

A Robust Hybrid Steganography Mechanism for Security in Data Communication Networks

Neha Tayal

Research Scholar, YMCA University of Science and Technology, Faridabad, India.
nehatayal2292@gmail.com

Sangeeta Dhall

Assistant Professor, YMCA University of Science and Technology, Faridabad, India.
sangeeta_dhall@yahoo.co.in

Shailender Gupta

Assistant Professor, YMCA University of Science and Technology, Faridabad, India.
shailender81@gmail.com

Abstract – Steganography is an art and science of hiding the secret information into a carrier such as image, audio etc. in order to conceal the existence of the data. It can be broadly classified into two categories: Spatial (Time) and Frequency domain. The former technique preserves the quality of the cover image while the latter technique provides robustness during the embedding process. As mentioned, both the techniques have their certain pros. Therefore, in this paper a hybrid scheme based on the merits of the two has been proposed. The scheme is implemented in MATLAB-10 and various performance metrics such as Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Correlation coefficient, Time Complexity, Bit Error Rate (BER), effect of Gaussian Noise & salt & pepper noise on image are used to evaluate the efficacy of the proposed mechanism in comparison to others in literature. The results show that the proposed mechanism is highly robust to various kinds of attacks and has low time complexity.

Index Terms – Time Complexity, Cropping attack, Noise, Steganography.

1. INTRODUCTION

With the advancement in the technology, people find internet as the best suitable and convenient way for transferring and sharing data. With this growth, data breaches across the world have also risen exponentially [1, 2]. Thus today maintaining security in data communication is at utmost priority and steganography is the key process required for it. "It is the art of communicating in a way that hides the existence of the valuable communication data i.e. embedded message inside redundant one". In this or particularly image steganography the unimportant image or cover data is taken initially, now the secret data or the message i.e. to be embedded in this is taken and inserted into the cover image to form the stego-image with a very less amendments to the pixel values. The changes made are not recognized easily by the intruders and thus ensures the

data safety. Now this final image is transmitted and at the receiver side by using suitable techniques and algorithms the embedded message is retrieve back from the stego-image (see Figure 1). Similar to image, steganography can also be used in audio and other multimedia objects as it is generally easy to add significant amount of payload by means of simple modifications in cover data while preserving the underlying cover image data.

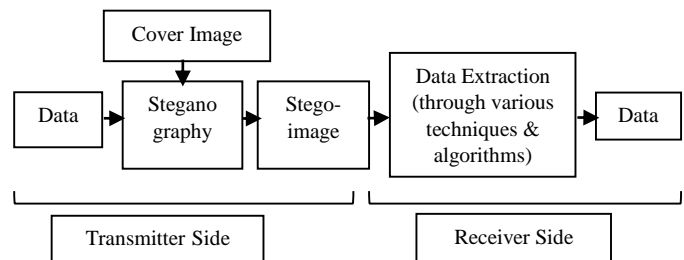


Figure 1 Steganographic Process

Based on embedding method used, steganography technique can be classified into following categories (see Figure 2):

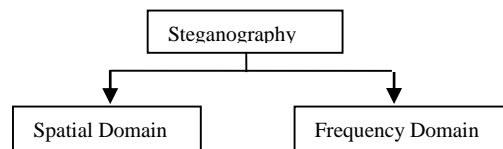


Figure 2 Classification of Steganographic technique

1.1. Spatial Domain Technique

The cover image in time domain is used to hide the data in least significant bits of pixels such that the image perceptual quality is not affected.

RESEARCH ARTICLE

1.1.1. Advantages

- Quality of the cover image remains almost same.
- Embedding capacity is high.
- Low perceptibility.

1.1.2. Disadvantages

- Less robust since one minute change in the image may lead to disruption of whole of the data.
- Access to key i.e. seed, will lead to the detection of the location of pixels in cover image data has been inserted.

1.2. Frequency Domain Technique

In this technique initially the cover image is transformed in frequency domain and then the message is embedded into this transformed image. This technique ensures robustness against various attacks as the data is embedded at the complex places which are not directly visible to the human eyes. Thus it disables the intruders to dig more into the image for data extraction. This technique is much more robust than time domain techniques since the cover image is subjected to transformation before storing data. Hence slight changes/modification that incurs in image during transmission process may not lead to total data loss.

1.2.1. Disadvantages

- Embedding capacity too low
- Time complexity is high.

Keeping above aspects in mind, this paper proposes a robust hybrid steganographic mechanism that combines the advantages of Improved BPCS (Time domain Technique)[3, 4] and DWT (Frequency Domain technique). The mechanism emphasized on both robustness and picture quality. The rest paper is organized as follows: Section 2 contains the detailed literature survey; Section 3 contains the proposed steganographic technique along with detailed mechanism of Improved BPCS and DWT; Section 4 contains information regarding simulation set up parameters and performance parameters that are required to check the robustness, security and performance of different techniques; Section 5 contains the results obtained for the proposed mechanism in comparison to other mechanisms; Section 6 contains final overall conclusion obtained which is followed by list of references.

2. LITERATURE SURVEY

Every technique mentioned in the Table 1 has its own advantages and disadvantages in comparison to other. The original BPCS steganography technique has highest data embedding capacity as compared to others but at the same time has high time complexity and is less robust. Similarly, when original BPCS was combined with IWT[5, 6] in order to reduce time complexity, the data embedding capacity decreased. Similar pros and cons were observed in other techniques i.e. Improved BPCS, Modified BPCS, etc.

In the Table 1 below various steganographic techniques has been mentioned along with their pros and cons.

