I. J. Computer Network and Information Security, **2016, 6, 67-78**
Published Online June 2016 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2016.06.08

An Improved Hybrid Mechanism for Secure Data Communication

Sangeeta Dhall
YMCA University of Science and Technology, Faridabad, India
E-mail: Sangeeta_dhall@yahoo.co.in

Bharat Bhushan
YMCA University of Science and Technology, Faridabad, India
E-mail: bhrts@yahoo.co.in

Shailender Gupta
YMCA University of Science and Technology, Faridabad, India
E-mail: Shailender81@gmail.com

Abstract—The In today's era with increase in the use of internet and networking devices, there is an increase in demand for more secure data communication. This problem has led to development of hybrid security mechanisms. Various techniques are available in literature that makes use of different steganography and cryptographic mechanisms which has certain pros and cons. In this paper, we propose a new hybrid security mechanism that tries to choose the best cryptographic and steganography mechanism. In addition, to increase the embedding capacity of the proposed mechanism, Huffman encoding scheme is used. The proposed strategy is implemented in MATLAB-09. In order to check the efficacy of the proposed technique three types of analysis were performed named as: security, robustness and efficiency analysis. It is found from the simulation and results that the proposed scheme outperforms other techniques in literature in every aspect.

Index Terms—Security, cryptography, steganography, compression technique and performance metrics.

I. INTRODUCTION

With the increase in number of internet users, the demand for robust and secure data communication requirement is gaining popularity day by day. The solution to this problem can be in the form of cryptography, the primary goal of which is to change data into some other form understandable only by the intended users. [1] Various cryptographic algorithms have been proposed to provide confidentiality to the data. In all these mechanism if an intruder is able to guess or steal the key than he can easily decrypt the encrypted data. Another popular mechanism to secure the data communication is steganography in which the data to be transmitted is hided in a cover image. [14, 16] Many steganography techniques have been proposed in literature that tries to embed the data in such a way that if an intruder gets the stego image still can't guess the presence of data in the image. To enhance the level of security, researchers focused their attention on the use of hybrid security mechanisms which involves encrypting the data first and then use steganography (see Fig. 1). [2] Though, this hybrid mechanism results in increased value of time complexity but provides much high brute force search time and far better security in comparison to stand alone techniques.

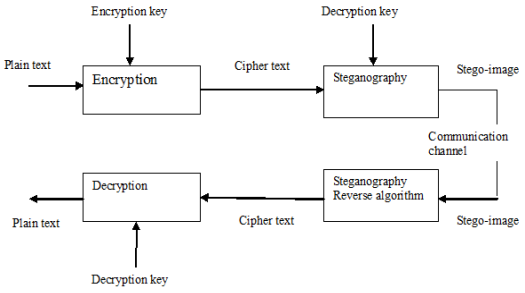

Fig.1. Hybrid Security Mechanism

Various researchers have tried to use several combinations of steganography and cryptography techniques but still there are chances for improvements. Therefore, in this paper a hybrid mechanism for security is proposed with the following objectives as follows:

- Peak signal to noise ratio should be high.
- Mean square and absolute error should be low.
- Perceptual quality of the image should be high.
- Time complexity should be low.
- Embedding capacity should be high.
- Intersection coefficient should be high.
- Embedded data should be robust.

Keeping in view all these goals, this paper is an effort to get optimum value of all the parameters. Organization of whole paper is as follows: Literature survey is described in section 2 along with problem definition on

hybrid mechanisms. Proposed scheme is described in Section 3. Analysis of proposed scheme is done in section 4, which is done using various performance metrics; these are security, robustness and efficiency analysis. Results are displayed in section 5. Overall conclusion is given in section 6. At last references are given.

II. LITERATURE SURVEY

Various techniques available in literature that make use of hybrid approach are given in Table 1. It can be easily observed from the literature survey that to have a good PSNR value, the best method is status bit [4] but this method has several drawbacks such as: the method use AES algorithm for encryption which has somewhat high time complexity making the process too slow. Also it has limited embedding capacity. We are of the opinion that the process chosen for cryptography should be strong but at the same time not too much time consuming. Therefore, we use vigenere cipher with slight modifications in it [10]. Also, to increase the embedding capacity [9], the use of Huffman encoding scheme is used which provides two benefits, firstly it increases the embedding capacity and secondly it can be treated as another encryption technique. The next section gives the proposed model.

Table 1. Literature Survey

Proposed by	Year of publication	Cryptography technique used	Steganography technique used	Advantage	Disadvantage
S.M. Masud Karim, et al. [13]	2011	Encryption using secret key	Modified LSB	Higher PSNR value Good security	High Time Complexity Secret key should be chosen properly
Gokul M., et al [11]	2012	Visual Cryptography	LSB	Low Time complexity	PSNR is very low because of use of visual cryptography
Shailender Gupta, et al. [8]	2012	RSA	LSB	Better Security	Limited Embedding Capacity High Time Complexity Message Size should be small
Mohammad A., et al. [28]	2012	Diffie Hellman	LSB	Better Security	Limited Embedding Capacity High Time Complexity Message Size should be small
R.Nivedhitha, et al. [1]	2012	DES	LSB	The mechanism is secure	High Time complexity than AES Limited Embedding Capacity
Ramakrishna Mathe, et al. [23]	2012	Diffie Hellman	LSB	Better Security	Limited Embedding Capacity High Time Complexity Message Size should be small
Md. Rashedul Islam, et al. [4]	2014	AES	LSB using Status bit	Good PSNR Can be used for large Messages	High Time complexity Limited Embedding Capacity
Pye Pye Aung,et al. [7]	2014	AES	DCT	Enhanced Security Can be used for large Message size	Distortion is high High Time complexity Limited Embedding Capacity
Shingote Parshuram N.,et al. [2]	2014	AES	LSB	Higher PSNR value Good security	High Time Complexity Limited Embedding Capacity

III. PROPOSED SCHEME

The complete flow chart for proposed hybrid technique is shown in Fig 2 below.

