IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

A Hybrid Scheme for Cryptography and Watermarking

Amandeep Kaur[1], Rajbir Kaur[2]

Electronics and Communication Engineering, Punjabi University, Patiala, Punjab, India[1]

Assistant Professor, Electronics and Communication Engineering, Punjabi University, Patiala, Punjab, India[2]

Abstract: With the rapid development the computer network, data has been an exchange in the form of text, image, audio and video, hence securing of all type of data is most necessary in today's era. To enhance security and copyright protection of digital data, we are implementing a hybrid scheme for cryptography and watermarking. In this scheme, the message divided the five different parts and encrypts them with the Fibonacci series, XOR cipher, PN sequence, RSA, Hill cipher. After obtaining the encrypted data, this data is hide using one bit LSB watermarking, two bit LSB watermarking and three bit LSB watermarking. This paper also represents the comparative analysis of one bit LSB watermarking, two bit LSB watermarking and three bit LSB watermarking.

Keywords: Encryption, Decryption, Cryptography, LSB, Watermarking, Fibonacci series, PN sequence, XOR cipher, RSA, Hill cipher, Hybrid technique.

I. INTRODUCTION

In the rapid growth of the multimedia technologies, digital data such as texts, images, videos, and audios have been expansively exploited in our everyday life. The process of the digital data makes human lives extra suitable. People can broadcast broadly data via computer networks. However, the security of the computer networks has been not enough, and the transmitted data could be captured by an illegal user. Therefore, how to ensure the digital data to be securely transmitted via the Internet is an important issue. Cryptography and digital watermarking are similar in the way that they both are used to protect essential information.

Cryptography is a process to convert plaintext into the cipher text using the secret key. These are two types cryptography algorithm such as conventional key cryptography and public key cryptography. Conventional key cryptography, the one key is used in both encryption and decryption process. These are different types of conventional key cryptography algorithms such as Data encryption standard (DES), Advanced encryption standard (AES), Fibonacci series, PN sequence and XOR cipher etc. Public key cryptography the different but related pair of the secret key is used in both encryption and decryption process. These are the different type of public key cryptography algorithms such as RSA, Hill cipher and Elliptic curve cryptography (ECC).

Digital watermarking is a science of hiding information invisible in the cover image. Digital watermarking is to hide the enormous existence of the message in the cover image.
Digital watermarking used to hide the information within the host image, which cannot able to be retrieved by the third party. These are two types digital watermarking algorithms such as spatial domain and frequency domain. Spatial domain technique applied in the pixels value of the primary image.
LSB and ISB are two techniques the spatial domains. In LSB technique pixels value of primary data inserts in the least significant bits of the cover image. Frequency domain technique applied into frequency coefficients of primary data. Discrete
Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) are techniques the frequency domain [6, 11].

II. PROPOSED METHODOLOGY

The data is passed through a series of mathematical operation, that generate an alternate form of that data is called encryption. The sequence of these operations is called algorithm. The unencrypted data is called plaintext and encrypted data as cipher text. The security of encryption depends on the capability of an algorithm to produce cipher text that is not easily recovered to the plaintext.

As we have obverse the single encryption methods are easy to decrypt once the secret key or logic is known to the third party, so in order to the enhance security of the data, we are used to the combination of different cryptography algorithms and LSB watermarking.

For example, if we take the input to be "The symmetric and asymmetric techniques", this message divided the five different parts and encrypts them with the five different cryptography algorithm as shown in figure 1.the encrypted data is hidden by the three different LSB watermarking algorithms.

DOI 10.17148/IJARCCE.2016.5737

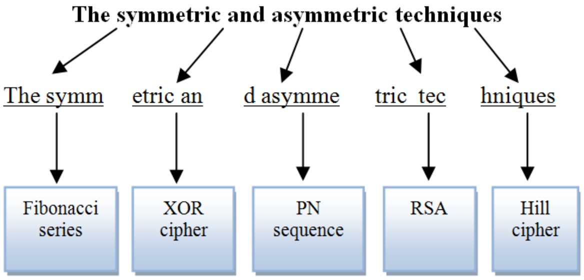

Figure 1: Representation of data splitting

The input data is segregated the five different parts. If the length of the input data is 39 characters, then the first 8 characters are encrypted using Fibonacci series. The next 8 characters are encrypted using XOR cipher. The next 8 characters are encrypted using PN sequence. The next 8 characters are encrypted using RSA and remaining 7 characters are encrypted using Hill cipher.