Proposed By	Year of publication	Steganography technique used	Advantage	Disadvantage	Robustness
E. Kawaguchi et. al.[7]	1998	Original BPCS	<ul style="list-style-type: none"> • Highest data embedding capacity • Privacy & security • High PSNR 	<ul style="list-style-type: none"> • High time complexity 	Less robust due to spatial domain
Silvia Torres et. al.[8]	2006	Original BPCS combined with IWT	<ul style="list-style-type: none"> • Low time complexity • Privacy & security • Low bit error rate 	<ul style="list-style-type: none"> • Low data embedding capacity 	Robust as transform domain is used
Peipei Shi et. al.[9]	2010	Improved BPCS	<ul style="list-style-type: none"> • High data embedding capacity • Privacy & security • Higher PSNR 	<ul style="list-style-type: none"> • High time complexity 	Less robust due to spatial domain

RESEARCH ARTICLE

Smita P. Bansod et. al.[10]	2012	Modified BPCS using DES encryption and RSA compression algorithms	<ul style="list-style-type: none"> • High data embedding capacity • Privacy & high security • High PSNR 	<ul style="list-style-type: none"> • Highest time complexity • Become complex when data size increases 	Less robust due to spatial domain
Vipul J. Patel et. al.[11]	2013	Modified BPCS	<ul style="list-style-type: none"> • High data embedding capacity • Privacy & security • High PSNR 	<ul style="list-style-type: none"> • Higher time complexity 	Less robust due to spatial domain

Table 1 Literature Survey

After analyzing the details, a new hybrid mechanism in this paper is proposed based on the merits of Improved BPCS and DWT. This technique fulfills the standards of steganography i.e.

- High data embedding capacity
- High privacy and security.
- High PSNR and various other parameters.
- High robustness.
- Low time complexity.

The proposed technique has been described in the next section.

3. PROPOSED STEGANOGRAPHIC TECHNIQUE

In the proposed technique, firstly DWT is applied to the cover image on every plane i.e. Red (R), Blue (B) and Green (G) plane. The data is then embedded using improved BPCS algorithm. After embedding the data, inverse DWT (IDWT) is applied to form a stego-image. The image thus obtained is transmitted to the receiver side (see Figure 3).

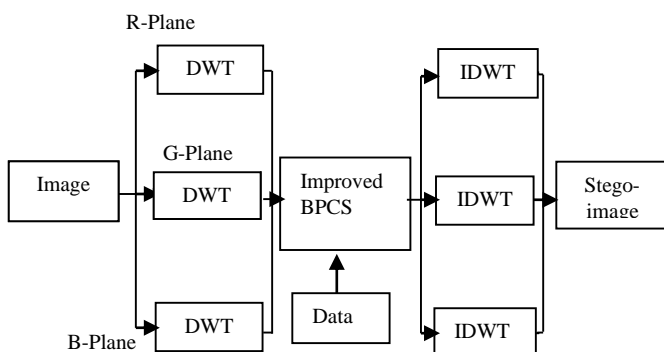


Figure 3 Block diagram of Proposed mechanism at sender's side

As shown in Figure 4, at the receiver side in order to extract data from the stego image, again DWT is applied to each plane

of the stego-image. On this image, improved BPCS technique is applied to extract the data.

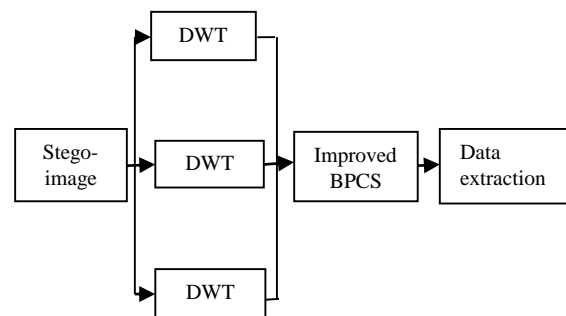


Figure 4 Block diagram of Proposed mechanism at receiver's side

The detailed explanation of the all the blocks is in the subsequent sections.

3.1. Discrete Wavelet Transform (DWT) steganography

In this transform, image in the time domain is passed through low-pass and high-pass filters banks in order to extract low and high frequency components from the image. Thus DWT for a discrete time-domain signal is obtained by successive low pass (averaging) and high pass (differencing) filtering (see Figure 5). In this figure let image is first passed through the low and high pass filters and the rate of output sampled signal is decreased i.e. down sampling is done for row elements. The outputs of the previous stage (H, L) are again passed through banks of low and high pass filters and finally different frequencies components i.e. HH, HL, LH and LL are obtained after down sampling of column elements.

In case of 2D-DWT first one-step transform is done on all row elements and finally a matrix is obtained. The left side of matrix contains down sampled low pass coefficients of each row while right side contains the high pass coefficients (see

RESEARCH ARTICLE

Figure 6). After that transform is applied on all columns and coefficients i.e. LL, LH, HL, HH are obtained (see Figure 7).

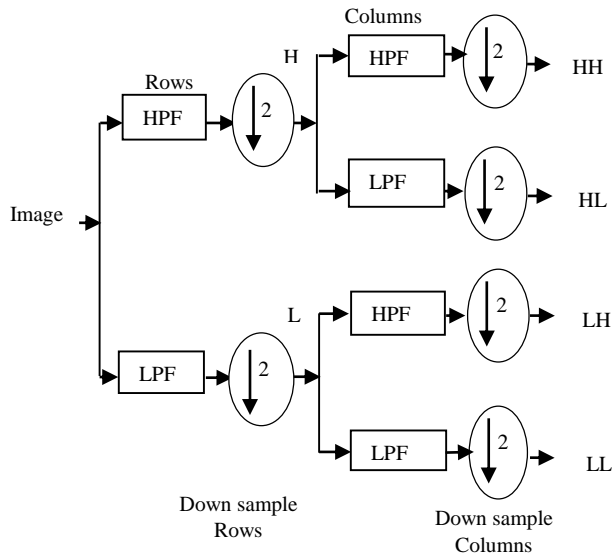


Figure 5 Block diagram representing 2-D DWT technique

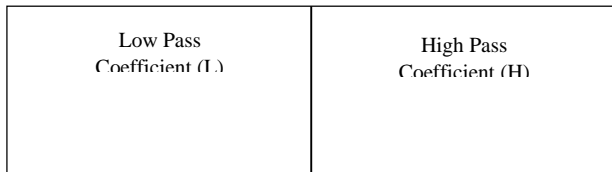


Figure 6 First step of wavelet decomposition

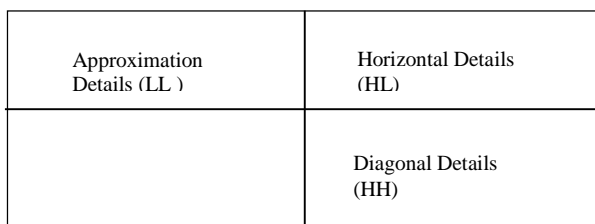


Figure 7 Final Output after wavelet decomposition

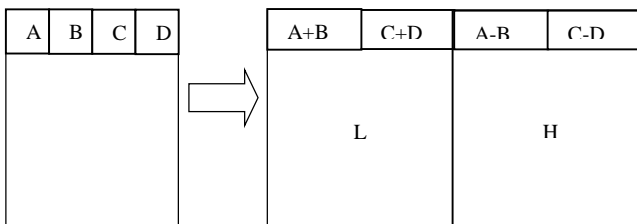


Figure 8 Output after applying Haar-DWT in horizontal direction

The proposed mechanism uses Haar-DWT frequency domain transforms technique as it is the simplest one and widely used mechanism. This mechanism scans pixels from left to right in