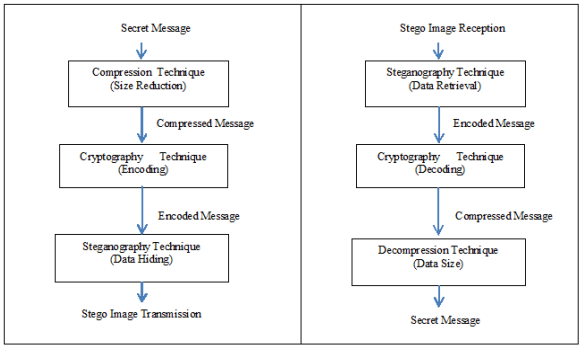

Fig.2. Proposed Hybrid Security Model

The proposed model first compresses the data using Huffman encoding scheme. This is used to increase the embedding capacity as well as it enhances the security level. The next step is to encrypt the encoded text using vigenere cipher. In this paper we modified the vigenere cipher also to increase the brute force search time which will be explained in the subsequent section. The last step is to use pseudo random LSB status bit steganography. This method has the advantage over simple plain LSB i.e. it is very difficult for the hacker to know about which pixel values contains the data and what sequence is used to combine it since hacker doesn't know about the seed value. The reverse process is carried out at the receiver side as shown in the Fig. 2. The details of each step are explained in the subsequent section.

A. Compression Technique

The purpose of using compression technique is to reduce the size of data to be transmitted so that amount of data to be hidden in the cover image gets increased. Huffman coding is used in this paper; it is a lossless data compression algorithm. As per this algorithm input characters are assigned variable-length codes. The lengths of the assigned codes are decided by calculating frequencies of corresponding characters.

First step in encoding process is to form dictionary, which requires two parameters; first is set of all characters and second is there probability of occurrence in the secret message. Then the secret message with the help of dictionary will be encoded. The characters with high frequency gets smallest code and characters with lowest frequency will get the largest code. The algorithm for the same is given below [9]: In data compression algorithm, firstly probability of all the symbols is calculated. *Symbols* are taken from 0 to 255.

Data Compression Algorithm

```
symbols=0:255;
prob_o=ones(1,length(symbols));
flag1=0;
for j=min(symbols):max(symbols)
for i=1:length(data)
if data(i)== j
flag1=flag1+1;
end
end
prob_o(j+1)=flag1/length(data);
flag1=0;
end
dict = huffmandict(symbols,prob_o);
hcode= huffmanenco(data,dict);
transmit=(hcode);
```

Data Decompression Algorithm

```
Receive=(hcode)
Data=secret data;
symbols=0:255;
prob_o=ones(1,length(symbols));
flag1=0;
for j=min(symbols):max(symbols)
for i=1:length(data)
if data(i)== j
flag1=flag1+1;
end
end
prob_o(j+1)=flag1/length(data);
flag1=0;
end
dict = huffmandict(symbols,prob_o);
dhsig= huffmandeco(hcode,dict);
decompressed data=dhsig;
```

Prob_o is the output matrix having size same as number of symbols. *Flag1* is variable used to count frequency of occurrence of each symbol. Two loops are used, range of first loop is includes all symbols and size of second loop is equal to data to be compressed. These two loops count number of times each symbol occurs in secret data and then its probability. With the help of function *dict* a dictionary is formed having two input parameters, set of all symbols and corresponding probability *{symbols, prob_o}*. Using function *huffmanenco* Huffman coding of data is obtained having secret data and dictionary as input parameters *{data,dict}*. *hcode* is final compressed data.

In data decompression algorithm input is compressed data *hcode*. In this process also first step is formation of dictionary which will be formed with *dict* function having two input parameters these are set of all symbols and matrix containing probability of all corresponding symbols in the compressed data*{symbols, prob_o}*. Finally, decompressed data is obtained with the help of function *huffmandeco* having compressed data and dictionary as input parameters *{hcode, dict}*. *Dhsig* is final decompressed data. The output obtained after the algorithm has less number of bits as compared to the original secret message. On receiver side, decompression is the last stage in which original secret message will be obtained by dictionary and compressed message.

B. Cryptography Technique

First layer of security is a cryptography technique. It is used to encode the message in such a form that can be safely moved on communication channel. In this paper vigenere cryptography technique is used because it is very simple, efficient and secure technique. Further, it is a polyalphabetic substitution cipher which uses two or more cipher alphabets. They have one to many correspondences between each letter and its substitutes. First step in this encoding process is to form a vigenere table which is as follows. In this table each row is formed by shifting cyclically the sequence of characters towards left. First row is formed by 0 step shifting, second by one step shifting, and third by two steps shifting and so on, this way complete table will be formed [10].

Vigenere table

```
symbols=0:255;
j=1;
for i=1:256
dict_vig(j)=char(symbols(i));
j=j+1;
end
ref=dict_vig;
m=length(ref);
i=1;
ref1(1,:)=ref;
for(i=2:1:m)
for(j=1:1:m-1)
ref1(i,j)=ref(j+1);
end
ref1(i,m)=ref(1);
ref=ref1(i,:);
 end
vigenere table=ref1;
```

In forming vigenere table set of all symbols is declared as variable having range from 0 to 255. First for loop converts all these symbols into characters named *dict_vig* or *ref* size is 256. This is taken as first row of the table. Then two loops are used to shift cyclically this row to form subsequent rows. One loop will form rows starting from second row and other loop will form columns position of this selected row having range one less than the number of elements in first row i.e. 255 so that first element of first row can be substituted as a last element of next row. This modified row is taken as reference row for shifting next row. This way the entire rows are shifted

and table is formed *ref1*.