1. Encryption algorithm

1. Select a spring input message.
2. Segregate the message into five different parts.
3. Fibonacci series applied the first part of the message.
4. XOR cipher applied the second part of the message.
5. PN sequence applied the third part of the message.
6. RSA algorithm applied the fourth part of the message.
7. Hill cipher applied the fifth part of the message.
8. After used these algorithms message is concatenated and encrypted message obtain to output.
9. Select the host image.
10. One bit LSB watermarking, two bit LSB watermarking and three bit LSB watermarking are utilized to hide the encrypted message.
11. Calculated the parameters such as PSNR, MSE and RMSE.

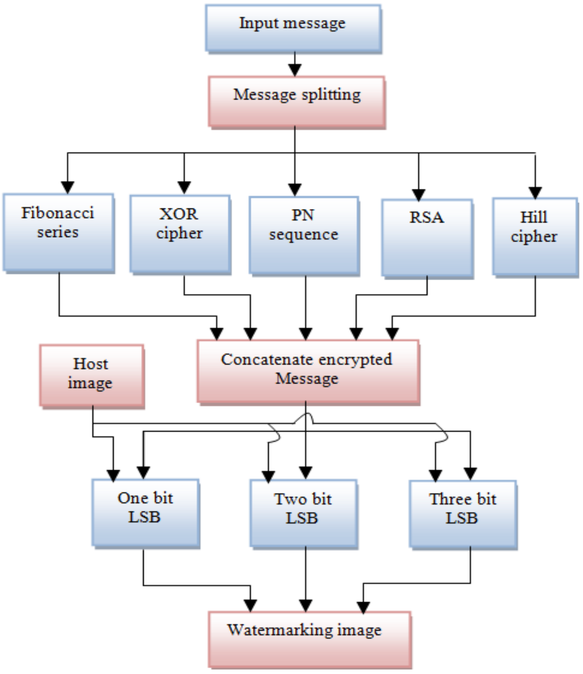

Figure 2: Block diagram of encryption

Figure 2 shows the block diagram of the hybrid technique of cryptography and LSB watermarking in encryption. While the data is encrypt used the five cryptography algorithms and encrypted data is hide by the three different LSB watermarking. The same cryptography algorithms and key is used to decrypt the cipher text at receiver side as shown in figure 3.

2. Decryption algorithm

1. One bit LSB watermarking, two bit LSB watermarking and three bit LSB watermarking are utilized to the watermarked image.
2. To employ the one bit LSB watermarking, two bit LSB watermarking and three bit LSB watermarking to obtain the encrypted message.
3. Segregate the encrypted message into five parts that are same as the encryption.
4. Fibonacci series applied the first part of the message.
5. XOR cipher applied the second part of the message.
6. PN sequence applied the third part of the message.
7. RSA algorithm applied the fourth part of the message.
8. Hill cipher applied the fifth part of the message.
9. After applied these algorithms message is concatenated and original message obtains to output.

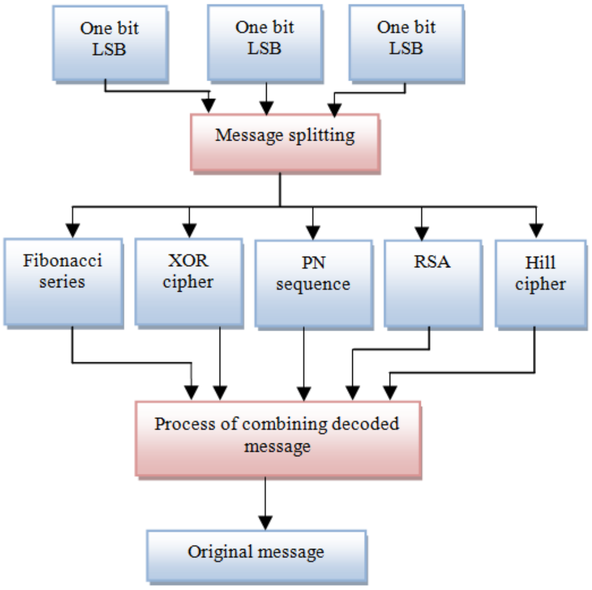

Figure 3: Block diagram of decryption

A. Fibonacci series

1. Procure the message.
2. Convert the character into ASCII value.
3. Generate the Fibonacci series.
4. Add the ASCII value into the Fibonacci series in the encryption.
5. Subtract the ASCII value into the Fibonacci series in the decryption.
6. Convert the ASCII value into the character.