arrow i.e. in the horizontal direction. During this horizontal scanning of the pixels the addition and subtraction on the adjacent pixel values are performed. Finally fine details in small area are recorded in which pixel addition represents the lower frequency component (L) and subtraction represents higher frequency components (H) [12, 13] (see Figure 8).

As mentioned earlier (see Figure 6) the output of this image contains two halves i.e. left half (L) contains the low pass coefficient while the right half (H) contains high frequency coefficients. In the similar fashion scanning of the pixels is done from top to bottom in vertical direction i.e. column-wise and again addition and subtraction operations are performed for the adjacent pixels. After the operation in the vertical direction the sum is stored in the upper half and the difference in the lower half and matrix is obtained as shown below (see Figure 9).

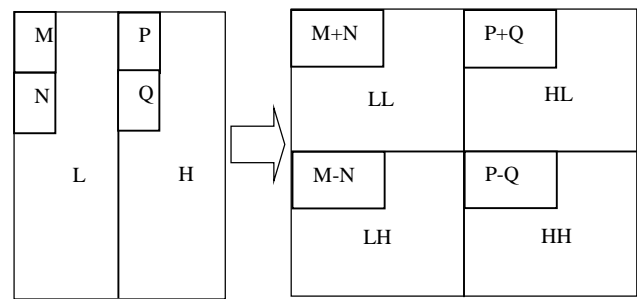


Figure 9 Output after applying Haar-DWT in vertical direction

Thus after performing Haar-DWT we had transformed image, in which with the help of Improved BPCS technique required data is embedded. The Improved BPCS technique has been described below.

3.2. Improved BPCS

The human eyes cannot differentiate in shapes and information of the image in the complex planes i.e. the noise-like regions. This property is exploited in Bit-Plane Complexity Segmentation (BPCS)[14-16] Steganography and therefore its performance in terms of embedding capacity is better than other LSB steganography techniques. At the same time it preserves the picture quality too. The complete flowchart for proposed technique based on BPCS is shown in Figure 10.

In this proposal improved BPCS is applied to the image obtained by performing Haar-DWT. This output image of the previous stage (DWT) is first converted into matrix where each pixel value is expressed as 8 bit number. From these pixel values 8 bit planes are formed for R, G and B planes respectively (see Figure 11). First all the LSBs of the pixel values are combined in order to form Bit 0 plane. Similarly, in this fashion planes are formed from Bit 0 to Bit 7 and finally we will have 8 x 3=24 bit planes in total i.e. from bit 0 to bit 7.