Encryption Process

```
key=['Y' 'M' 'C' 'A' 'U' 'S' 'T'];
i=1;fv=0;
for(k=1:1:length(data))
d=data(k)-0;
t=k;
if k>length(key)
while t > length(key)
t=t-length(key);
end
end
k1=key(t)-0;
if d==0
d=d+1;
fv=fv+1;
end
data_eny(i)=ref1(d,k1);
i=i+1;
end
transmit =(data_eny, fv)
```

For encoding of data using vigenere cryptography Vigenere table as shown above and a key is required. This key will be of fixed size and value and will be shared by receiver and transmitter. Key taken in this paper is *['Y' 'M''C''A''U''S''T']*. Data to be encrypted is compressed data *data*. In this table character of keys are located column wise and character of data to be encoded are located row wise. As the data is to be encoded is larger than the number of characters of key. Thus repetition of key characters is used. In this algorithm combination of '*if*' and '*while*' loop is used for repetition the key characters. .Variable *fv* is used to keep track of number of times value of data encountered as 0 (as index value can't be 0) as it is incremented to form index and locate row element. Variable *d* gets characters of data one by one to locate row element and variable *k1* gets characters of key one by one to locate column element. Then, intersection of these two is encoded character *{d, k1}*. Thus, *data_eny* is final encoded data.

Decryption Process

```
Receive= (data_eny,fv,vigenere table)
key=['Y' 'M' 'C' 'A' 'U' 'S' 'T'];
for(k=1:1:length(data_eny))
t=k;
if k>length(key)
while t>length(key)
t=t-length(key);
end
end
k1=key(t)-0;
j=k1;
for i=1:1:length(ref1)
if ref1(i,j)==data_eny(k)
break;
end
end
dec(k)=ref1(i,2);
if fv > 0
if  double(dec(k))==1
dec(k)=dec(k)-1;
fv=fv-1;
end
end
end
decrypted data=dec;
```

For decryption of data three information are used *Vigenere table*, *Key* and variable *fv*. Length of key is shorter than data, so its repetition is done, *if* and *while* loops are used for this purpose. Variable *k1* is used to locate column in the table. Elements of encrypted data are located in the row of selected column. When selected using break loop will be terminated and corresponding element in the column is found which is encrypted data. Using *fv* variable correction in value of data is done. Finally, *dec* is decrypted data.

Table 2. Vigenere Table

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

C. *Steganography Technique*

In this paper second layer of security is introduced using steganography technique. It is a technique of hiding secret message in the cover image, so that its existence cannot be detected. There are many techniques available but widely used technique is LSB substitution, because it is simple to implement and also by modifying least significant bit in pixel value of the image matrix will not make any visual change in Image, thus data is secure. In this paper Pseudo-random LSB substitution technique is used which is modification in LSB substitution.

In pseudo-random LSB substitution technique pixels in which secret message bits are to be hidden are randomly located, so that it cannot be easily detected and retrieved. A seed is selected which is used to generate random numbers in the Image. At this randomly selected pixel secret bit is embedded [8, 21].

1) Embedding Algorithm

Step1. Get the secret message and convert it into binary form.

Step2. Get the cover image to which data is to embed.

Step3. Initialize the random key termed as seed, which is used to generate random locations in the cover image.

Step4. From first randomly identified pixel, MSBs of all three planes (red, green, blue planes) are collected and used to find out lightest, darkest and medium pixel of image.

Step5. Convert these MSBs into decimal number Dn. For lightest Dn=7, for darkest Dn=0 and when Dn=1, 2, 3, 4, 5 or 6 then pixel is medium.

Step6. If pixel is lightest or darkest then the secret message bit is embed into LSB of blue plane of the plane.

Step7. For medium pixel bit position of blue colour component on Dn is checked

```
If {(message bit = bit position of blue. plane)
    then
    LSB of blue plane=1
    else
    LSB of blue plane=0
  }
end
```

Step8. Number of Image pixels modified depends on the size of secret message bits.

Step9. Write Stego-Image.

Step10. Evaluation of stego-image is carried out based on various performance parameters.

2) Algorithm to retrieve secret message

Step1. Read stego-image.

Step2. Initialize the random key termed as seed, which is used to generate random locations in the cover image.

Step3. From first randomly identified pixel, MSBs of all three planes (red, green, blue planes) are collected and used to find out lightest, darkest and medium pixel of image.

Step4. If pixel is lightest or darkest then the LSB of blue plane is retrieved as a secret message bit.

Step5. For medium pixel bit position of blue colour component on Dn is checked

```
If {LSB of blue plane=1
    then
    message bit = bit position of blue. plane
    else
    message bit = complement of bit. position of blue plane
  }
end
```

Step6. Each group of eight bits is converted to bytes and then characters to get the required secret message.

IV. Simulation Setup

A. Performance Metrics

For complete analysis of the proposed scheme different parameters are used, which are divided into following categories [9, 27]:

1) Robustness Analysis: The parameters under this category measure the picture quality. Widely used parameters are:

1.1 Mean Absolute Error (MAE): The MAE represents the mean absolute error between the stego Image and the original image.

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

In the above formula, the mean absolute error is an mean value of the absolute errors,. where f is the pixel value of original image and y is the true value of stego image. Size of image is mxn monochrome image. For coloured images size of image will be mxnx3.

1.2 Mean Square Error (MSE): The MSE stands for cumulative squared error between the stego image and the original image. Lower the value of MSE means lower error. It is defined by the relation given below any m x n monochrome image.

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

For coloured image size of image will be m x n x 3.

1.3 Peak Signal Noise Ratio (PSNR): It is defined as the ratio of peak square value of pixels by mean square error (MSE). It is expressed in decibel. The PSNR is defined as:

$$PSNR = 10.\log_{10}(\frac{{MAX_I}^2}{MSE})$$

Where, MAX_I represents maximum value of pixel of the image. In the images with pixel having 8 bits per sample, its value is 255.

