach (Part B)

2.1 Reversible Data Hiding Algorithm

Input: Original Cover image
Output: Marked (Stego) image, index table, peak points, zero points

Step 1: Read the image and divide into blocks

The original cover image of size *MXN* is divided into4×4 non-overlap blocks $B_{k,}$ $\{Bk \mid k$=1,2….T}, where $T = MXN / 4X4$.

Step 2: Compute the pixel appearance frequency of blocks

Each block $B_k$has 16 pixels $b_{i,}\{b_i \mid i$=1, 2….16}. Compute the pixel appearance frequency $b_i$of block B_k, and find out the pixel which is the most frequency.

PixelFrequency(B_{i}) =No. of occurrences of{ $B_{1\,,}\,B_2 \ldots B_{16}$ }

MaxPixelFrequencyCount = Max(PixelFrequency(B_i)) where i=1,2…16

If there are more than one pixel having same frequency count which is maximum, then the average of pixels having equal maximumfrequency is calculated using (1) and considered as mode value.

If MaxPixelFrequencyCount>1

$$\text{AvgMaxFrequency} = \sum_{i=1}^{count} \frac{PixelFrequency(B_i)}{Count} \qquad (1)$$

ModeValue M_k=AvgMaxFrequency

All mode-values $M_k\{M_k \mid k_=$ 1 2…T}of each block B_k, are orderly recorded in an index table. The index tablecan be used as predictive values in hiding procedure and it can be used as secret key in extracting and restoring procedure.

Step 3: Compute the predictive difference

The image is scanned in inverse S order as shown in figure 2.3 and the prediction difference image generated.

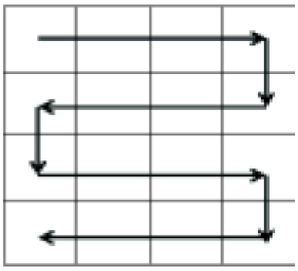


Fig 2.3: Inverse S order scanning

Compute the predictive differences by subtracting pixel values of each block by mode value. Assume the predictive difference d_i, *i= 1, 2...16*, in block B_k, d_i should satisfy $-255 \leq d_i \leq 255$, the predictive differences are computed as (2)

$$d_i = m_k - b_i \qquad (2)$$

Where i=1,2,...,16

Predictive differences are stored in array with size $M \times N$ and generates a predictive difference image.

Step 4: Evaluate the histogram of predictive difference image.

The system evaluates the frequency of predictive difference *di* and generates the histogramof predictive difference image.

Step 5: Find the peak and zero points of histogram of prediction difference

The system has to find two pairs of peak and zero points in histogram, which is divided into positive group 0 ≤ d_i ≤ *255* and negative group -255≤ d_i ≤−*1*. Each group has a peak point and a zero point. The peak point and zero point are shown in Figure 2.4(a). The peak point of positive group is pixel value *PH* = 0, which is 12 of frequency, and the zero point of positive group is pixel value PZ =3, which is 0 of frequency. On the other hand, the peak point of negative group is pixel value *NH* = -1, which is 8 of frequency, and the zero point of negative group is pixel value NZ= -4, which is 0 of frequency. After found the values of PH,PZ,NH,NZ, the system should record them and use for further extracting procedure.

Step 6: Shift pixels of predictive difference histogram

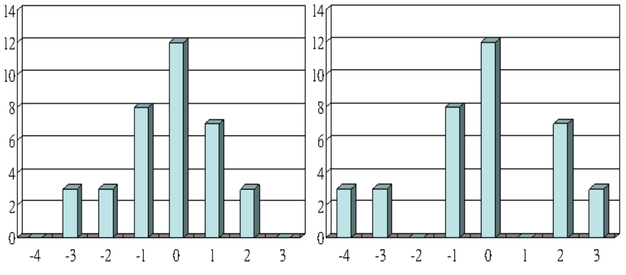
In order to hiding secret message in two peak points, thepixels of predictive difference between the peak point and zeropoint should be shifted left or right one bit. That is, thepredictive difference $d_{i,}$ adds one unit, $d_i = d_i+1$, ifpredictive difference d_i Є [PH+1, PZ−1]. On the otherhand, the prediction difference subtracts one bit $d_i = d_i-1$ if predictive difference d_i Є [NZ+1, NH−1]. After shifting the positions, the pixels of *PH* +1and *NH* −1 is empty, this will be used for hiding secret message. The histogram of shifting predictive difference is depicted in Figure 2.4(b). The predictive difference is increased one bit, $d_i = d_i+1$, if prediction difference d_i Є [1, 2], that is, the prediction difference image shifted right one bit.On the other hand, the predictive difference is decreased one bit, $d_i = d_i-1$, if prediction difference d_i Є [-3, -2], that is, the predictive difference is shifted left one bit. After shifted the pixels of predictive difference completely, the system can obtain the shifting predictive difference image and shifting histogram.