RESEARCH ARTICLE

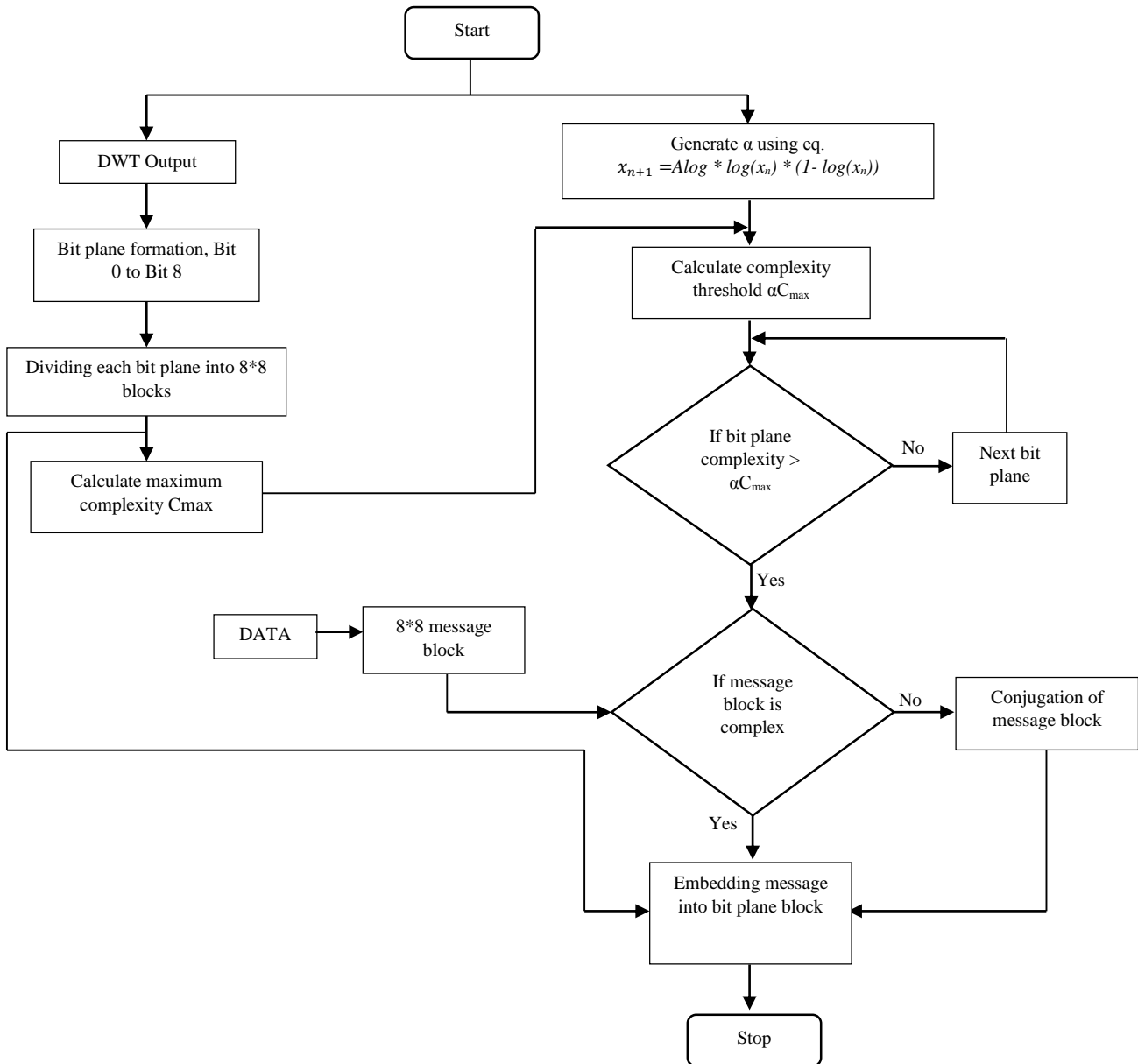


Figure 10 Block diagram of Improved BPCS

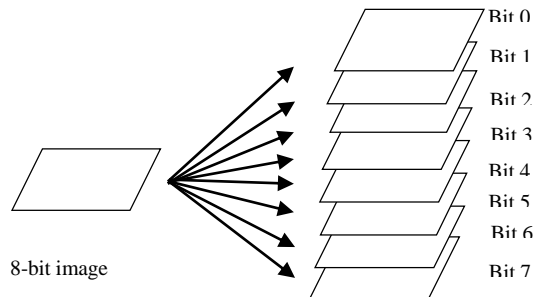


Figure 11 Dividing of bits to form bit planes



RESEARCH ARTICLE

These bit planes are further converted into 8x8 block planes, and then maximum complexity is calculated. Complexity is defined as the amount of all the adjacent pixels that get different values i.e. one pixel value is 0, and the other is 1. The maximum possible value of the complexity is denoted as Cmax. This complexity is then used to calculate complexity threshold. For calculating complexity threshold another parameter α is required, which is generated dynamically using chaotic map as explained below. Using these two parameters complexity threshold, αC_{max} is calculated and then compared with the complexity value of each bit plane. If this calculated complexity value of given bit plane is greater than the required one i.e. αC_{max} the complex message is embed into it otherwise this bit plane is skipped. If the message is not complex then conjugation is done before embedding process.

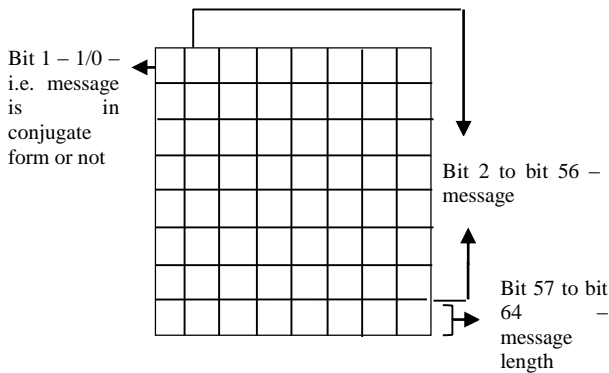


Figure 12 Structure of bit plane block

Thus this 8 x 8 block contains all the information regarding the message and data length (see Figure 12). First bit i.e. bit 1 gives information regarding status of message embedded, which means if it is 0 then information block is not conjugate and if it is 1 then information block is conjugate. Bit 2 to bit 56 contains the message or data and bit 57 to bit 64 contain the information regarding the length of the message that has been embedded.

• Chaotic map:

In this proposed technique parameter α which is used for finding complexity threshold is calculated using chaotic map. This map includes generation of random sequence for various 1D and 2D discrete maps based on mathematical equations and relations i.e. Logistic map, Cubic map, Ricker's map, Sin map, Henon map, Gingerbreadman map, Burgers' map, Tinkerbell map, etc.

One of the most studied examples of a one-dimensional system is logarithmic map, its properties and chaotic performance is also similar to logistic map. Its equation is

Logistic Map equation

$$x_{(n+1)} = \text{Alog} * \log(x_n) * (1 - \log(x_n))$$

The behaviors displayed by the Logistic map depends on parameter Alog and initial value x_n where $0 < x_n < 1$. The properties like unpredictability and randomness ensured the usage of logistic map. Moreover chaotic maps are sensitive to variations in the initial condition thus the sequence can be varied even with a small change in this value.

In this technique we had used chaotic sequence generation in order to generate sequence from 0 to 1 which can be further used to set the corresponding threshold i.e.

Let x be the data generated, then $0 \leq x \leq 1$ and

- 2 for $0 \leq x < 0.2$
- 1 for $0.2 \leq x < 0.4$
- 0 for $0.4 \leq x < 0.6$
- 1 for $0.6 \leq x < 0.8$
- 2 for $0.8 \leq x \leq 1$

Thus this dynamically generated threshold is one of the deciding factor for finding whether the bit plane block can be used to embed the secret data or not.

3.3. Algorithm

Embedding algorithm (Sender's Side):

1. Convert secret message into binary form and then make 8*8 size blocks of this binary secret data.
2. Obtain the cover image and split the image in R,G,B planes.
3. Apply Haar-DWT for all the three Planes.
4. Now, converting one of the four sub band of any plane obtained from DWT first in binary form and then in gray code.
5. This transformed cover image is then divided into different bit planes i.e. from 0 to 7 for all three planes.
6. These bit planes are further converted into 8x8 block planes, and then maximum complexity Cmax is calculated.
7. Another parameter α is generated dynamically using chaotic map. Using these two parameters complexity threshold, αC_{max} is calculated.
8. This complexity threshold, αC_{max} is compared with the complexity value of each bit plane.
9. If the calculated complexity value of given bit plane is greater than the required one i.e. αC_{max} the message is embed into it else complexity of next plane will get compared.

RESEARCH ARTICLE

10. Before embedding the message its complexity is also checked using the same procedure. If the message is complex then it is embed as such else its conjugate is obtained and embed.
11. Repeat steps 8 and 9 for each bit plane and message block.
12. Then, reform the image by reversing the above process i.e. first converting the bit plane blocks into bit planes, and apply inverse DWT to form stego-image.