B. XOR cipher

1. Procure the message.
2. Convert the character into ASCII value.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

3. Convert the ASCII value into the binary value.
4. Generate the secure key.
5. XOR operation is utilized to secure key and binary value.
6. Convert the binary value into the character.

C. PN sequence
1. Procure the message.
2. Convert the character into ASCII value.
3. Generate the PN sequence.
4. Add the ASCII value into the PN sequence in the encryption.
5. Subtract the ASCII value into the PN sequence in the decryption.
6. Convert the ASCII value into the character.

D. RSA
1. Select two random prime numbers p and q.
2. Calculate the value of Pk = p x q.
3. Calculate the value of phi = (p - 1) x (q -1).
4. Calculate the encryption key e using while loop

```
x=2;e=1;
while x > 1
e=e+1;
x=gcd(Phi,e);
end
```

5. Calculate the decryption key d using e and Phi (dxe)%Phi=1
6. Generate the cipher text S operate the following method
   Cipher text $S = M^e \operatorname{Mod}(n)$
7. Generate the plaintext M operate the following method

Plaintext $M = S^d \operatorname{Mod}(n)$

E. Hill cipher
1. Procure the message.
2. Select the square 2x2 matrix.
3. Group the plaintext into pairs.
4. Convert each pair of character into vectors value.
5. Generate the cipher text C operate the following method C = PK mod M
6. Generate the plaintext P operate the following method

$P=CK^{-1}$mod M

F. Least Significant Bit (LSB)
1. Select the cover image.
2. Read the cover image.
3. Defines the value of three primary colors in the cover image.
4. Calculate the size of the cover image.
5. Convert the encrypted message into double.
6. Rotate the binary value.
7. Calculate the size of the encrypted message.
8. Set the LSB bit of the cover image (ii, jj) according to the message in the encryption.
9. Display the watermarked image.
10. Pick up the LSB bit of the cover image (ii, jj) according to the encrypted message.
11. Convert the binary value into characters.

III. EXPERIMENTAL RESULTS

Analysis using several host images and its different message has done in MATLAB. The host images are 512x512 sizes in shown figure 4.

Waterfall.jpg World security.jpg

Globe.jpg Security key.jpg

Golden temple.jpg

Figure 4: Various host Images

Table1. Original text and cipher text

No of bit	Original text	Cipher text
136	Trust human being	Tsv vq%m zwp !b > $H:
200	Maximum character encoded	Mbyk hph%f mk • u , >1 +@aV3w=
256	Businesspeople life professional	Bvtkqj vvu`ju qo/ , „ 1-w>P 9;JT.e
312	The symmetric and asymmetric techniques	Tif"v~uz `qwlf%dk i*p‡’ <‡¡ 1v,b • >,[Z1$L5a
400	Uniform distribution provided described techniques	Uojhrwu-y vqwpgpqlj s* ‡ˆ ”ŒE ’-† d>P,1v >d x6SbZ1$L5a

A. Evaluation Of Image Quality
We calculate the quality of watermarked images in terms of MSE (Mean Square Error), RMSE (Root Mean Square Error) and PSNR (Peak Signal to Noise Ratio). In imaginary case, PSNR should be finite and MSE should be zero. In virtual case, PSNR is large and MSE is small.

DOI 10.17148/IJARCCE.2016.5737

1) MSE
Mean square error can be calculated using formula

$$\mathrm{MSE} = \frac{\sum \mathrm{M,N}[\mathrm{I}_1(\mathrm{m,n}) - \mathrm{I}_2(\mathrm{m,n})]^2}{\mathrm{M} * \mathrm{N}}$$

Where I_1 (m, n) is the host image and I_2 (m, n) is the watermarked image, M and N are the numbers of rows and columns in the host image.

2) PSNR
Peak Signal to Noise Ratio can be calculated using formula

$$\mathrm{PSNR} = 10 \log_{10}\left[\frac{\mathrm{R}^2}{\mathrm{MSE}}\right]$$

Where R is the maximum fluctuation or values the images.