2) Security Analysis: The parameters under this category measure the closeness of stego-image and cover image. Widely used parameters are:

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:

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

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

ρ (A, B) is the correlation coefficient between image matrices A and B

cov (A,B) is the covariance between matrices A and B

$\sigma_A$is the standard deviation of A
$\sigma_B$is the standard deviation of B

2.2 Normalized Histogram Intersection Coefficient: This parameter gives count of the same value of pixels between two histograms. If the probability distribution of two images is taken as P and Q respectively, then Normalize Histogram Intersection coefficient is given by

$$I(A,B) = \sum_{i=1}^{N} \min\big(P(i), Q(i)\big)$$

Where A is cover image and B is stego image. The range of value for this coefficient is between 0 to1. Where 0 represents mismatch and 1 represents exactly match

2.3 Bhattacharyya Coefficient: This parameter gives approximate measure of amount of overlapping between two statistical samples which are two images in this case. In other words it measure the relative closeness between two images i.e. cover image and stego image. Bhattacharyya Coefficient is given as

$$BC(A,B) = \sum_{i=1}^{N} \sqrt{P(i)Q(i)}$$

Where P and Q are probability distributions of two images respectively i.e. cover image and stego image.

2.4 Universal Image Quality Index (UIQI): In an image, pixels values available at different positions shows different effect on Human Visual System (HVS). If some distortion or changes is introduced in the image, such distortion in image is calculated as a combination of three factors loss of correlation, contrast distortion and luminance distortion.

Luminance distortion, $L(A,B) = \frac{2\,\mu_A\mu_B}{{\mu_A}^2+{\mu_B}^2}$
Contrast distortion, $C(A,B) = \frac{2\sigma_A\sigma_B}{{\sigma_A}^2+{\sigma_B}^2}$
Loss of correlation, $S(A,B) = \frac{2\sigma_{AB}}{\sigma_A+\sigma_B}$

$$UIQI(A,B) = L(A,B) * C(A,B) * S(A,B)$$

Where A is cover image, μ_A and σ_A are mean and standard deviation, respectively of A. B is stego image, μ_B and σ_B is mean and standard deviation, respectively of B.

σ_{AB} is covariance between A and B.

3) Efficiency Analysis: The parameters under this category give the Qualitative measure of image and time required to accomplish the process. Widely used parameters are:

3.1 Time Complexity: It is defined as the total processing time on receiver side or receiver and transmitter side. In this paper comparison of time consumption by all receiver side processes is taken. 3.2 Qualitative Analysis: The cover image may undergo change in pixel values during embedding operation as a result of which the difference may observe in both the images. Thus qualitative visual analysis helps to observe any change in visual quality.

B. Simulation setup parameters

The set up parameters are shown in table 3 as follows

Table 3. Setup Parameters

Cover image pixel size (N x N x3)	N= 256, 384, 512, 640
Image type	.png
Simulation Tool	MATLAB 7.8.0.347
Pseudo Random Number Generator	MATLAB rng with seed= 256 Where rng=random number generator
Secret data for Steganography	“ABCDEFABCDEFABCD”
Image type	.png
Simulation tool	MATLAB 7.8.0.347 32 bit (win 32)
Vigenere Cryptography table size	256x256, characters of numbers 0 to255
Huffman encoding	No of symbols, n=256 Characters corresponding to numbers 0 to 255
Processor	Intel ®Core(TM) i3-3227U, CPU@1.90GHz, 400 GB, X64 based processor

V. Simulation Results

A. *Robustness Parameters Results Comparison*

1) Comparison of PSNR for Image1:

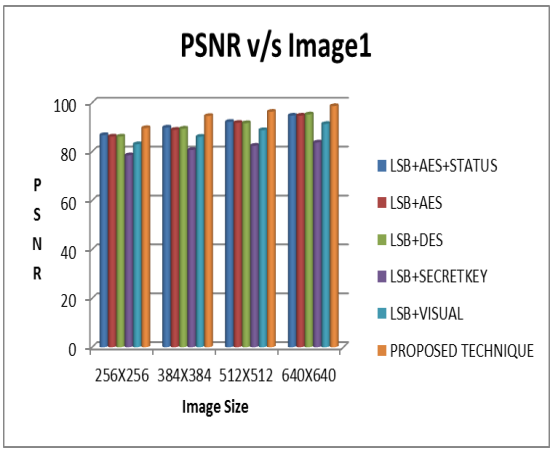

Fig.3. PSNR for Image1

2) Comparison of PSNR for Image2:

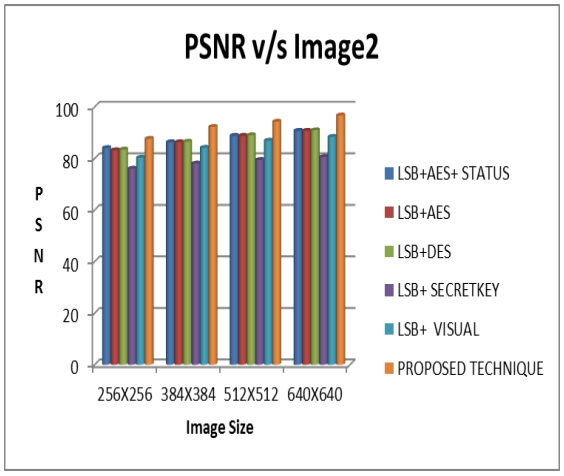

Fig.4. PSNR for Image2

3) Comparison of MAE for Image1:

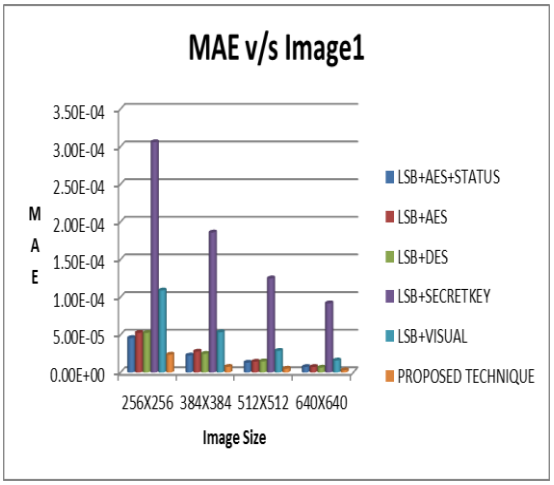

Fig.5. MAE for Image1

4) Comparison of MAE for Image2:

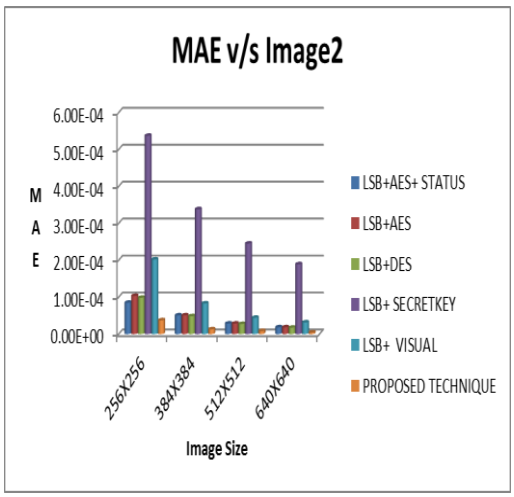

Fig.6. PSNR for Image2

5) Comparison of MSE for Image1:

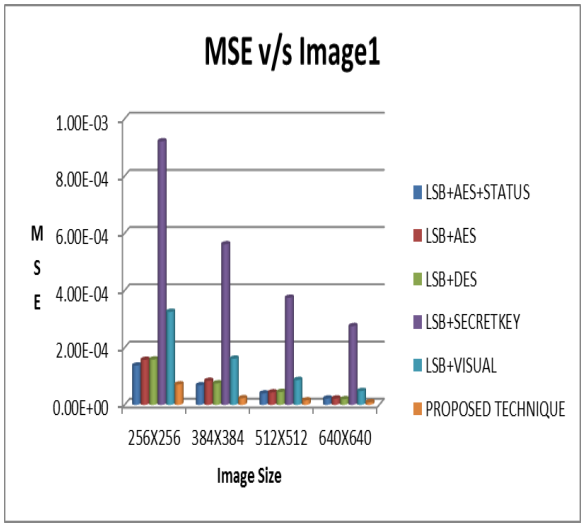

Fig.7. MSE for Image1

6) Comparison of MSE for Image2:

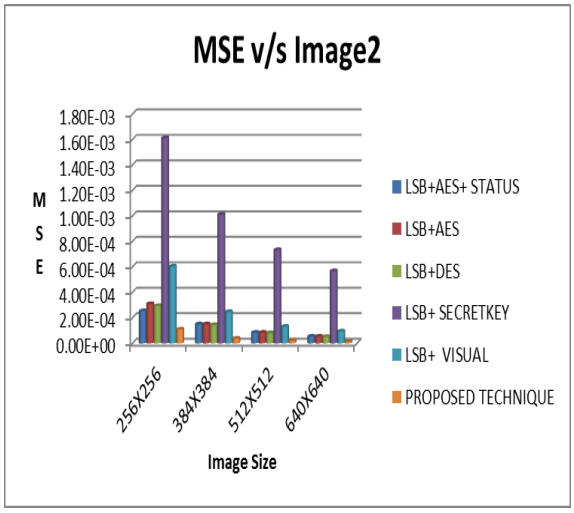

Fig.8. MSE for Image2

As seen from results of different parameters PSNR value is highest for proposed scheme as compared to available hybrid techniques. For different images and for different sizes of same images, value is highest. Similarly, MAE and MSE i.e. mean squared and absolute error values are smallest amongst all techniques. Thus, as per these results proposed technique is highly robust. It is also seen that as the image size increases, PSNR increases since the secret message is same for all the image size. The steganography technique used is Pseudo-random LSB, which will also decrease the possibility of data detection due to random nature of data insertion.

B. Security Comparison Results

1) Comparison of Intersection Coefficient for Image1:

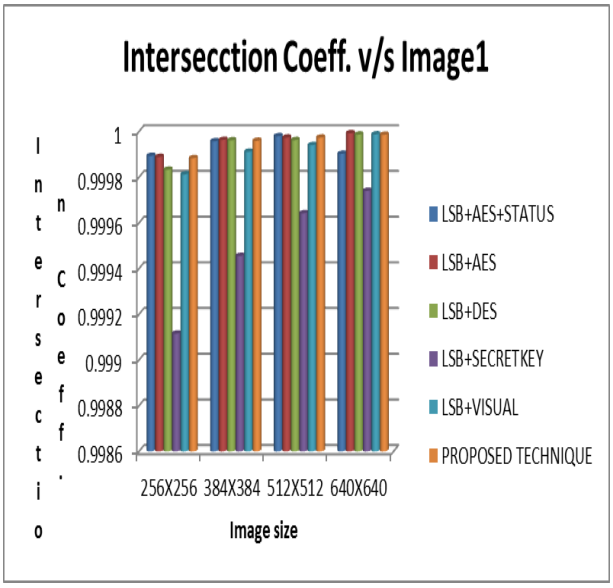

Fig.9. Intersection Coeff. for Image1

2) Comparison of Intersection Coefficient for Image2:

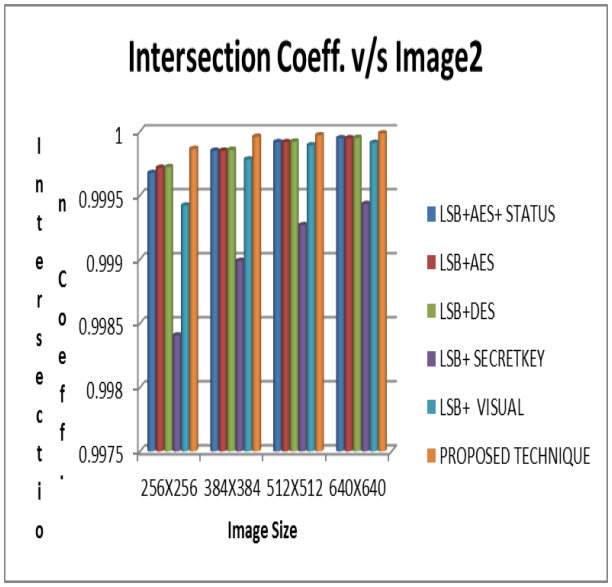

Fig.10. Intersection Coeff. for Image2

3) Comparison of Bhattacharya Coefficient for Image1:

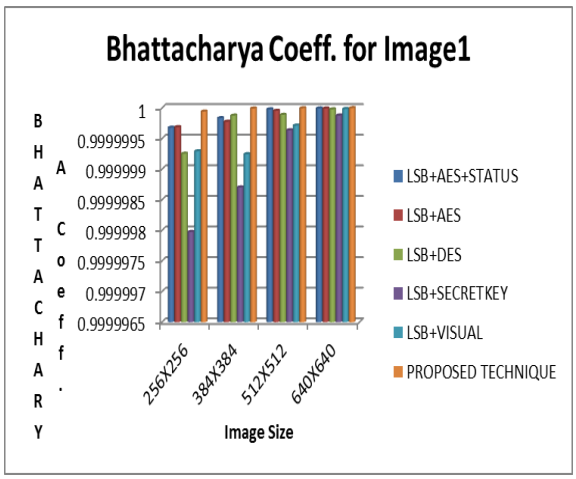

Fig.11. Bhattacharya Coeff. for Image1

4) Comparison of Bhattacharya Coefficient for Image2:

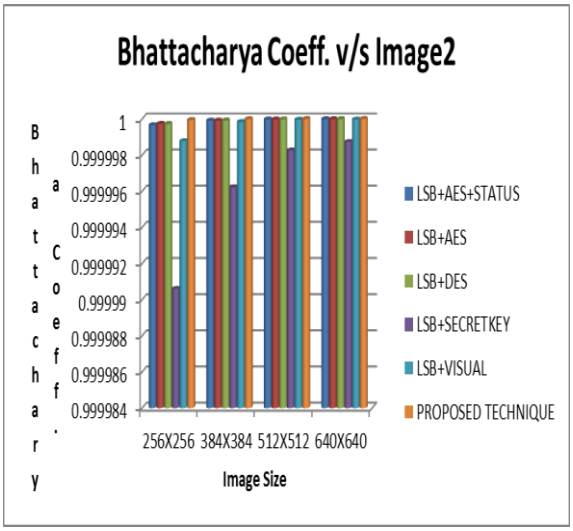

Fig.12. Bhattacharya Coeff. for Image2

5) Comparison of UIQI for Image1:

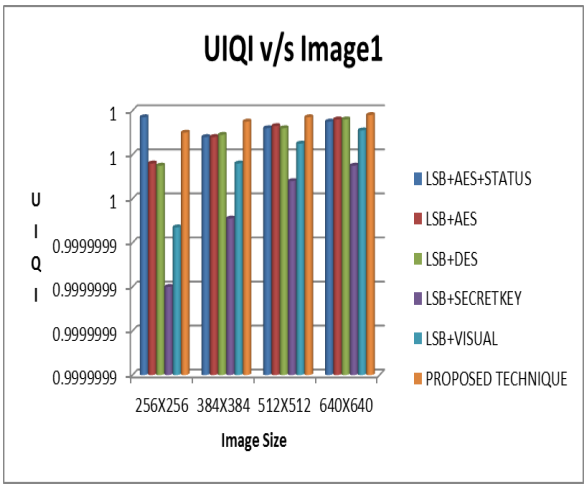

Fig.13. UIQI for Image1

6) Comparison of UIQI for Image2:

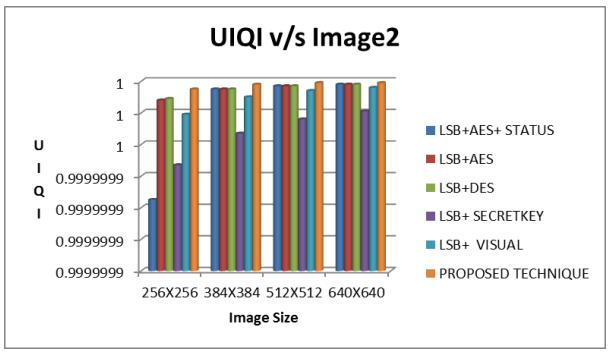

Fig.14. UIQI for Image2

7) Comparison of Correlation Coefficient for Image1:

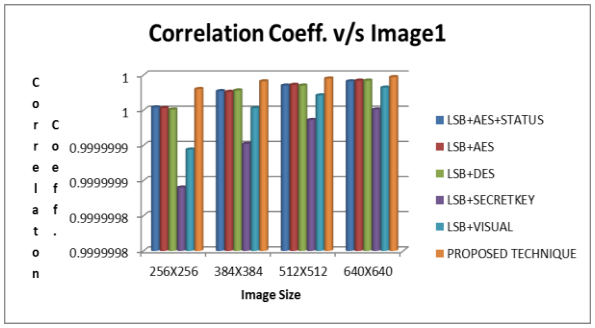

Fig.15. Correlation Coeff. for Image1

8) Comparison of Correlation Coefficient for Image2:

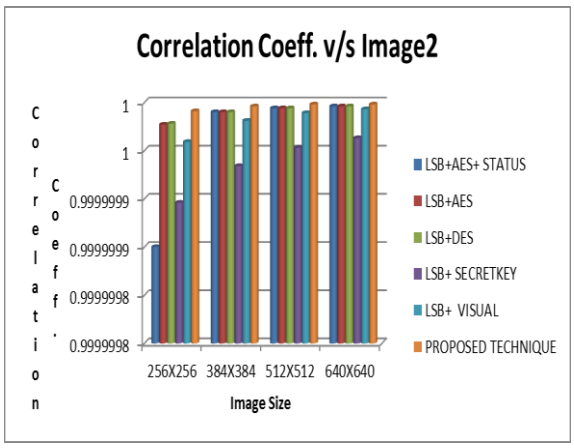

Fig.16. Correlation Coeff. for Image2

These security parameters are the measure of closeness of resultant image with cover image. As per results values of all the parameters for proposed scheme is approaching 1 (perfect matching). The stego-image is very close to cover image, due to this it is extremely difficult for an intruder to detect presence of secret message in image, and thus information is secure.

