A Novel Crypt-Stego Technique for Information Security in Communication Networks

Surbhi Singhania[1], Shailender Gupta[2], Bharat Bhushan[3] and Ajay Nain[4]
YMCA University of Science and Technology
surbhidec24@gmail.com[1], shailender81@gmail.com[2], bhrts@yahoo.com[3], aknain90@gmail.com[4]

Abstract

With recent advances in Internet computing and its growing importance in our day to day life, the need for confidential communication has increased. The falling of sensitive and confidential data such as top intelligence secrets into an enemy nation's hands can lead to the misuse of technology and destruction of masses. Therefore, researchers have developed techniques such as cryptography and steganography to protect the data being transmitted. Cryptography uses mathematical algorithms to convert the data into an unreadable form and steganography on the other hand hides the data in a carrier such as image, data, audio or video. Both of these algorithms have disadvantages i.e. in case of cryptography the altered text can be easily detected by an intruder while in steganography the distortion of the carrier can attract an adversary. The proposal combines the advantages of both the techniques and provides a study tool for security. It calls for the combination of the two techniques which increases the brute force search time but at the same time ensures that the increase in time complexity of the result and process is within acceptable limits. Moreover this paper depicts a mathematical calculation of the errors in the embedded image with respect to the original image through the calculation of mean square error, peak signal to noise ratio and histogram representations.

Keywords: *Brute force search time, Cryptography, Image Steganography, information hiding, time complexity*

1. Introduction

There is an ever increasing requirement of secrecy in data communication between two entities at various levels, for instance the transmission of plan for a new missile from labs to higher ministries for approval. The falling of this sensitive data into an enemy nation's hands can lead to misuse of technology and destruction of masses. The data cannot be personally handled because the information is very large and mostly stored on computers [3]. Therefore researchers have developed methods for secure transmission of this data from one party to another. Two such techniques commonly used are cryptography and steganography.

Cryptography [3] is a method of securing data which dates back to a time as old as the World War I. It is a method by which information is converted to an unreadable form using a mathematical algorithm whose important factors (keys) are known only to the sender and the receiver. High speed computer processors have enabled us to encrypt large data files in very short duration despite using a very complex algorithm. Despite the above advantages it is not viable to use public key [3] cryptography mechanism as it has a very high time complexity and is generally used only for sharing of the key which is smaller in size comparison to the whole data. Therefore this paper focuses on use of private key cryptography and stream cipher technique for encryption and decryption.

Steganography [1, 2, 4, 5] is another mechanism used by researchers with a process very different from cryptography but having the same aim i.e. to secure data. It works on the idea of hiding the data inside an image, video, another data file, etc. The object used for data hiding is called a carrier. Steganographic techniques allow the user to hide data in an image, image in an image, image in data, *etc.* The advantage of steganography over cryptography is that it does not attract attention of an otherwise unaware person if the distortion of the carrier is minimal, unlike in cryptography where unreadable symbols might draw an adversary's attention.

The technique proposed in this paper combines cryptography and steganography. The benefit of this combination is that even if the adversary is able to detect the presence of confidential information, he still needs to search the decryption key to decrypt the data. This paper depicts the algorithms and the results of a simulator that was created in MATLAB to practically implement the above idea. The steganographic techniques used are Substitution [6-11], Distortion [12-15] and Direct Cosine Transform [16] and the cryptographic techniques include Data Encryption Standard (DES) [3] and RC4 [3]. DES uses a 64 bit key. In order to compare the various methods, parameters such as time complexity, signal to noise ratio, mean square error and histogram were recorded and compared.

The rest of the paper is organized as follows: Section 2 provides the literature survey of the work in this direction. Section 3 discusses algorithm of the proposed technique. Section 4 provides the simulation set up parameters and metrics used to evaluate the performance of the work. Section 5 provides the results followed by conclusion.

2. Literature Survey

Little work has been done to combine cryptography and steganography to provide an enhanced security in data communication networks. Their work is as follows:

Sujay Narayana, *et al.*, [17] proposed a scheme using S-DES algorithm combined with LSB substitution technique. The image to be hidden was first encrypted using a key and the encrypted image was embedded in the cover image. Their work like others [18] was primarily focused on the change in image quality.

The work done by Shailender Gupta, *et al.*, [19] proposed a hybrid model that combines steganography and cryptography. The Cryptographic technique used was RSA and Diffie Hellman and the steganographic technique used was LSB substitution. Since the public key mechanisms are having higher time complexity than other mechanisms hence it is not practical to use them for sharing large data. They can be used for sharing of small data and key.

3. The Proposed Method

In this method steganography and cryptography (private key) are combined to test the following parameters:

- Picture quality
- The time complexity
- Brute force search time
- Maximum capacity

Before discussing the proposed algorithm we would like to give a brief description of the variables and functions (see Table 1) used in our proposal that will help the readers in better understanding of the proposal.

Table 1. Terminology used in the papers

Entity used	Description
C	Original Image
S	Stego-Image
N	Plain Text
M	Cipher Text
L(m)	Length of data
Pxq	Image dimensions
Seed	Common seed used to generate random numbers
Rand()	Function to generate random numbers
Dct2()	Discrete Cosine Transform
Decrypt()	Decrypt data
idct2()	Inverse discrete cosine transform
Encrypt()	Encrypt data using DES or RC4

3.1. Sender Side Procedure

The original data file to be transferred is read as a set of ASCII characters at the sender side and is referred to as

Algorithm: Embedding process of LSB substitution technique

```
S=C;
k=0;
m= encrypt (n);
j=rand (l (m), seed);
k=j1
for i =1 to l (m)
   Sk ← mi
   k= (k +ji+1) % pxqx3;
end for;
```

the plain text (n). This plain text is then provided as the input to the cryptographic algorithms (using encrypt () function) to convert it into cipher text (m). The next step is to embed the cipher text into the cover image (S) using one of the steganographic- techniques mentioned in the paper.