Thus in Improved BPCS the data can be placed at the region insensitive to human vision i.e. complex noise-like region in order to prevent its secrecy and maintain the robustness of the steganographic process.

Thus after embedding the bits at the complex places, IDWT is applied to obtain the image again, known as stego image and contains the message embedded in it (see figure 3). This stego image is transmitted to the receiver. At the receiver side too in the same fashion the message can be retrieve back i.e. initially checking the complexity of the bit plane and then getting information about the conjugation from the first bit i.e. bit 1 and as per the status of this bit retrieving the original message. Thus this proposed technique ensures high security of the data and high robustness.

3.4. Algorithm

Extraction Algorithm (Receiver’s Side):

At the receiver side the stego image is taken and DWT is performed on it.

1. Obtain the stego image. Split the image in R,G,B planes
2. Convert the pixel values into discrete form for all the three planes.
3. Perform Haar-DWT for all the Planes.
4. Now, converting one of the four sub band of any plane obtained from DWT first in binary form and then in gray code.
5. This transformed cover image is then divided into different bit planes i.e. from 0 to 7 for all three planes.
6. Then, find the complexity of each bit plane block. If complexity is less than complexity threshold, α_{Cmax} then skip that block else check the status of conjugation of secret message.
7. Extract the length of message from last row, and finally retrieve the message from bit locations 2-56.
8. Repeat step 6 and 7 for all the bit planes as per the length of the message.

9. Now, recover the secret message by converting the message obtained in step 7 into original form.

4. SIMULATION SET UP PARAMETERS AND PERFORMANCE METRICS

4.1. Simulation Set Up Parameters

The simulation Set Up parameters are given in Table 2.

Processor	Core-i3 1.7GHz RAM 4GB
Operating system	Windows 8.1
Image size	64*64 128*128 256*256 512*512
Image type	.png
Simulation tool	MATLAB 7.10.0.499 64 bit (win 64)
Text used for embedding	“ABCDEFABCDEFABCD0123456789012345”
Color type	RGB
Threshold parameter α used in BPCS technique	$\alpha = k / (2 * 2^m * (2^m - 1))$ Where k is the length of border in image and m=3 for 8*8 size binary image

4.2. Performance metrics

For complete analysis of the proposed scheme various parameters and effects of different attacks on these parameters are observed, which are divided into following categories:

4.2.1. Robustness Analysis

4.2.1.1. Mean Absolute Error (MAE)

The MAE is the mean absolute error between the image obtained after performing steganography and the original

RESEARCH ARTICLE

version of the image. Lower the value of MAE means lower is the error.

$$MAE = \sum_{i=1}^n \sum_{j=1}^m |f(i, j) - y(i, j)|$$

Where,

$f(i, j)$ is the pixel value of original image,

$y(i, j)$ is the pixel value of new image,

Size of image is $m \times n$ for monochrome image and $m \times n \times 3$ for colored image.

4.2.1.2. Mean Square Error (MSE)

The MSE is obtained as a cumulative of the square of the errors between the image obtained after steganography and the original image. Lower the value of MSE means lower is the error.

$$MSE = \frac{1}{\text{size}} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [f(i, j) - K(i, j)]^2$$

Where,

$f(i, j)$ is the pixel value of original image,

$K(i, j)$ is the pixel value of new image (noisy approximation),

size of image is $m \times n$ for monochrome image and $m \times n \times 3$ for colored image.

4.2.1.3. Peak Signal Noise Ratio (PSNR)

It is defined as the ratio between the maximum possible power of a signal and the power of corrupting noise. It is the ratio of peak square value of pixels by mean square error (MSE). It is expressed in decibel (db). The PSNR is defined as:

$$PSNR = 10 \cdot \log_{10} \left(\frac{MAX_I^2}{MSE} \right)$$

Where,

MAX_I represents maximum value of pixel of the image,

MSE is the mean square error.

4.2.1.4. Time Complexity

It is defined as the time taken or the processing time by the algorithm to run which is implemented in a function to perform a specific task.

4.2.2. Similarity Analysis

The parameters under this category measure the closeness of stego-image and cover image.

4.2.2.1. Correlation coefficient

This parameter is a measure of the linear correlation i.e. dependence between two images A and B. Its range is between -1 to +1 both inclusive, where 1 signifies perfect match and -1 signifies total mismatch. The correlation coefficient can be calculated as:

$$\rho(A, B) = \frac{\text{cov}(A, B)}{\sigma_A \sigma_B}$$

Where,

A is cover image and B is the stego-image,

$\rho(A, B)$ is the correlation coefficient between image matrices A and B.

$\text{cov}(A, B)$ is the covariance between matrices A and B,

σ_A is the standard deviation of A,

σ_B is the standard deviation of B.

4.2.3. Security Analysis

As the images and data moves from transmitter to receiver through transmission channel various types of noises are encountered with. Some prominent occurring noises are as follows, thus their effect will be seen on different techniques.

4.2.3.1. Salt and Pepper Noise

It is the external disturbance or the form of noise seen on the images. It is also known as Impulse Noise. This noise can be caused by sharp and sudden disturbances in the image signal. Its appearance can be seen as sparingly occurring of white and black pixels on the image.

4.2.3.2. Gaussian Noise

It is the noise caused by the random fluctuations in the signal. It is a statistical noise which is defined as normal or Gaussian distribution i.e. probability density function (PDF) $p(z)$ can be defined as:

$$p(z) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(z-\mu)^2}{2\sigma^2}}$$

Where z represents the grey level, μ the mean value and σ the standard deviation.

4.2.3.3. Bit Error Rate (BER)

In the digital transmission of data over the communication channel sometimes the alteration of bits occurs due to noise, interference, etc. Thus it is defined as the probability of error in terms of number of erroneous bits transmitted per unit time i.e. it can be obtained by dividing the number of error bit to the total number of bits transmitted. As the quality of the channel decreases the BER increases.

RESEARCH ARTICLE

4.2.3.4. Cropping Attack

Cropping states to the removal of the outer portions of an image to improve framing, highlight subject matter or change aspect ratio.