3) RMSE
Root Mean Square Error can be calculated using formula

$$\mathrm{RMSE} = \sqrt{\mathrm{MSE}}$$

Table 2 shows MSE of one bit LSB, two bit LSB and three bit LSB of five different host images with five different messages. Figure 5 shows the graph of comparison MSE of one bit LSB, two bit LSB and three bit LSB. Table 3 shows PSNR of one bit LSB, two bit LSB and three bit LSB of five different host images with five different messages. Figure 6 shows the graph of comparison PSNR of one bit LSB, two bit LSB and three bit LSB. Table4 shows RMSE of one bit LSB, two bit LSB and three bit LSB of five different host images with five different messages. Figure 7 shows the graph of comparison RMSE of one bit LSB, two bit LSB and three bit LSB.

Table2. MSE for Different Bit Substitution

Image name	Message length in character	No of bit	One bit LSB	Two bit LSB	Three bit LSB
			MSE	MSE	MSE
Waterfall	17	136	2.40E-04	9.57E-04	2.30E-03
	25	200	2.82E-04	1.30E-03	2.90E-03
	32	256	3.36E-04	1.50E-03	3.40E-03
	39	312	3.85E-04	1.70E-03	3.20E-03
	50	400	4.46E-04	2.40E-03	4.20E-03
World	17	136	2.98E-04	9.04E-04	4.40E-03
	25	200	4.01E-04	9.68E-04	5.00E-03
	32	256	4.39E-04	1.80E-03	6.10E-03
	39	312	5.19E-04	1.70E-03	7.60E-03
	50	400	6.10E-04	2.30E-03	7.80E-03
Globe	17	136	3.59E-04	1.90E-03	7.60E-03
	25	200	4.46E-04	2.20E-03	9.80E-03
	32	256	5.31E-04	2.30E-03	1.13E-02
	39	312	6.18E-04	2.40E-03	1.22E-02
	50	400	7.25E-04	2.90E-03	1.27E-02
Security key	17	136	4.04E-04	1.90E-03	7.60E-03
	25	200	4.88E-04	2.20E-03	9.80E-03
	32	256	5.80E-04	2.50E-03	1.14E-02
	39	312	7.75E-04	2.70E-03	1.25E-02
	50	400	8.81E-04	2.90E-03	1.15E-01
Golden temple	17	136	1.95E-04	1.00E-03	3.90E-03
	25	200	2.40E-04	1.20E-03	5.00E-03
	32	256	3.32E-04	1.50E-03	5.00E-03
	39	312	4.46E-04	1.90E-03	4.70E-03
	50	400	6.37E-04	2.10E-03	6.93E-02