3.1.1. Embedding Process of LSB substitution technique: The first step of LSB substitution is to identify the pixels of the steganographic cover (S) where the message bit is to be embedded. These are selected pseudo-randomly with reference to a particular seed (using rand() function) that is known to both the sender and the receiver. These pixels (Sk) are modified by replacing their LSBs with the message bit (mi) which can be either 0 or 1.

Algorithm: Embedding process of Distortion technique

```
S=C;
k=0;
m= encrypt (n);
j=rand (l (m), seed);
k=j1;
for i =1 to l (m)
    if (mi==1)
     Sk =Sk+ Δ ;
End if ;
k= (k +ji+1) % pxqx3;
end for;
```

3.1.2. Embedding Process of Distortion substitution technique: Distortion is similar to LSB substitution except for the fact that this method changes the value of the selected pixel (Sk) by adding a definite Δ if the corresponding message bit (mi) to be embedded is 1 and is left as it is for the bit (mi) being 0.

Algorithm: Embedding process of DCT technique

For *i=1 to l(m)*
Choose one cover block bi
B_i*=dct2(*b_i*);*
if m_i *= 0 then*
if B_i*(u1; v1) > Bi(u2; v2) then*
swap B_i*(u1; v1) and* B_i*(u2; v2)*
end if
else
if *Bi(u1; v1) < Bi(u2; v2) then*
swap Bi(u1; v1) and Bi(u2; v2)
end if
end if
adjust both values so that
|Bi(u1; v1) − Bi(u2; v2)| > x
b_{0i} *=idct2(Bi);*
end fo
create stego-image out of all b_{0i} *block.*

3.1.3. Embedding Process of DCT steganography technique: The process is commonly used when the image carrying the embedded data is likely to be subjected to image modification processes like cropping, jpeg compression, etc. The algorithm is designed to store data at the significant parts of the image which are less likely to be affected during the above mentioned processes. The image is divided into an array (b) of blocks (8x8 dimensions). To embed a data bit, one of the blocks is chosen and a discrete cosine transform of this block is taken. Matrix index (u1; v1) and (u2; v2) are chosen according to the standard quantization matrix used for jpeg compression.

The two indices are chosen such that the coefficients at these indices correspond to the cosine function with middle frequencies. This ensures that the data is stored in the substantial parts of the image. The matrix positions (5, 2) and (4, 3) or (2, 3) and (4, 1) are favorable for this operation. Using the steps mentioned in the algorithm changes are made in this DCT transformed block (Bi). Last step of the algorithm is important as it ensures that the changes remain evident in case the values of coefficients at the two chosen indices are nearly same.

$$| Bi (u1; v1) – Bi (u2; v2) | > x \text{ for } x>0$$

$$\begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 29 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix}$$

3.2. Receiver side Procedure

After receiving the image the receiver retrieves the embedded data (m) using the inverse of the steganographic - technique used by the sender. To obtain the plain text (n), corresponding decryption algorithm is used. The receiver already has an access to key used in the process of steganography or cryptography.

Algorithm: Extraction process of LSB Substitution technique

```
k=0;
 j=rand (l (m), seed);
k=j1 ;
for i =1 to l (m)
mi ← LSB(Sk )
 k= (k +ji+1) % pxqx3;
end for;
n=decrypt(m);
```

3.2.1. Extraction process of LSB Substitution technique: The receiver selects the pixels (Sk) pseudo-randomly from the cover image (S) using the same seed used by the sender. From the LSB of these pixels the message array (m) is extracted. This message array on being decrypted gives the final data array (n) which was initially intended for transmission.

Algorithm: Extracting process of Distortion technique

```
d=S-C;
k=0;
j=rand (l (m), seed);
k=j1;
for i =1 to l (m)
    if (dk==0)
            mi=0;
    else
            mi=1;
    end if;
k= (k +ji+1) % pxqx3;
end for;
N=decrypt(m);
```

3.2.2. Extraction process of Distortion technique: This process is more or less similar to LSB substitution

Algorithm: Extraction process of DCT Technique

```
for i = 1 to l(m) do
get cover-block bi associated with bit i
Bi = dct2(bi)
if Bi(u1; v1) ≤Bi(u2; v2) then
mi = 0
else
mi = 1
end if
end for
n= decrypt(m)
```

except for the fact that, in Distortion the receiver must have the original cover image (C). On subtracting the pixels of the received stego-image (S) from the pixels of original image (C), the receiver obtains a difference matrix (d) which is composed of elements either being 0 or Δ.

This difference matrix is traversed using the pseudo-random pixel selection approach used in the substitution method and comes up with a matrix (m) element of which are assigned 1 for every Δ and 0 for every 0 of the difference matrix (d). Finally on decryption of m the plaintext matrix n is obtained. In the extraction process of DCT the received image is divided into an array of blocks (8x8 in dimension). After checking the value of coefficients according to the above algorithm message bits (m) and final data array (n) is recovered.

4. Simulation Set up

4.1. Performance Metric

The performance metrics used for comparison of different techniques and their combinations are as under:

- **Time Complexity:** The total time taken by all the processing on receiver and sender side comprises of time complexity [18-19].
- **Qualitative Analysis:** The original image after embedding of data undergoes distortion as steganography causes change in pixel value of an image [18-19]. The image is subject to qualitative visual analysis to observe any noticeable change in image quality.
- **Histogram:** A histogram [20] is a graphical representation of the distribution of the data. In our case we measured the variation in number of occurrences of a particular color value between the original and final stego-image to show how much error is introduced in the image after applying steganography.
- **Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE):** These two parameters [21] are a quantitative representation of the error incurred in the final embedded image with respect to the original image.

$$MSE = \frac{1}{XY}\sum_{i=0}^{X-1}\sum_{j=0}^{Y-1}[I(i,j) - K(i,j)]^2 \quad (1)$$

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

X and Y are the dimensions of the image taken into consideration.
I(i, j) is the pixel value of the (i, j)th pixel value of the original Image
K(i, j) is the pixel value of the (i, j)th pixel value of the final embedded Image
MAX is the maximum possible pixel value of the image which is 255 in our case.