In order to apply this attack on the received stego image, cropping of image has been done as follows:

- Perform the steps below for different values of aspect ratio ranging from 6.25% to 25%, where aspect ratio= width/height.
- Apply cropping attack on the stego image obtained as:
A= imcrop (I,rect)
I= image on which cropping is to be applied

rect= four-element position vector described as:

rect= [x(min), y(min), width, height]

x (min)= minimum distance from x-axis.

y (min)= minimum distance from y-axis.

width = horizontal dimension for cropping.

height = vertical dimension for cropping.

5. RESULTS

5.1. Snapshots

Comparison of various images after applying different approaches is shown in Figure 13.






Original image	Image after applying E. Kawaguchi et. al.	Image after applying Silvia Torres et. al.	Image after applying Peipei Shi et. al.	Image after applying Vipul J. Patel	Image after applying proposed technique
					
					
					
					

Figure 13 Snapshot

5.2. Effects of attacks on different parameters

Various attacks have been applied on different steganographic techniques which prove that the proposed technique is highly robust [17].

Figure 14 and 15 depicts that Peipei Shi et. al. is the best technique in terms of PSNR. At no noise, it provides highest PSNR. But as the noise increases, PSNR goes down rapidly for all the defined techniques except the proposed one. Thus in the practical scenario where presence of noise is pertinent

RESEARCH ARTICLE

proposed technique gives best results by showing little sensitivity towards noise.

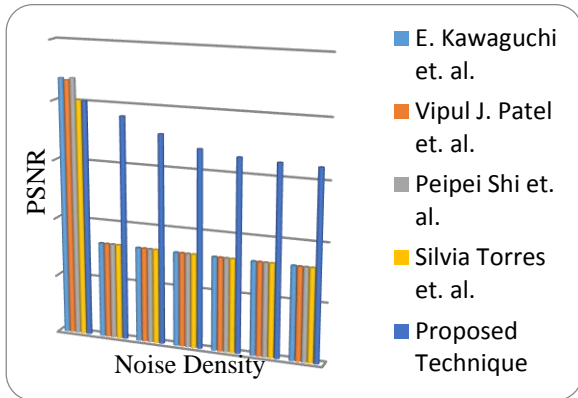


Figure 14 Comparison of PSNR after addition of Gaussian noise

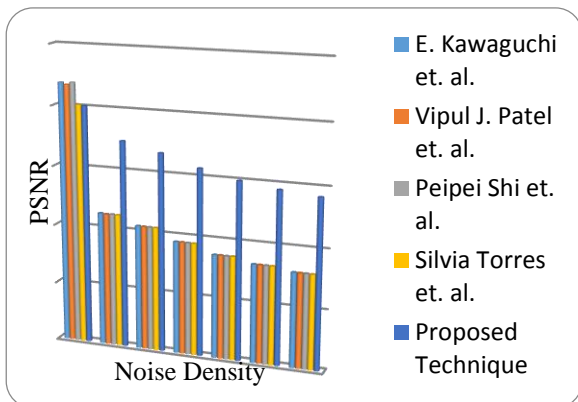


Figure 15 Comparison of PSNR after addition of Salt & Pepper noise

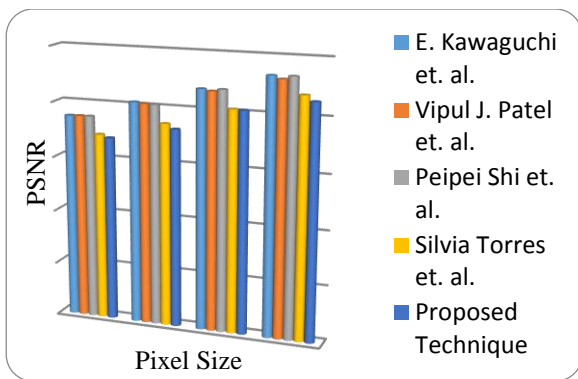


Figure 16 Comparison of PSNR on different Pixel Size

Figure 16 shows that as the size of image increases, PSNR value increases for all the techniques and it is highest in case of Peipei Shi et. al. because of the similarity between original image and stego image. Since the proposed technique uses transform domain, so its PSNR is somewhat less than others.

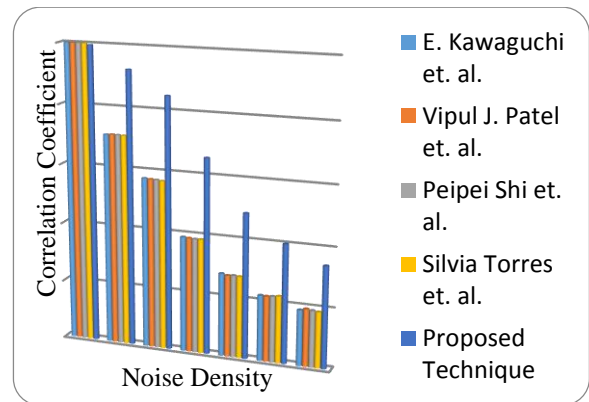


Figure 17 Comparison of Correlation Coefficient after addition of Gaussian noise

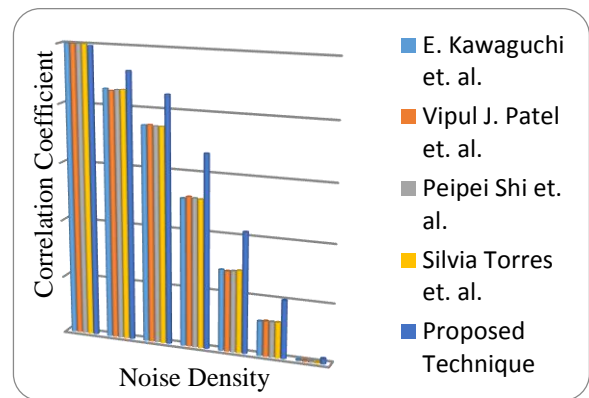


Figure 18 Comparison of Correlation Coefficient after addition of Gaussian noise

Figure 17 and 18 depicts that at zero noise, all of the techniques have highest correlation coefficient value as 1. But as the noise grows, this value falls down rapidly for all the techniques except the proposed one which proves that the proposed technique is robust amongst all.