Step7: Embed the secret message.

The secretmessage is converted into binary and embedded into shifted predictive difference image. Firstly, the system scans the shifted image, and embeds secret message into the pixels. The pixel d_i' is not changed if d_i' is equal to peak point *PH* of positive group and peak point *NH* of negative group, and the secret message is $(0)_2$. On the other and, the peak point of positive group is increased one bit, i.e. $d_i'' = d_i'+1$, or the peak point of negative group is decreased one bit, i.e.$d_i'' = d_i'-1$, if the secret message is $(1)_2$. Repeat the Step until the secret messages are embedded.

Step 8: Construct the stego-image by predictive difference.

According to the hidden image, the system can construct the stego-image. Firstly, the hidden message image is divided into 4×4 non-overlapping blocks and scanned the blocks in inverse S scanning order. The system finds the predictive value m_k *of* block B_k and subtracts the pixel values of block B_k by using the index table. After the blocks are computed completely, we can obtain the stego-image, which has been hidden the secret messages.



(a) (b)

Fig.2.4 (a) Histogram of predictive difference image (b) Shifting Histogram of predictive difference image

2.2 *Hash Encryption Algorithm (SHA-1)*

a) Algorithm for Creating Transformation Table

```
Step 1: Select Image to be encryption from data store
Step 2: Insert key of 256 bits
Step3:Calculate Image Pixels Value
    Horizontal Value of Pixel = PixelWidth/10
    Vertical Value of Pixel = PixelHeight/10
Step 4:Select a Random Function to Calculate Final value for Horizontal and Vertical Pixels
    HorizontalPixel→Select Random Value between Horizontal Value of Pixel and PixelWidth
    VerticalPixel→Select Random Value between Vertical Value of Pixel and PixelHeight
Step 5:Select a Variable No-Of-Pixel to store Multiple Value of HorizontalPixel and VerticalPixel
    No-Of-Pixel = HorizontalPixel×VerticalPixel
Step 6:Using Hash Function (SHA-1) generate a Seed Value. This SHA-1 will apply on 256 bits Selected Key
    Seed = SHA-1(Above Selected KEY)
Step 7:Divide Seed into two Part equally Seed-1, Seed-2
    Seed-1 =First Half of Seed
    Seed-2=Second Half of Seed
Step 8: If Seed-1 is Greater Than Seed-2 Then Select another Variable SeedValue and assign any numeric value between 0 and 4 (Random) Otherwise Value of Seed Value Variable vary between 5 and 9 (Random).
Step 9: If Variable SeedValue is Equal Between 0 to 4 then calculate new seed value (Here we are working on ASCII value of seed).
    Seed = Seed + (Seed-1 Mod 2) + 1
Otherwise
    Seed = Seed + (Seed-2 Mod 2) + 1
Step 10: Repeat Process 8 to 9 till No-Of-Pixel/2
Step 11: Final Output of Step 10 will represent Create transformation Table
Step 12: Exit
```

b) Algorithm for Encryption

```
Step 1: Select an Image which is having at least 256 bits in Size to be encryption.
Step 2: Calculate Binary Value of Image.
```