4.2. Setup Parameters

A simulator was designed in MATLAB 7.12.0 to simulate the combinations of the cryptographic and steganographic techniques for different image sizes. The simulation setup parameters used are given in Table 2 below:

Table 2. Setup Parameters

Component	Parameter	Value of parameter
Steganography	Techniques	Substitution (seed=2) Distortion (Seed=2) DCT
	Image Size	1024x1024 2048x2048 3072x3072
	Plain text size	1 K Byte
Cryptography	Technique	DES (Key size = 64 bit) RC4=String= 'ajaynain'
Processor	Type	I5-64 bit, 2 GHz
	RAM:	2 GB
	Speed:	2 GHz

5. Simulation Results

5.1. Impact on Image Quality

Qualitative Analysis helps to identify pictographically the changes incurred in the cover image after applying the proposed method. This change in image quality is due steganographic technique, as these techniques define the extent to which the image is modified. After careful study of the Figure 1 the following inferences can be made:

- It can be easily seen from the figures that addition of cryptography to steganography does not introduce any significant changes in the image quality. This is due to the fact that the amount of data embedded in both the cases is almost same.
- DCT introduces maximum alteration in the image quality as compared to the other techniques discussed as it changes the pixel by a large value whereas distortion and LSB substitution varies the pixel value by a small factor.

5.2. Histogram representation

Histogram is used to graphically represent the changes incurred in the cover image by applying the proposed mechanism. Figure 2(a) shows the histogram of the actual image while the Figure 2(b) shows the impact after applying substitution steganography on image. Figure 2(c) to Figure 2(k) show the differences in the number of pixel values between original image and the image obtained after applying the proposed mechanism. The following inference can be drawn from the Figure 2:

- The distortion is much prominent in DCT. Additionally using DCT with any cryptographic mechanism will lead to further degradation of the image. Therefore hiding data using this mechanism will be vulnerable to attacks by hackers.
- With the naked eye the impact of steganography was not visible (see Figure 1) but the histogram results show that number of pixel values changes is significant using the proposed mechanism as is evident from the Figure 2.

5.3. Impact on MSE and PSNR

The histogram results show that using steganography and cryptography changes in the picture quality though this variation is marginal as seen from the naked eye. This gives an insight to check the variation mathematically. On doing so we observed the following changes as follows:

- The difference between the picture qualities using steganography and steganography with cryptography is between -0.3 to 8.1 percent (see Figure 3).
- Application of cryptography with steganography results in marginal decrease in the value of PSNR and marginal increase in the value of MSE in comparison to application of steganography alone.
- The maximum variation of PSNR and MSE is observed when distortion is applied with DES while the minimum variation is observed when DCT is applied with DES
- As the image size increases the value of PSNR increases and that of MSE decreases. This is due to the fact that MSE is inversely proportional to the dimensions of the cover image and PSNR is inversely proportional to MSE from eq. (1) and eq. (2).

5.4. Impact on Capacity and time complexity

Applying cryptography combined with steganography increases the time taken by the overall process. On the other hand capacity is only a function of steganography and combining it with cryptography does not in any way affect the maximum data hiding capacity of the carrier compared to steganography applied alone (see Figure 4).

- The capacity increases with increase in image size
- Distortion and Substitution have a capacity that is 64 times that of the maximum capacity of the DCT technique combined with any cryptographic technique. This is because in the first 2 cases a single data bit can be embedded in every possible pixel whereas in DCT only one pixel is embedded in one 8x8 block of the whole image. Moreover, the capacity of substitution can further be increased if more than one least significant bit per pixel is replaced with the data bits.
- With increase in image size the time taken to complete one process increases.
- Compared to RC4, DES cryptography introduces more increase in time complexity for all types of steganographic techniques.