C. Efficiency comparison results

1) Qualitative Analysis (Snapshots):

Original Image	LSB+status+AES	LSB+AES	Proposed Technique
			
LSB+DES	LSB+Secret Key	LSB+Visual	
			

Fig.17. Snapshots for Image2 (384x384)

Fig.18. Snapshots for Image1 (256x256)

2) Comparison of Time Complexity for image1:

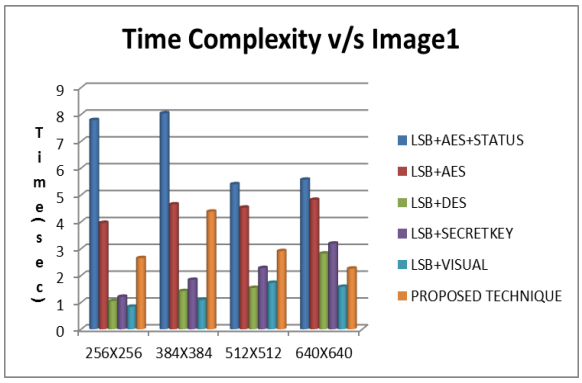

Fig.19. Time Complexity for Image1

3) Comparison of Time Complexity for Image2:

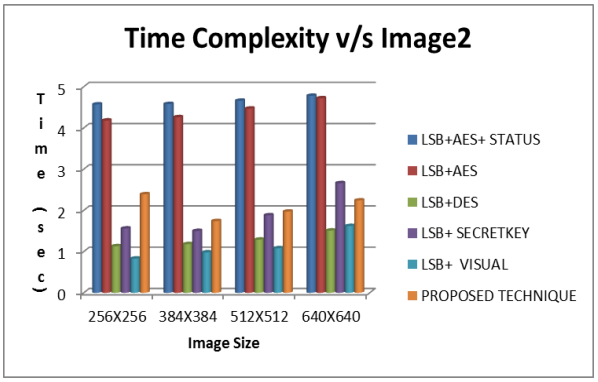

Fig.20. Time Complexity for Image2

As per results of qualitative analysis, it is not possible to identify the presence of any type of information in the image. While visual inspection both images are seems to be alike. Time complexity of proposed technique is also very low, because we have used vigenere cryptography, which is a matching process having very low time complexity. But due to employing pseudo-random LSB technique instead of LSB, time requirement has increased from some techniques like technique using LSB. That too is not very significant.

VI. CONCLUSION

The technique proposed in this paper is a hybrid technique, which has increased the layers of security in overall system. Along with cryptography and steganography Huffman compression is also used. Due to introduction of this feature system will not only become robust and more efficient but its embedding capacity will also increase. This technique is better than available techniques in all aspects.

- As per the results proposed technique is more robust, high PSNR and low MSE and MAE values gives this information.
- Embedding capacity is increased due to inclusion of Huffman compression technique.
- Brute force search time is increased because of inclusion of vigenere cryptography symmetric table having all the symbols corresponding to numbers 0 to 256. Also being matching process its time complexity is low.
- Pseudo-random status steganography increases robustness. Also data can be embedded in entire blue plane.
- This steganography technique increases time complexity in comparison to certain available techniques, but that too is very marginal, so cannot be considered as any overhead. This can be verified from the results of time complexity.

- Overall conclusion is that proposed technique is introducing more secure environment as compared to available techniques without much overhead.

Table 4. Overall Conclusion Table

Parameters	LSB+AES+ STATUS	LSB+AES	LSB+DES	LSB+ SECRETKEY	LSB+ VISUAL	PROPOSED TECHNIQUE
Robustness	2	4	3	6	5	1
Security	1	2	2	4	3	1
Perceptual quality	2	4	3	6	5	1
Embedding capacity	3	2	2	2	2	1
Time Complexity	6	5	2	3	1	4

Where 1 to 6 indicates high to low performance. *1-Very Good, 2-Good, 3-Moderate, 4-Moderate, 5-Above Least, 6-Least.*

REFERENCES

[1] R.Nivedhitha, Dr.T.Meyyappan, "Image Security Using Steganography and Cryptographic Techniques" in International Journal of Engineering and Technology Vol. 3, Issue 3, pp 366-371, 2012.

[2] Shingote Parshuram N., Syed Akhter Hussain and Bhujbal Pallavi M., "Advanced Security Using Cryptography and LSB Matching Steganography" in International Journal of Computer and Electronics Research Vol. 3, Issue 2, pp 52-55, 2014.

[3] Moumita Pramanaik, Kalpana Sharma, "Analysis of Visual Cryptography, Steganography Schemes and its Hybrid Approach for Security of Images" in International Journal of Emerging Technology and Advanced Engineering, Vol.6, Issue 2, pp 174-178, 2014.

[4] Md. Rashedul Islam, AyashaSiddiqa, Md. Palash Uddin, Ashis Kumar Mandal and Md. Delowar Hossain, "An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography" in proceedings of 3rd International Conference On Informatics, Electronics & Vision, pp 1-6, 2014.

[5] Abdul-Gabbar Tarish Al-Tamimi, Abdulmalek Abduljabbar Aloqobaty, "Image Steganography Using Least Significant Bits (LSBs): A Noval Algorithm" in International Journal of Computer Science and Information Security, Vol. 13, No. 1, pp 1-5, 2015.