*Step 3:*Select First 256 bits form Binary Value and create 16 sub blocks of 16 bits. This process will repeat till end of file.
*Step 4:*Select Key Value of 256 bits. And create 16 sub blocks of 16 bits.
*Step 5:*Select 64 bits from transformation table. And create 4 blocks of 16 bits.
*Step 6:*Apply Logical operation XOR between first 8 block of selected image and second 8 block of selected key. Result will stored in image blocks of
*Step 7:*Apply Logical operation XOR between last 4 blocks of selected images and 4 blocks of transformation table. Result will store in image blocks.
Step 8: Apply Circular Shift Operation on last 4 block of selected key and second last 4 block of selected image.
Step 9: Apply logical XOR operation between selected image and key which is output of step 8. Result will store in image block.
*Step 10:*Apply Circular Shift Operation on 4 blocks of transformation table and second last 4 block of selected key.
Step 11: Apply logical XOR operation between transformation t table and selected key, which is output of step 10. Result will store in key block.
Step 12: Combine output of step 6, 7, 9, and 11 in such that it should be produced 256 bits total.
Step 13: output of step 12 will become input for next round.
Step 14: Repeat step-1 to step-13, 10 times.
*Step 15:*After 10th round, cipher text will produce of selected image.
Step 16: Exit.

The resulted encrypted stego image can be now safely transferred across the network. For an intruder it is difficult to decrypt the image and guess the existence of hidden data in it. At the receiver side image will be decrypted first and secret text data can be extracted and original image will be recovered.

2.3 Image Decryption

Decryption process is reverse of above image encryption, which results in decrypted image with hidden data in it.

2.4 Data Extraction an image reconstruction

The data extraction and image recovery is reversion procedure of embedding method.To extract secretinformation from the stego-image, the system uses the peakpoint, zero point and index table of predictive value. By following all the steps in reverse order secret data can be extracted and original image is recovered.

3. Experimental Results

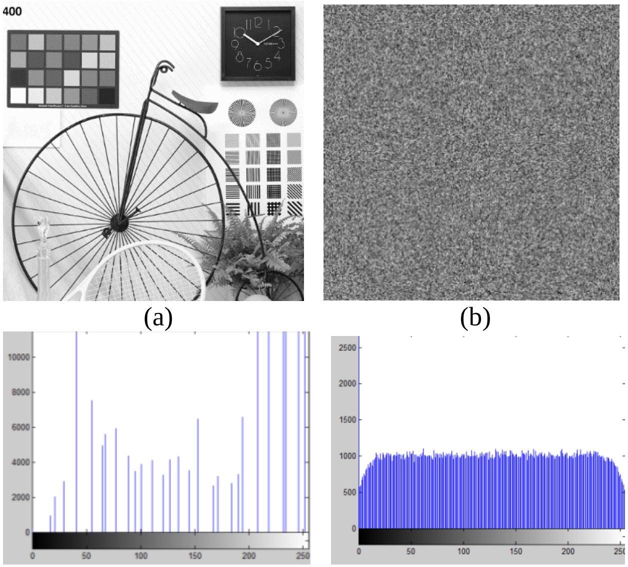
Experiments are performed on grayscale images of size 512×512. Secret Text data maximum up to 1000 bytes can be converted to binary and can embedded in these images. Then hash encryption is performed on these images. Entropy of original, stego-image and encrypted images are measured and compared. The correlation coefficient between original and stego-image, stego-image and encrypted images are calculated. Next, Image is decrypted and secret data is extracted. After recovering original image, image quality preservation is tested by computing MSE, PSNR and SNR parameters.By using pixel appearance frequency as predictive values this method explores the property of the image i.e. neighboring pixels have similarities and their values are minor changed. Thus, stego-images are able to preserve the good quality. Due to human eye perception it is not possible to detect the hidden data.Fig 3.1(a)-(e) Shows different bitmap images of size 512×512 used for experiments. Fig 3.2(a)-(e) shows Original, Stego-image, Encrypted image, Decrypted Image and Reconstructed Image after Data Extraction of Boat image.

3.1 Security Analysis

A good cryptosystem must be strong enough against attacks. In the following section security of proposed system is discussed against brute force Attack, statistical attack and texture analysis.

3.1.1 Key space Analysis: The Hash image encryption algorithm uses 256 bit key, resulting in key space size 2^{256} which is large enough to repel brute force attack.

3.1.2 Histogram Analysis: In order to prevent statistical analysis of cryptosystem it is important to ensure there is no similarities between histograms of original and encrypted images. Fig. shows histograms of original and encrypted images. It has been observed that histogram of encrypted image is uniformly distributed and significantly different from histogram of original image. Fig.3.3(a)-(d)shows histograms of originaland encrypted bitmap image.