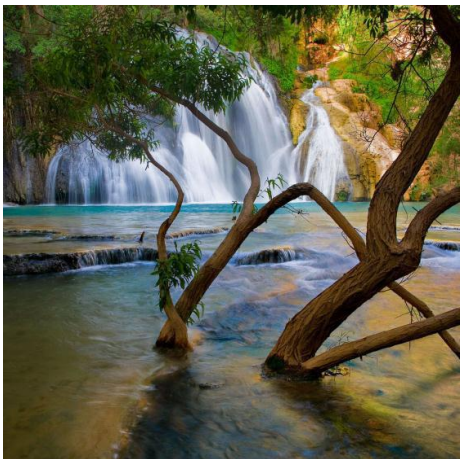

Figure 1(a). Original Image

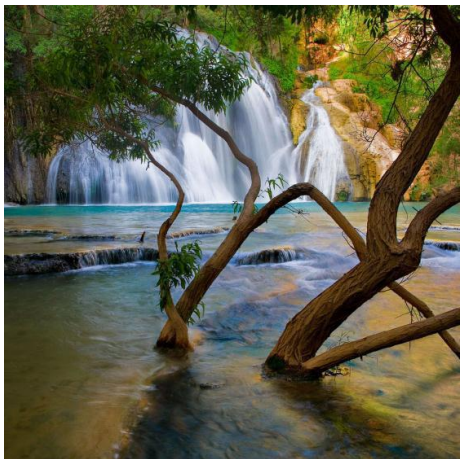

Figure 1(b). Impact of Substitution

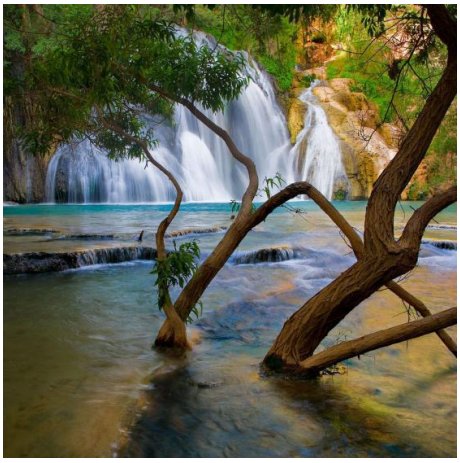

Figure 1(c). Impact of Substitution &RC4

Figure 1(d). Impact of Substitution & DES

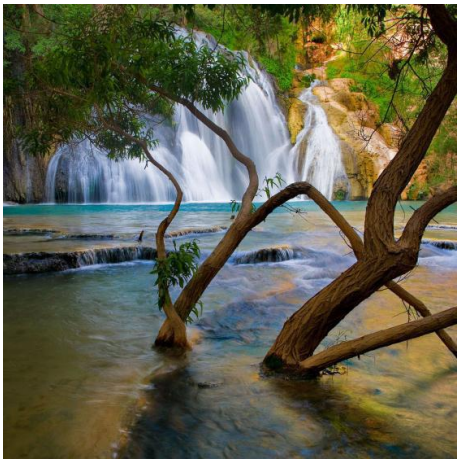

Figure 1(e). Impact of Distortion

Figure 1(f). Impact of Distortion & RC4

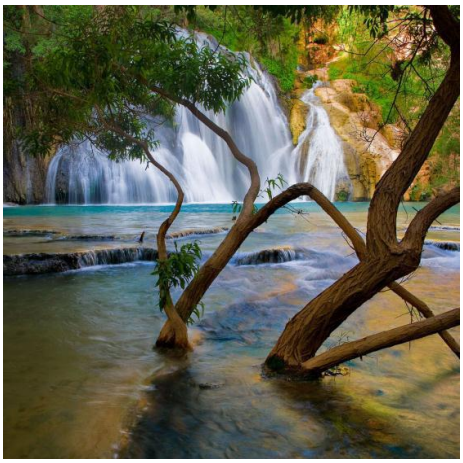

Figure 1(g). Impact of Distortion & DES

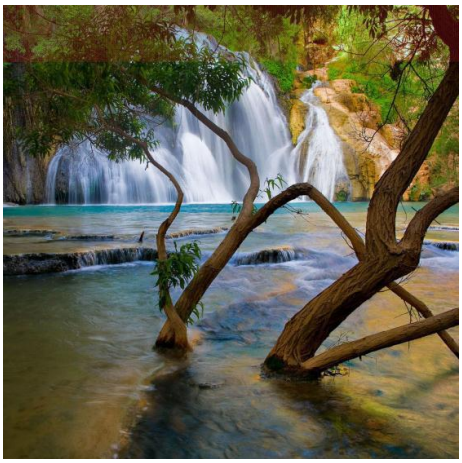

Figure 1(h). Impact of DCT

Figure 1(i). Impact of DCT & DES