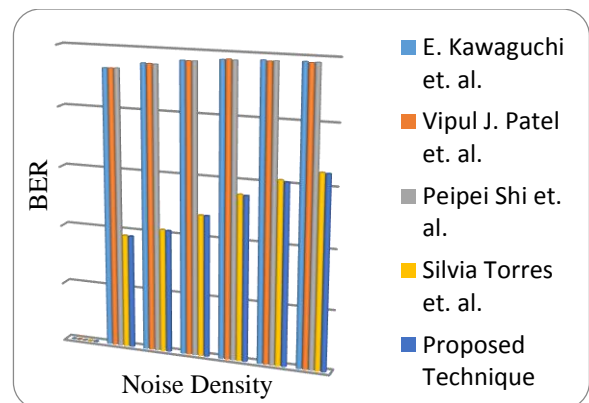


Figure 19 Comparison of BER after addition of Gaussian noise

RESEARCH ARTICLE

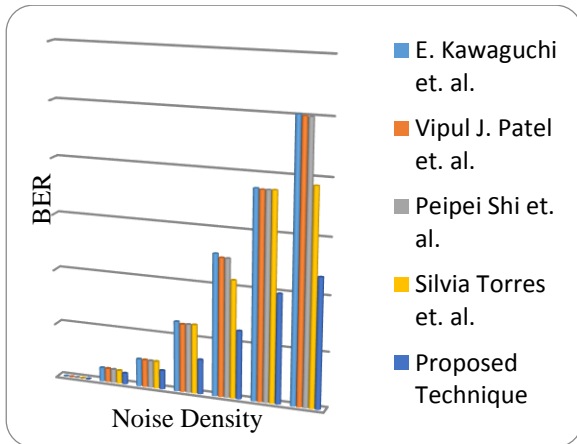


Figure 20 Comparison of BER after addition of Salt & Pepper noise

In Figure 19 and 20, at zero noise, there is no effect on bit error rate. But as the noise density rises, the number of error bits in stego image increases in all techniques. But this increase is slow in proposed technique which again proves the robustness of this technique compared to any other.

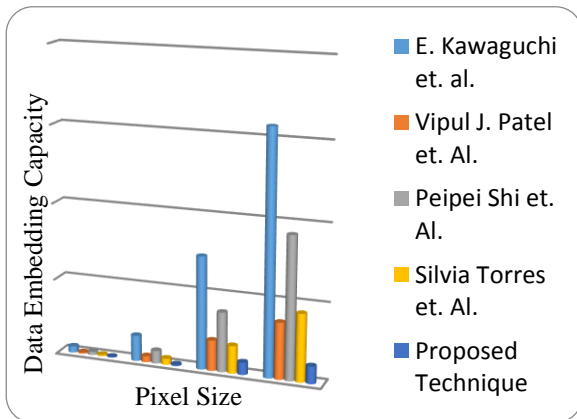


Figure 21 Comparison of Data Embedding Capacity on different Pixel Size

Figure 21 depicts that as the pixel size increases, data embedding capacity also increases and it is highest in E. Kawaguchi et. al. as there is no change in the threshold value to calculate complexity of every bit plane. Vipul J. Patel et. al. uses variable threshold for every bit plane which is highest for MSB bit plane, so its embedding capacity goes down. And the proposed technique uses dynamic threshold in which every bit plane and every bit plane block has dynamic threshold value which ensures its security against steganalysis, so its embedding capacity decreases.

Figure 22 clearly shows that proposed technique has lowest time complexity as transform domain is used because spatial domain technique requires much time to process. Hence, proposed technique is best in terms of time complexity.

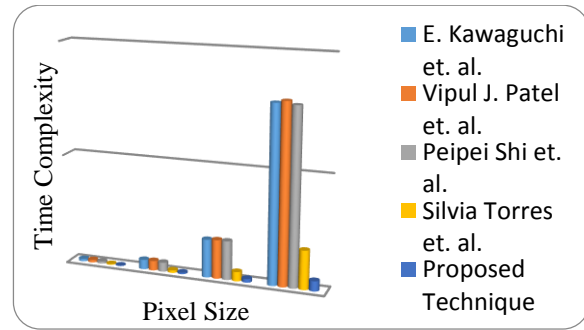


Figure 22 Comparison of Time Complexity on different Pixel Size

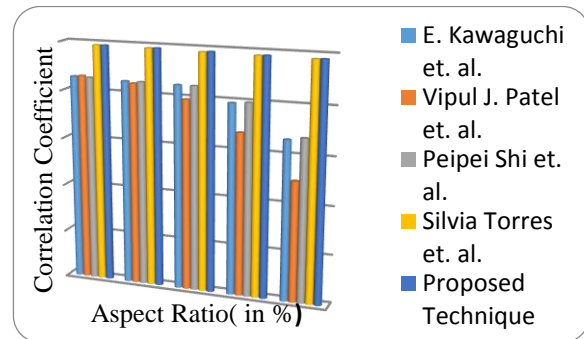


Figure 23 Comparison of Correlation Coefficient after performing Cropping

Figure 23 depicts that as the cropping ratio increases, there is a high reduction in correlation coefficient which increases the chances for the intruder to judge the stego image for the presence of data. The proposed technique shows a uniform value for any ratio of cropping, hence it proves to be most robust amongst all.

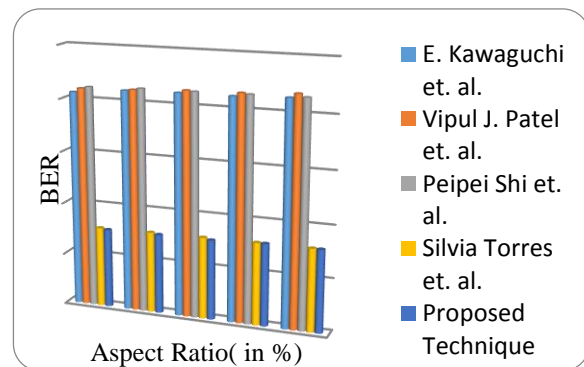


Figure 24 Comparison of BER after performing Cropping

Figure 24 shows that as the aspect ratio intensifies, the effect of cropping attack almost remains a constant for transform domain techniques, which again ensures the robustness of this frequency domain technique. But it highly affects the spatial domain techniques which again make them vulnerable to attacks.