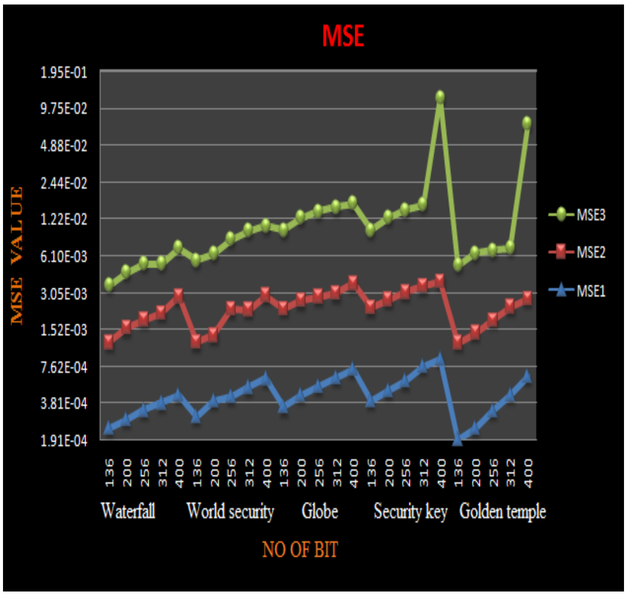

Figure 5: MSE comparison graph for Different Bit Substitution

Table3. PSNR for Different Bit Substitution

Image name	Message length in character	No of bit	One bit LSB	Two bit LSB	Three bit LSB
			PSNR	PSNR	PSNR
Waterfall	17	136	84.3228	78.3195	74.4487
	25	200	83.6239	76.8385	73.5425
	32	256	82.8714	76.3833	72.8274
	39	312	82.273	75.8522	72.0425
	50	400	81.6343	74.4134	71.9221
World security	17	136	83.3953	78.5687	71.7206
	25	200	82.1043	78.2679	71.1601
	32	256	81.7092	75.6886	70.2886
	39	312	80.2211	75.0015	69.3124
	50	400	80.1750	74.6077	69.1881
Globe	17	136	82.5849	75.4231	69.3037
	25	200	81.6343	74.8034	68.2287
	32	256	81.1105	74.4204	67.6265
	39	312	80.2211	74.3297	67.552
	50	400	79.5387	73.5425	67.0761
Security key	17	136	82.0631	75.4231	68.3037
	25	200	81.2441	74.6298	68.2287
	32	256	80.4978	74.1871	67.5435
	39	312	79.3936	73.7489	67.1721
	50	400	78.6801	73.4853	66.7820
Golden temple	17	136	85.2405	77.9387	72.1794
	25	200	84.3228	77.1840	71.1835
	32	256	82.9210	76.4616	71.1302
	39	312	81.6343	75.3439	70.4242
	50	400	80.0890	74.9126	69.3194

Table4. RMSE for Different Bit Substitution

Image name	Message length in character	No of bit	One bit LSB	Two bit LSB	Three bit LSB
			RMSE	RMSE	RMSE
Waterfall	17	136	0.0155	0.0309	0.0483
	25	200	0.0168	0.0367	0.0536
	32	256	0.0183	0.0387	0.0583
	39	312	0.0196	0.0411	0.0598
	50	400	0.0211	0.0485	0.0646
World security	17	136	0.0172	0.0301	0.0661
	25	200	0.0200	0.0311	0.0706
	32	256	0.0209	0.0419	0.0780
	39	312	0.0228	0.0429	0.0873
	50	400	0.0247	0.0474	0.0885
Globe	17	136	0.0189	0.0432	0.0874
	25	200	0.0211	0.0464	0.0989
	32	256	0.0224	0.0485	0.1041
	39	312	0.0249	0.0490	0.1057
	50	400	0.0269	0.0536	0.1129
Security key	17	136	0.0201	0.0432	0.0874
	25	200	0.0221	0.0473	0.0989
	32	256	0.0241	0.0498	0.1070
	39	312	0.0273	0.0524	0.1170
	50	400	0.0297	0.0540	0.1188
Golden temple	17	136	0.0139	0.0323	0.0597
	25	200	0.0155	0.0353	0.0604
	32	256	0.0182	0.0383	0.0608
	39	312	0.0211	0.0436	0.0684
	50	400	0.0252	0.0458	0.0693