[6] K.P.Uday Kanth, D.Vidyasagar, "An Effective Implementation of LSB Steganography Using DWT Techniques" in proceedings of 10th IRF International Conference, Chennai, pp 1-3, 2014.

[7] Pye Pye Aung, Tun Min Naing, "A Noval Secure Combination Technique of Steganography and Cryptography" in International Journal of Information Technology, Modelling and Computing, Vol. 2, No. 1, pp 55-62, 2014.

[8] Surbhi Singhania, Shailender Gupta, Bharat Bhushan and Ajay Nain, "A Novel Crypt-Stego Technique for Information Security in Communication Networks" in International Journal of Signal Processing, Image Processing and Pattern Recognition, Vol. 6,No. 2, pp 87-102, 2013.

[9] Pratishtha Gupta, G.N Purohit and Varsha Bansal, "A Survey on Image Compression Techniques" in International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 8, pp 7762-7768, 2014.

[10] Quist-Aphetsi Kester, "A cryptosystem based on Vigenère cipher with varying key" in International Journal of Advanced Research in Computer Engineering & Technology, Vol. 1, Issue 10, pp 108-113, 2012.

[11] Gokul.M, Umeshbabu R, Shriram K Vasudevan and Deepak Karthik, "Hybrid Steganography Using Visual Cryptography and LSB Encryption Method" in International Journal of Computer Applications, Vol. 59, No. 14, pp 5-8, 2012.

[12] Shailender Gupta, Ankur Goyal and Bharat Bhushan, "Information Hiding using Least Significant Bit Steganography and Cryptography" in I.J. Modern Education and Computer Science, Vol. 6, pp 27-34, 2012.

[13] S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain, "A New Approach for LSB Based Image Steganography using Secret Key" in Proceedings of 14th International Conference on Computer and Information Technology, pp 22-24, 2011.

[14] Sujay Narayan, Gaurav Prasad., "Two New Approaches for Secured Image Steganography Using Cryptographic Techniques and Type Conversions" in Signal & Image Processing: An International Journal, Vol. 1, No. 2, pp 60-73, 2010.

[15] Piyush Marwaha, Paresh Marwaha, "Visual Cryptographic Steganography in Images" in proceedings of Second International conference on Computing, Communication and Networking Technologies, pp 1-6, 2010.

[16] Zaidoon Kh.Al-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan.O.Alanazi, "Overview: Main Fundamentals for Steganography" in Journal of Computing, Vol. 2, Issue 3, pp 158-165, 2010.

[17] XIE Qing, XIE Jianquan and XIAO Yunhua, "A High Capacity Information Algorithm In Color Image" in IEEE, 2010.

[18] A.Joseph Raphael, V.Sundaram, "Cryptography and Steganography - A Survey" in International Journal of Computer Technology Application, Vol. 2, Issue 3, pp 626-630, 2011.

[19] "Cryptography and Network Security: principles and practices", William Stallings, Pearson education, first Indian reprint 2003.

[20] Zhou Wang, Alan C. Bovik, "A Universal Image Quality Index" IEEE Signal Processing Letters, Vol. 9, No. 3, pp. 81-84, 2002.

[21] Md. Jakir Hossain, "Information-Hiding Using Image Steganography With Pseudorandom Permutation" in Bangladesh Research Publications Journal, Vol. 9, Issue 3,

pp 215-225, 2014.
[22] S Usha, G A Satish Kumar and K Boopathybagan, "A Secure Triple Level Encryption Method Using Cryptography and Steganography" in proceedings of International Conference on Computer Science and Network Technology, pp 1017-1020, 2011.
[23] Ramakrishna Mathe, Veera RaghavRao Atukuri and Srinivasa Kumar Devireddy, "Securing Information: Cryptography and Steganography" in International Journal of Computer Science and Information Technologies, Vol. 3, Issue 3, pp 4251-4255, 2012.
[24] Lokesh Kumar, "Novel Security Scheme for Image Steganography using Cryptography Technique" in International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, Issue 4, pp143-146, 2012.
[25] Zhi Zhou, Ghonzalo R. Arce, Giovanni Di Crescenzo, "Halftone Visual Cryptography" in IEEE Transactions on Image Processing, Vol.15, No. 8, pp 2441-2453, 2006.
[26] Hossein Sheisi, Jafar Mesgarian and Mostafa Rashmani, "Steganography: DCT Coefficient Replacement Method and Compare With JSteg Algorithm" in International Journal of Computer and Electrical Engineering, Vol. 4, No. 4, pp 458-462, 2012.
[27] V.Asha, P.Nagabhushan, N.U.Bhajantri, "Similarity measures for Automatic defect detection on patterned textures", International journal of Image processing and vision sciences, Vol. 1, Issue 1, pp 18-24, 2012.
[28] Mohammad, A. A., and Abdel Fatah, "Public-Key Steganography Based on Matching Method" in European Journal of Scientific Research, pp 223-231, 2012.

Authors' Profiles

Ms. Sangeeta Dhall is Assistant Professor in Electronics department at YMCA university of Science and Technology. Her interest includes image processing and Embedded system design.

Mr. Bharat Bhushan is B.Tech (Electronics Engineering), M.Tech (Electronics Engineering). His academic interests include network security, Embedded System. Currently working as Assistant Professor in Electronics Engineering department at YMCA University of Science and Technology, Faridabad, India.

Dr. Shailender Gupta is B.Tech (Electronics Engineering), M.Tech (Computer Engineering) and recieved his Ph. D in the area of ad-hoc mobile network security. His academic interests include network security, Signal Processing, automata theory and fuzzy logic. Currently working as Assistant Professor in Electronics Engineering department at YMCA University of Science and Technology, Faridabad, India.

How to cite this paper: Sangeeta Dhall, Bharat Bhushan, Shailender Gupta,"An Improved Hybrid Mechanism for Secure Data Communication", International Journal of Computer Network and Information Security(IJCNIS), Vol.8, No.6, pp.67-78, 2016.DOI: 10.5815/ijcnis.2016.06.08