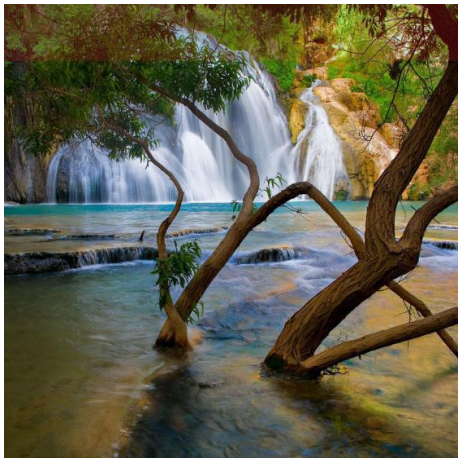

Figure 1(j). Impact of DCT & RC4

Figure 1. Impact on Image Quality

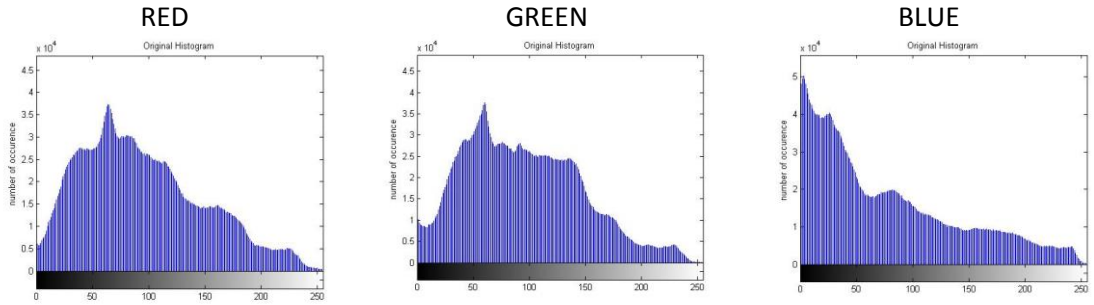

Figure 2(a). Color Value of Original Image

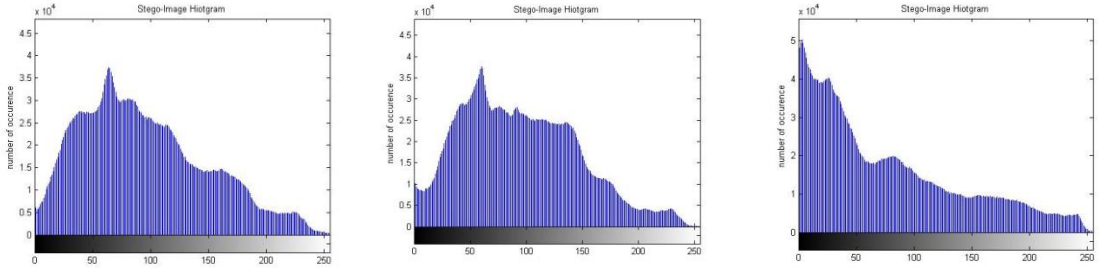

Figure 2(b). Color value of Final Image for Substitution

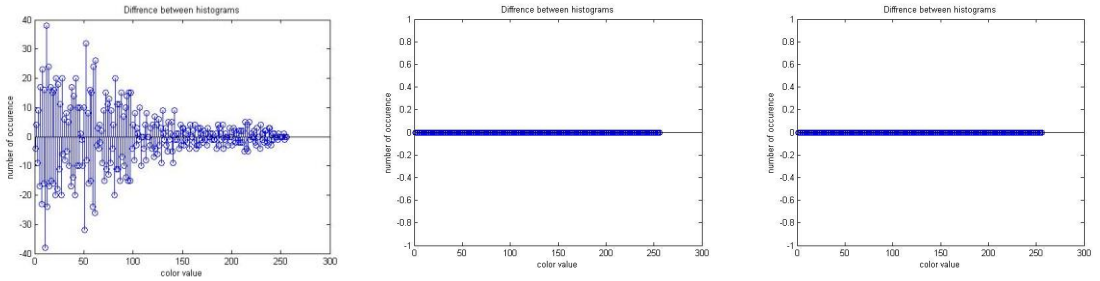

Figure 2(c). Difference in color value for Substitution

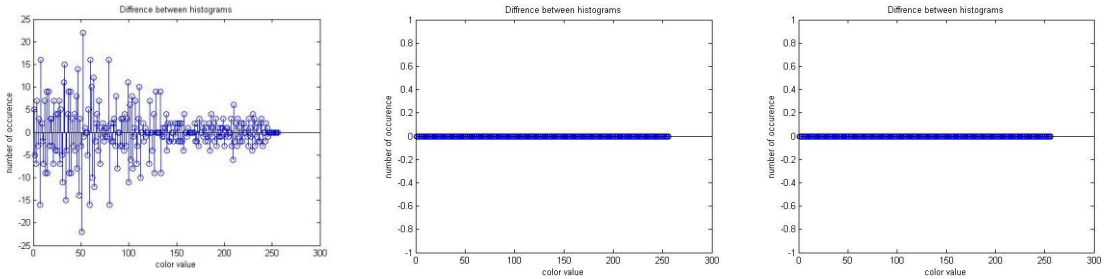

Figure 2(d). Difference in color value for Substitution and DES

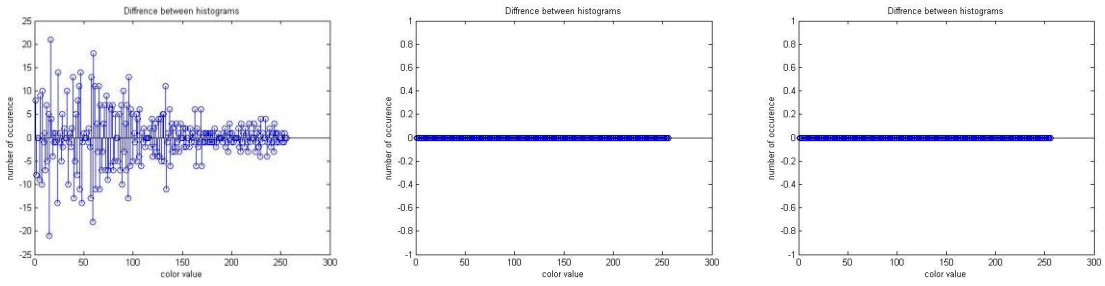

Figure 2(e). Difference in color value for Substitution and RC4