(a) (b)

(c) (d)

Fig.3.3 Histogram Analysis (a) Original Image (b) Encrypted Image (c) Original image histogram (d) Encrypted image histogram

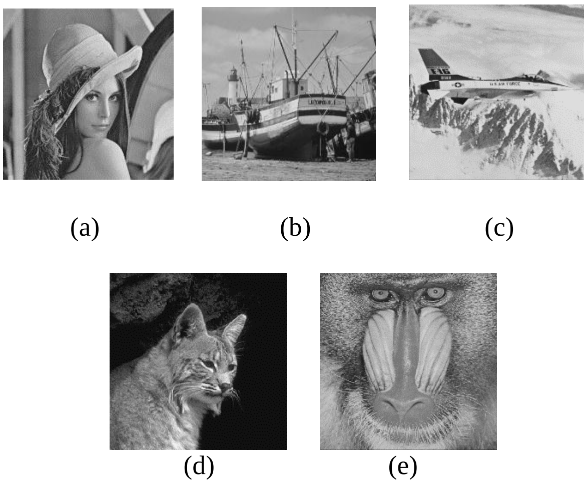


Fig. 3.1 (a) Lena (b) Boat (c) Airplane (d) Cat (e)Baboon images used in experiments.

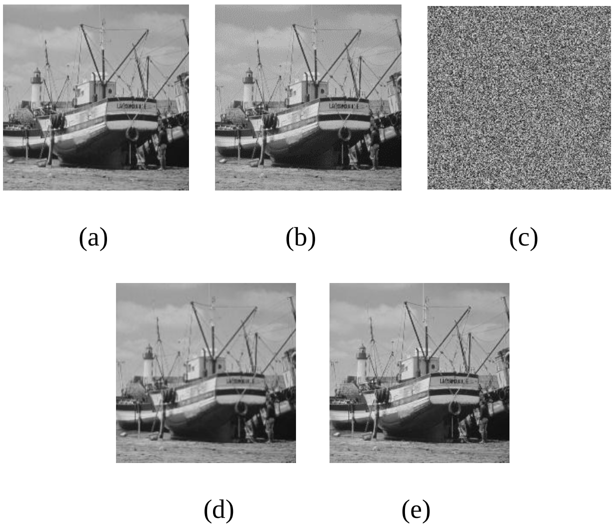


Fig. 3.2 (a) Original (b) Stego (c) Encrypted (d) Decrypted (e) Reconstructed Boat images.

3.1.3 Image Entropy: Entropy is the measure of randomness in the image. Shannon's Entropy (C.E.Shannon, 1948: C.E.Shannon, 1949; Yue Wu *et al*, 2011; Yue Wu *et al*, 2013) can be used to express degree of uncertainties in the encrypted image. The maximum entropy score of an encrypted image will be 8 for an 8 bit-gray scale image. In the context of image data Shannon's entropy is given as (3),

$$H(X) = -\sum_{l=1}^{L-1} P_l \log_2 P_l \tag{3}$$

Where L= 256 gray scales from 0 to 255 for a 8-bit grayscale image X, l is pixel intensity scale.This image entropy attains its maximum when a pixel's intensity is equally likely at any scale l An ideally encrypted image is completely random and thus its entropy reaches the theoretical maximum $\log_2$ L.

The table 3.1 compares the Entropy values of original, Stego-image and Encrypted stego-image. It is observed that randomness in the encrypted image is very high which near to maximum randomness value.

Table 3.1 Entropy values of Original, Stego image and Encrypted Stego images

Image	Entropy of original image	Entropy of stego image	Entropy of encrypted image
Lena.bmp	7.4455	7.4470	7.9587
Boat.bmp	7.1238	7.1373	7.9591
Airplane.bmp	6.6776	6.6978	7.9575
Cat.bmp	5.1924	5.9969	7.9579
Baboon.bmp	7.2562	7.2552	7.9571

3.1.4 Image Correlation: Pearson Correlation Coefficient (A.A.Goshtasby, 2012) is used as measure of similarity between two image sequences. Given two sequences of measurements $X = \{xi{:}i= 1. . . n\}$ and $Y = \{yi: i=1, . . . , n\}$, where. X and Y can represent images and xi and yi are intensities of corresponding pixels in the images.