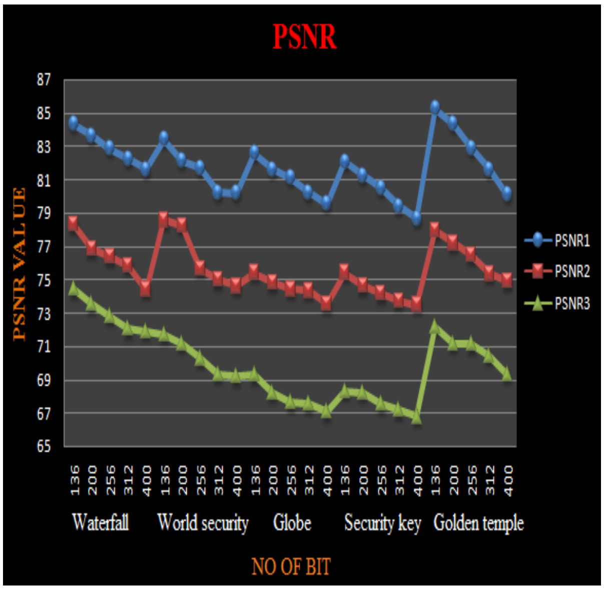

Figure 6: PSNR comparison graph for Different Bit Substitution

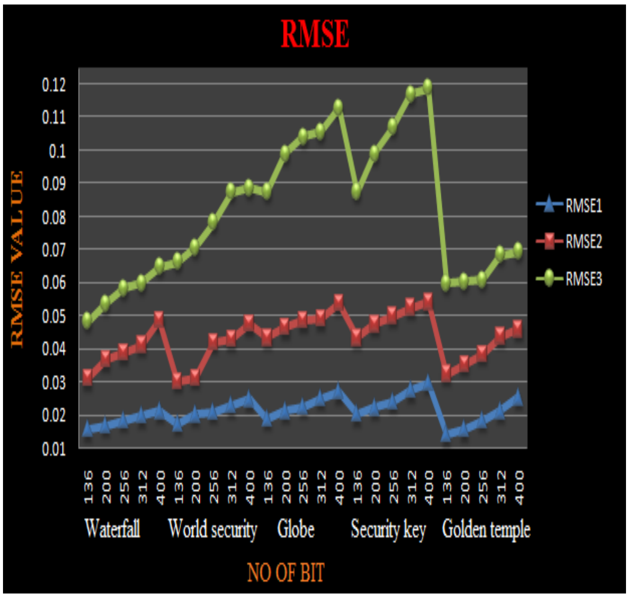

Figure 7: RMSE comparison graph for Different Bit Substitution

DOI 10.17148/IJARCCE.2016.5737

IV. CONCLUSION

This paper represents the hybrid scheme for cryptography and watermarking. The security of the data is increased which is used the five cryptography algorithms to encrypted the data. After encrypted the data, LSB techniques are used to embed encrypted data in the host image. This paper also gives the comparison between the one bit LSB, two bit LSB and three bit LSB. This paper also calculates the image quality measure by using the MSE, RMSE and PSNR between the one bit LSB, two bit LSB and three bit LSB.

REFERENCES

[1] Rohit Minni, Kaushal Sultania, Saurabh Mishra, Prof Durai Raj Vincent PM "An Algorithm to Enhance Security in RSA" VIT University, IEEE ICCCNT 2 July, 2013, Tiruchengode, India, 31661.

[2] Gurpreet Kaur, Kamaljit Kaur "Implementing LSB on Image Watermarking Using Text and Image" Sri Guru Granth Sahib World University, Fatehgarh, Vol. 2, Issue 8, August 2013.

[3] Udepal Singh, Upasna Garg "An ASCII value based text data encryption system"Guru Kashi University (Talwandi Sabo), INDIA,Volume 3, Issue 11, November 2013.

[4] Manoj Mukherjee and Debabrata Samanta "Fibonacci Based Text Hiding Using Image Cryptography" Acharya Institute of Technology, Department of MCA, Bangalore, India, Vol. 2, No. 2, June 2014.

[5] Lim Chong Han, Nor Muzlifah Mahyuddin "An Implementation of Caesar Cipher and XOR Encryption Technique in a Secure Wireless Communication" Universiti Sains Malaysia, IEEE ICED, 2014,978-1-4799-610.

[6] Sanjeev Kumar, Tanupreet Singh "Performance improvement of simple LSB watermarking using SVD" Amritsar College of Engg. and Technology Amritsar, India, IEEE CIPECH14,29 November 2014.

[7] Sangita A. Jaju, Santosh S. Chowhan "A Modified RSA Algorithm to Enhance Security for Digital Signature" Dayanand Science College Latur, (M.S.), India, 978-1-4799-6908-1, 2015.

[8] Narendra B. Parmar, Dr.Kirit R. Bhatt "Hill Cipher Modifications: A Detailed Review" Sardar Vallabhbhai Patel Institute of Technology Vasad, Gujarat, India, Vol. 3, Issue 3, March 2015.

[9] Jai Singh, Kamil Hasan, Ravinder Kumar, Helina Patel "Enhance Security for Image Encryption and Decryption by Applying Hybrid Techniques" FALAH University, Faridabad, Haryana, India, Vol. 3, Issue 7, July 2015.

[10] Md.Atiullah Khan, Kailash Kr.Mishra, N.Santhi, J.Jayakumari "A New Hybrid Technique for Data Encryption" Noorul Islam University, Kumaracoil, Tamil Nadu, India, GCCT IEEE, 978-1-4799-8553-1, 2015.

[11] Prabhishek Singh, R S Chadha "A survey of digital watermarking techniques, applications and attacks" International journal of engineering and innovative technology, vol. 2 issue 9, March 2013.

[12] Saravanan chandran, Koushik Bhattachary " Performance analysis of LSB, DCT and DWT for digital watermarking application using steganography" National Institute of Technology, durgaphur , India, EESCO IEEE, 978-1-4799-7678-2,2015.

DOI 10.17148/IJARCCE.2016.5737