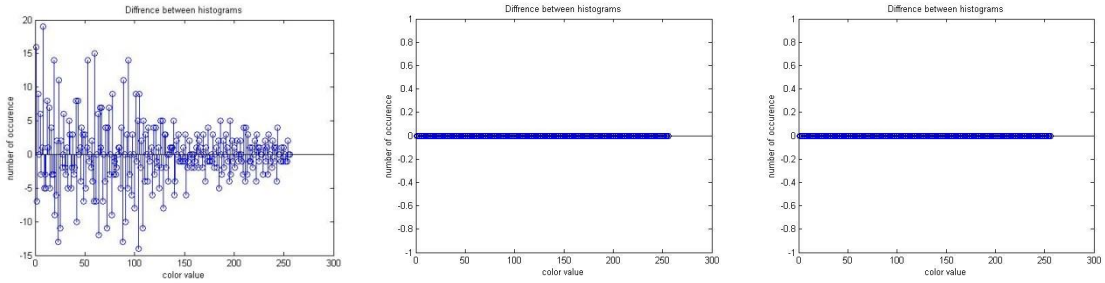

Figure 2(f). Difference in color value for Distortion

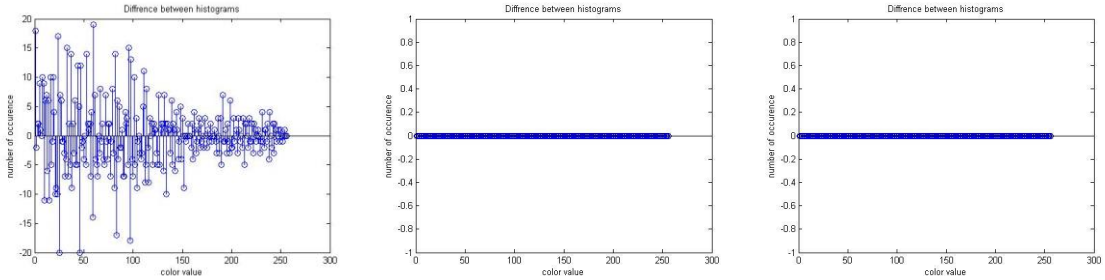

Figure 2(g). Difference in color value for Distortion and DES

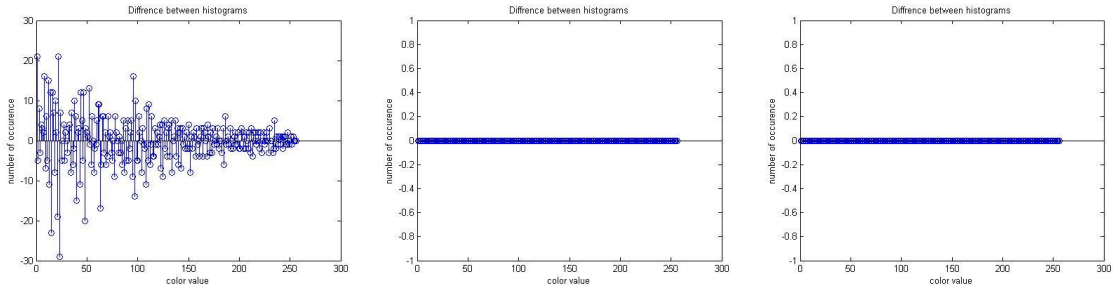

Figure 2(h). Difference in color value for Distortion and RC4

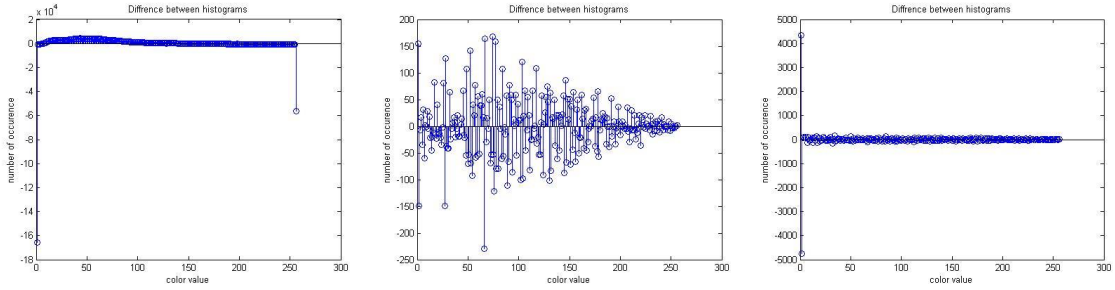

Figure 2(i). Difference in color value for DCT

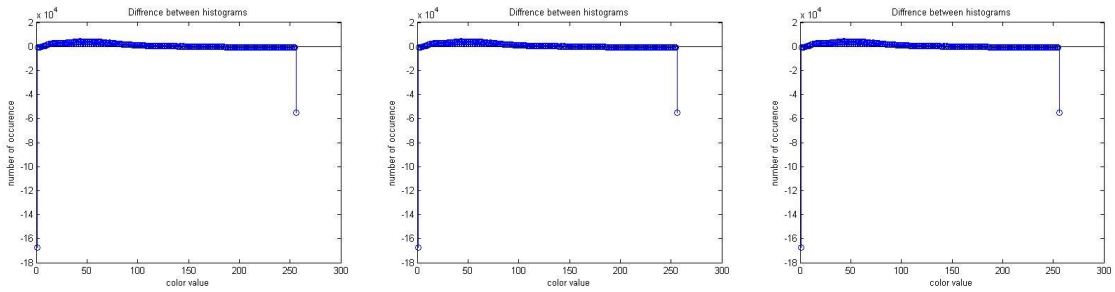

Figure 2(j). Difference in color value for DCT and DES

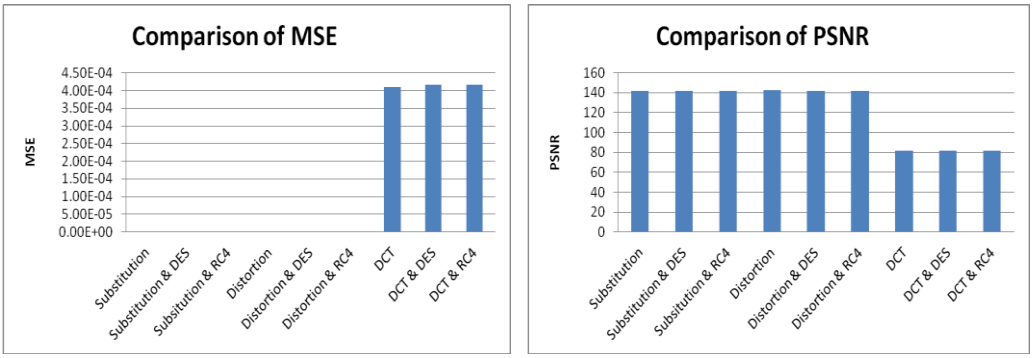

Figure 3(a). MSE & PSNR (1024 X 1024)