The correlation coefficient between sequences X and $Y$is defined by (4)

$$r = \frac{\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{\sqrt{\{\sum_{i=1}^{n}(x_i-\bar{x})^2\}}\,\sqrt{\{\sum_{i=1}^{n}(y_i-\bar{y})^2\}}}- \tag{4}$$

Where$\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i$ and $\bar{y} = \frac{1}{n}\sum_{i=1}^{n} y_i$

Correlation coefficient r varies between −1 and +1. The case r = +1, called perfect positive correlation and the caser =−1, called the perfect negative correlation.The table 2 compares thecorrelation coefficient between original and stego-image, stego-image and encrypted image, encrypted and decrypted images. From the results it is clear that correlation between stego-image and encrypted image is very low indicating high level of dissimilarity between these two images. Low correlation indicates higher security of encrypted image. Table 3.2 describes correlation among different images. Encryption of the image breaks the correlation of pixels in the image.

Table 3.2 Correlation coefficient values of Original, Stego image and Encrypted Stego images.

Image	Correlation between Original and Stego-image	Correlation between Original image and Encrypted image	Correlation between Original Image and Decrypted image
Lena.bmp	1	0.0016	1
Boat.bmp	1	0.0025	1
Airplane.bmp	1	0.0026	1
Cat.bmp	1	0.0026	1
Baboon.bmp	1	0.0021	1

3.2 Image Quality Analysis

After the extraction of hidden secret data, image is reconstructed. Various performance measures such as MSE, PSNR and SNR has been evaluated. These parameters are used for image quality analysis (Ravi Kumar *et al*, 2012).

Mean Squared Error (MSE) measures level of distortion (error) between original and stego image. It is calculated as in (5).

$$\text{MSE}=\left(\frac{1}{mn}\right)\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[(I(i,j)-K(i,j)]^2 \qquad (5)$$

Where *I (i, j)* is original image
K (i, j) is stego image

Peak Signal to Noise Ratio (PSNR) is used to measure quality of reconstruction of images. It is the ratio between signal (Original image) and noise (error). Generally higher PSNR indicates higher quality.The PSNR is defined using (6)

$$\text{PSNR}=10.\log_{10}(MAX^{\wedge 2}/MSE) \qquad (6)$$

Where MAX is the maximum pixel value of the image. 255 for 8 bit image.The PSNR nothing but the SNR when all pixel values are equal to the maximum possible value. Table 3.3 shows the MSE, PSNR and SNR values obtained in experiments.

Table 3.3 MSE, PSNR, and SNR values of Reconstructed Images with respect to Original Images

Image	MSE	PSNR	SNR
Lena.bmp	0.7098	49.5855	22.0034
Boat.bmp	0.7790	48.5429	22.2043
Airplane.bmp	1.0000	47.4950	22.6897
Cat.bmp	0.3828	52.3016	21.5520
Baboon.bmp	0.7750	48.5282	22.0674

Conclusions

As the security is the major issue in many applications like banking, military and law forensics the confidential data need to be protected against various security attacks. Data hiding in images plays an important role in managing secrecy of data but may be vulnerable to attack. Our proposed approach combines image encryption with data hiding for providing further security to the images which contain the confidential data. This work is more suitable for the applications where original image and data both are confidential and Image need to preserve its quality. From the experiments we can conclude that,

1) The proposed approach protects the image containing secret data by making it secure against attacks. It will be difficult for an attacker to obtain secret information as attacker has to decrypt the image.
2) The Entropy values obtained are very high nearer to 8 which is the peak randomness of encrypted images.
3) Lower correlation values are achieved indicating there is no similarities with original image, thus it a strong encryption.
4) Reversible Data Hiding method helps in extracting the secret data without any loss of data as well as it helps in preserving Quality of original image after data extraction.
5) By dividing image into smaller blocks and then using mode value to construct prediction difference image increases the number of peak points and zero points in the histogram and thereby increases the embedding capacity.
6) Higher PSNR and low MSE values obtained in the experiments indicates image quality preservation.

References

J. Tian (2003) Reversible Data Embedding Using a Difference Expansion, *IEEE Tran. Circuits and Systems for Video Technology,* vol. 13, issue 8, pp. 890-896.

V. Fotopoulos, A. N. Sukodras (2007), A reversible data hiding technique embedding in the image histogram, *Hellenic Open University Journal of Informatics*,Technical Report HOU-CS-TR-2006-08-GR.