RESEARCH ARTICLE

6. CONCLUSION

Along with the advancement in technology, the risk of more sophisticated attacks to check the presence of secret message also increases. So, there is a need to make some amendments in various security mechanisms to make the secret message more secure and private. In this paper, various steganographic mechanisms have been compared in terms of robustness, BER,

correlation coefficient, time complexity and security. Most of the techniques employ spatial domain steganographic techniques while the proposed hybrid mechanism combines spatial and frequency domain techniques. Thus it is more robust and secure and also preserves the quality of the image. Table 3 shows the overall comparison of various steganographic techniques present in the literature with the proposed mechanism.

Parameters	E. Kawaguchi et.al.	Vipul J. Patel et.al.	Peipei Shi et.al.	Silvia Torres et. al.	Proposed Technique
Robustness	Low	Low	Low	High	High
Security	Secure	Secure	Secure	Secure	Highly secure
Perceptual quality	High	High	High	High	Low
Embedding capacity	Highest	High	Moderate	Moderate	Low
PSNR	High	High	High	Moderate	Moderate
Time Complexity	Higher	Highest	High	Low	Lowest

Table 3 Overall Comparison

REFERENCES

- [1] Joe, M. Milton, B. Ramakrishnan, “A Survey of Various Security Issues in Online Social Networks”, in proceedings of International Journal of Computer Networks and Applications, Vol. 1, Issue 1, pp 11-14, 2014.
- [2] Emad Abu-Shanab, Salam Matalqa, “Security and Fraud Issues of E-banking”, in proceedings of International Journal of Computer Networks and Applications, Vol. 2, Issue 4, pp 179-187, 2015.
- [3] Chintan Jain, VivekParate, Ajay Dhamanikar, RakeshBadgujar, “Review on Steganography and BPCS Technology in Steganography for Increasing Data Embedding Capacity”, in proceedings of International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 1, pp 60-65, 2015.
- [4] Pranita P. khairmar, Prof. V. S. Ubale, “Steganography Using BPCS Technology”, in proceedings of International Journal of Engineering And Science, Vol. 3, Issue 2, pp 08-16, 2013.
- [5] PreetiChaturvedi, R. K. Bairwa, “An Integer Wavelet Transform Based Steganography Technique for Concealing Data in colored Images”, in proceedings of International Journal of Recent Research and Review, Vol. 8, Issue 1, pp 49-57, 2014.
- [6] M. Vijay, V. VigneshKumar, “Image Steganography Method Using Integer wavelet Transform”, in proceedings of International Journal of Innovative Research in Science, Engineering and Technology, Vol. 3, Issue 3, pp 1207-1211, 2014.
- [7] Eiji Kawaguchi, Richard O. Eason, “Principle and Applications of BPCS-Steganography”, in proceedings of Society of Photographic Instrumentation Engineers (SPIE), Vol. 3528, pp 464-473, 1998.
- [8] Silvia Torres-Maya, Marika Nakano-Miyatake, Hector Perez-Meana SEPI, “An Image Steganography Systems Based on BPCS and IWT”, in proceedings of 16th IEEE International Conference on Electronics, Communications and Computers, 2006.
- [9] Peipei Shi, Zhaohui Li, “An improved BPCS Steganography based on Dynamic Threshold”, in proceedings of International Conference on Multimedia Information Networking and Security, pp 388-391, 2010.
- [10] Smita P. Bansod, Vanita M. Mane, Leena R. Ragha, “Modified BPCS Steganography using Hybrid Cryptography for Improving Data embedding Capacity”, in proceedings of International Conference on Communication, Information & Computing Technology (ICCICT), 2012.
- [11] Vipul J. Patel, Ms. NehaRipalSoni, “Uncompressed Image Steganography using BPCS: Survey and Analysis”, in proceedings of IOSR Journal of Computer Engineering, Vol. 15, Issue 4, pp 57-64, 2013.
- [12] Barnali Gupta, Prof. Samir K. Bandyopadhyay, “A DWT Method for Image Steganography”, in proceedings of International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 6, pp 983-989, 2013.
- [13] Amitava Nag, SushantaBiswas, DebasreeSarkar, ParthaPratimSarkar, “A Novel Technique for Image Steganography Based on DWT and Huffman Encoding”, in proceedings of International Journal of Computer Science and Security, Vol. 4, Issue 6, pp 561-570.
- [14] Shrikant S. Khaire, Dr. Sanjay L. Nalbalwar, “Review: Steganography-Bit Plane Complexity Segmentation(BPCS) Technique”, in proceedings of International Journal of Engineering Science and Technology, Vol. 2(9), pp 4860-4868, 2010.
- [15] Sarita, KamleshLahwani, ShilpaChoudhary, “An Improved BPCS Image Steganography in Integer Wavelet Transform Domain using 4x4 Block Size”, in proceedings of International Journal of Engineering Research & Technology, Vol. 1, Issue 8, pp 1-8, 2012.
- [16] Vaishali, AbhishekKajal, “Increasing Data Hiding Capacity of Carrier Image Using BPCS Steganography”, in proceedings of International Journal of Science and Research(IJSR), Vol. 4, Issue 5, pp 434-437, 2015.
- [17] Siddharth Singh, Tanveer J. Siddiqui, “A Security enhanced Robust Steganography Algorithm for Data Hiding”, in proceedings of International Journal of Computer Science Issues, Vol. 9, Issue 3, No. 1, pp 131-139, 2012.

Authors



Neha Tayal is pursuing M.Tech in the field of Electronics and communication at YMCA University of Science and Technology, Faridabad. She has passed her B.tech in the same field from G.S. Modern Vidya Niketan Institute of Engineering and Technology, Palwal.

RESEARCH ARTICLE



Sangeeta Dhall has obtained M. Tech degree from YMCA University of Science and Technology. Her interest includes the following topics: Image processing, Embedded System Design and image encryption.



Shailender gupta has obtained Ph. D from YMCA University of Science and Technology. His interest includes the following topics: Image processing, Embedded System Design and image encryption, Networking.