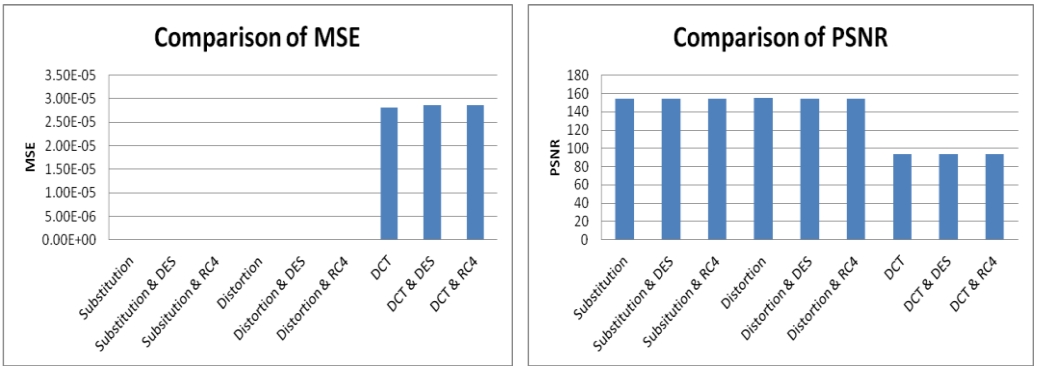

Figure 3(b). MSE & PSNR (2048 X 2048)

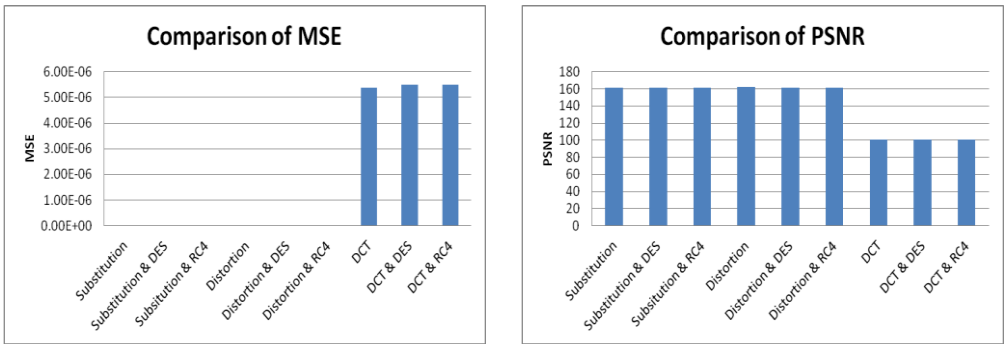

Figure 3(c). MSE & PSNR (3072 X 3072)

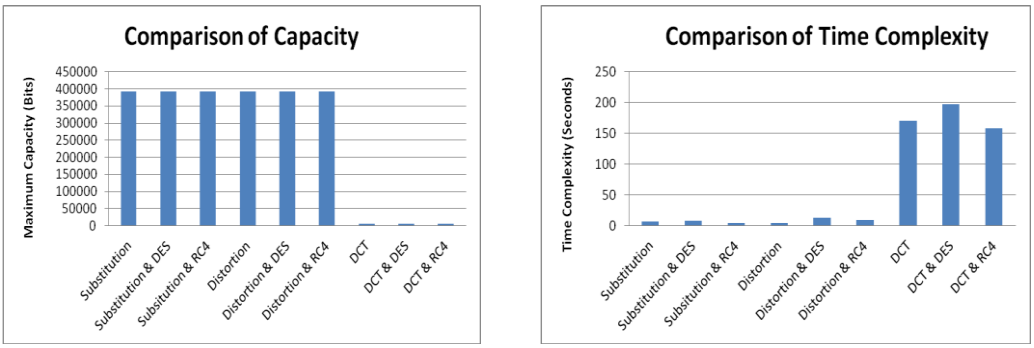

Figure 4(a). Capacity for Image (1024 X 1024)

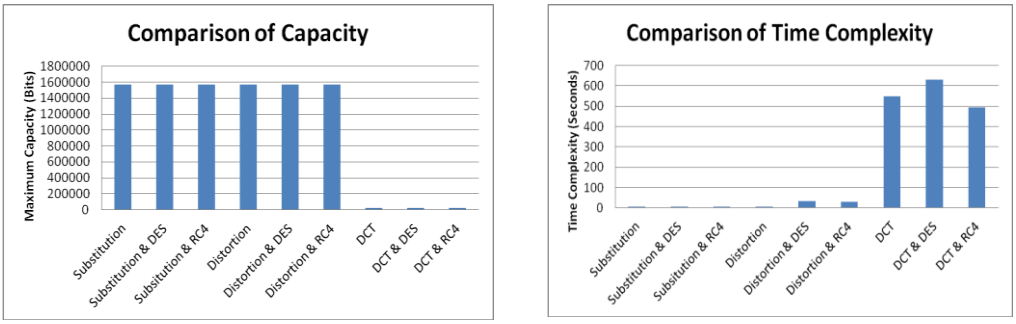

Figure 4(b). Capacity for Image (2048 X 2048)

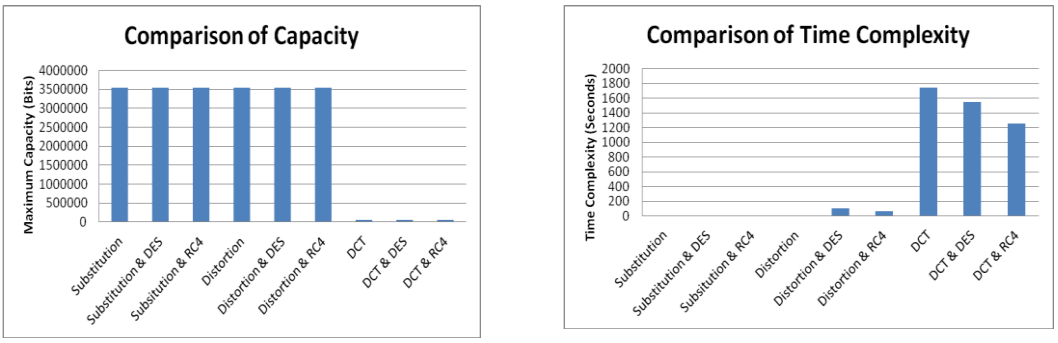

Figure 4(c). Capacity for Image (3072 X 3072)

6. Conclusion and Future Scope

The mechanism proposed in this paper tries to provide enhanced security for sensitive data by using both steganography and cryptography. The overall results can be summarized as follows:

- This mechanism increases time complexity but the increase is marginal since 64 bit key is used. If the key size is increased the security will certainly be enhanced but at the cost of increased time complexity.