Wei Lee, Wen-Hsiang Tsai (2010), A Lossless Data Hiding Method by Histogram Shifting Based on an Adaptive Block Division Scheme, *Pattern Recognition and Machine Vision,* River Publishers, pp. 1–14,

Chin-Chen Chang, Wei-Liang Tai and Chia-Chen Lin (2006). A Reversible Data Hiding Scheme Based On Side Match Vector Quantization, *IEEE Transactions on Circuits And Systems For Video Technology*, Vol. 16, No. 10.

Ramandeep Kaur Grewa (2012), Image Compression Using Discrete Cosine Transform & Discrete Wavelet Transform, *International Journal of Computing & Business Research*, ISSN: 2229-6166

Z. Ni, Yun Q. Shi, N. Ansari, and W. Su (2006) Reversible Data Hiding, *IEEE Tran. Circuits and Systems for Video Technology,* vol. 16, no. 3, PP. 354-362

H. L. Yeh (2007), Prediction-Based Reversible Data Hiding, Master Thesis, Department of Computer Science and Information Management, Providence University, Taiwan, Republic of China

Wen-chung kuo, Dong-jinjiang and Vu-chihhuang (2008), A reversible data hiding scheme based on block division, *IEEE* , 978-0-7695-3119-9.

Ching-Te Wang, Ching-Lin Wang, Lin-Chun Li, Sheng-You Guo (2011), The Image High Capacity and Reversible Data Hiding Technique Based on Pixel Frequency of Block, *IEEE*, 978-1-4577-2119-9/12

Sowmyashree, R.R.Sedamkar, Sanjay sharma (2014), A modified pixel frequency based reversible data hiding for secure data communication, *IJCSIT*, ISSN: 0975-9646,Vol.5(6),2014,7035-7040

Rajkumar Ramaswamy, Vasuki Amurugam (2012), Lossless data hiding based on histogram modification, *The International Arab Journal of Information Technology*, Vol. 9, No. 5

Alireza Jolfael, Abdolrasoul Mirghadri (2010), An Image Encryption Approach using chaos and steam cipher, *JTAIT*, Vol.19 No.2.

Xiaojun Tong , Minggen Cui (2007), Image Encryption with compound chaotic sequence cipher shifting dynamically, *Elsevier journal Image and Vision Computing,* 843–850

Yuhong Zhang, Fenxia Zhao (2009), The algorithm of Fractional Fourier Transform and application in digital image encryption, *International conference on Information Engineering and computer science* , pp 1-4

Mohammad Ali Bani Younes and Aman Jantan (2007), Image Encryption Using Block-Based Transformation Algorithm, *IAENG International Journal of Computer Science*, 35:1, IJCS_35_1_03

Ching-Te Wang Ching-Lin Wang Lin-Chun Li Sheng-You Guo (2011), The Image High Capacity and Reversible Data Hiding Technique Based on Pixel Frequency of Block, *IEEE* , 978-1-4577-2119-9/12

Hiral Rathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma (2011), Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm (Hyper Image Encryption Algorithm), *International Journal of Computer Technology and Electronics Engineering (IJCTEE)* Volume 1, Issue3.

C.E.Shannon (1948), A mathematical theory of Communication, *Bell Syst. Tech. Journal*. 27,pp.379-423. 623-656

C. E. Shannon (1949), Communication Theory of Secrecy Systems, *Bell System Technical Journal*, vol.28-4, page 656—715.

Yue Wu, Joseph P. Noonan, Sos Agaian (2011), Shannon Entropy based Randomness Measurement and Test for Image Encryption, *Elsevier*, arXiv:1103.5520 v1[cs.CR]

Yue Wu, Yicong Zhou, George Saveriades, SosAgaian, Joseph P. Noonan, Premkumar Natarajan (2013), Local Shannon entropy measure with statistical tests for image randomness, *Elsevier*, Information Sciences, 323–342

A.A.Goshtasby (2012), Similarity and Dissimilarity Measures, *Advances in Computer Vision and Pattern Recognition (Springer)*, DOI 10.1007/978-1-4471-2458-0_2.

Ravi Kumar, Munish Rattan (2012), Analysis of Various Quality Metrics for Medical Image Processing, *IJARCSSE*, Volume 2, Issue 11, ISSN: 2277 128X