- Steganography introduces distortion in the carrier and may unnecessarily attract the adversary. But there are some algorithms that introduce less distortion than the others and if the data embedded in the image is of the size compliant with the carrier size the distortion can be reduced and hence not draw attention.

- It is observed that applying cryptography along with steganography increases the Brute force search time. Therefore the time required to break the mechanism by an adversary increases as a result of the above proposed mechanism.

Table 3. Overall inference of proposed scheme

Parameters	Pure Steganography	Steganography & Cryptography
Brute Force Search time	Low	High
MSE	Low	Marginally high
PSNR	High	Marginally low
Capacity	Same	Same
Visual Image Quality	Low	Marginal decrease
Time Complexity	Low	Marginal Increase
Time Complexity	Low	Marginal Increase

References

[1] N. F. Johnson and S. Jajodia, "Steganalysis of Image Created Using Current Steganography Software", Workshop of Information Hiding Proceedings, Portland Oregon, USA, 15-17 April,1998, Lecture Notes in Computer Science, vol. 1525, Springer-Verlag, **(1998)**.

[2] B. Clair, "Steganography: How to Send a Secret Message", **(2001)** November, www.strangehorizons.com/2001/20011008/steganography.shtml.

[3] W. Stallings, "Cryptography and Network Security: principles and practices", Pearsons education, first Indian reprint, **(2003)**.
[4] G. B. Rhodas, "Method and Apparatus Responsive to a Code Signal Conveyed Through a Graphic Image", U.S. Patent 5,710,834, **(1998)**.
[5] M. D. Swanson, B. Zhu and A. H. Tewk, "Transparent Robust Image Watermarking", in Proceedings of the IEEE International Conference on Image Processing, vol. 3, **(1996)**, pp. 211-214.
[6] W. Bender, D. Gruhl and N. Morimoto, "Techniques for data hiding", IBM Systems Journal , vol. 35, no. 3/4, **(1996)**, pp. 131-336.
[7] S. A. Moller, Pitzmann and I. Stirand, "Computer Based Steganography: How It Works and Why Therefore Any Restrictions on Cryptography Are Nonsense, At Best", in Information Hiding: First International Workshop, Proceedings, vol. 1174 of Lecture Notes in Computer Science, Springer, **(1996)**, pp. 7-21.
[8] D. Gruhl, A. Lu and W. Bender, "Echo Hiding in Information Hiding", First International Workshop, Proceedings, vol. 1174 of Lecture Notes in Computer Science, Springer, **(1996)**, pp. 295-316.
[9] C. Kurak and J. McHughes, "A Cautionary Note On Image Downgrading", in IEEE Computer Security Applications Conference 1992, Proceedings, IEEE Press, **(1992)**, pp. 153-159.
[10] R. G. Van Schyndel, A. Tirkel and C. F. Osborne, "A Digital Watermark", in Proceedings of the IEEE International Conference on Image Processing, vol. 2, **(1994)**, pp. 86-90.
[11] N. F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen", IEEE Computer, vol. 31, no. 2, **(1998)**, pp. 26-34.
[12] N. F. Maxemchuk, "Electronic Document Distribution", AT&T Technical Journal, **(1994)** September/October, pp. 73-80.
[13] S. H. Low, *et al.*, "Document Marking and Identifications Using Both Line and Word Shifting", in Proceedings of Infocom'95, **(1995)**, pp. 853-860.
[14] S. H. Low, N. F. Maxemchuk and A. M. Lapone, "Document Identification for Copyright Protection Using Centroid Detection", IEEE Transactions on Communications, vol. 46, no. 3, **(1998)**, pp. 372-383.
[15] S. H. Low and N. F. Maxemchuk, "Performance Comparison of Two Text Marking Methods", IEEE Journal on Selected Areas in Communications, vol. 16, no. 4, **(1998)**, pp. 561-572.
[16] G. B. Rhodas, "Method and Apparatus Responsive to a Code Signal Conveyed Through a Graphic Image", U.S. Patent 5,710,834, **(1998)**.
[17] S. Nararayana and G. Prasad, "Two New Approaches For Secured Image Steganography Using Cryptographic Technique and Type Conversions", Signal and Image Processing: An International Journal (SIPIJ), vol. 1, no. 2, **(2010)** December.
[18] S. Gupta, A. Goyal and B. Bhushan, "Information Hiding Using Least Significant Steganography and Cryptography", I. J Modern Education and Computer Science, vol. 6, IJMECS, **(2012)**, pp. 27-34.
[19] S. Gupta, B. Bhushan, S. Singhania and J. Gulani "A Hybrid approach for ensuring security in data communication", Accepted for publication in CCSIT 2013, **(2013)**.
[20] K. Solanki, K. Sullivan, U. Madhow, B. S. Manjunath and S. Chandrasekaran "Provably secure steganography: Achieving zero K-L Divergence using statistical restoration", Published in proceedings of ICIP 2006, IEEE, **(2006)**, pp. 125-128.
[21] H. Sheisi, J. Mesgarian and M. Rahmani, "Steganography: Dct Coefficient Replacement Method and Compare with Jsteg Algorithm", International Journal of Computer and Electrical Engineering, vol. 4, no. 4, **(2012)** August.