A HYBRID APPROACH FOR ENSURING SECURITY IN DATA COMMUNICATION

Shailender Gupta[1], Bharat Bhushan[2], Surbhi Singhania[3] and Jeetesh Gulani[4]

[1,2,3]Department of Electronics Engineering, YMCA University of Science and Technology, Faridabad, India
[1]shailender81@gmail.com, [2]bhrts@gmail.com, [3]surbhidec24@gmail.com
[4]Indian Institute of Technology Kharagpur,India
[4]jeetesh1993@iitkgp.ac.in

ABSTRACT

For a very long time, various forms of steganographic and cryptographic techniques have been used to ensure security in data communication. Whereas steganography is the art of hiding the fact that any communication is taking place, cryptography on the other hand ensures data security by changing the very form of the data being communicated by using a symmetric or an asymmetric key. But, both the methods are susceptible to being weakened by a challenger. In steganography, there is always a possibility of detection of the presence of a message by the opponent and most of the cryptographic techniques are vulnerable to disclosure of the key. This paper proposes a hybrid approach where in image steganography and cryptography are combined to protect the sensitive data thereby ensuring improved security in data communication. To find the impact of the same, a simulator was designed in MATLAB and corresponding time complexities were recorded. The simulation results depict that this hybrid technique although increases the time complexity but ensures an enhanced security in data communication.

KEYWORDS

Cryptography, Image Steganography, information hiding, time complexity

1. INTRODUCTION

With an increase in data communication in the recent past, the security of data over a communication channel is of paramount importance. Various Steganographic [1-2] and Cryptographic [3] algorithms have been proposed to ensure data security in communication.

Steganography is a smart strategy which calls for hiding the sensitive information in other data which is generally considered to be ordinary by an unaware viewer. This cover data may be in the form of text, image, audio, video, etc. The security of the data communication depends on the ingenuity in the alteration of the cover such that the adversary is not able to detect the presence of a secret message. The receiver uses the reverse approach to extract the data from the modified cover.

Jan Zizka (Eds) : CCSIT, SIPP, AISC, PDCTA - 2013
pp. 133–144, 2013. © CS & IT-CSCP 2013 DOI : 10.5121/csit.2013.3614

Cryptography refers to a science of transforming the messages into an unreadable form by means of a set procedure hence making the core data inaccessible to an interfering individual. In this approach, the original message called the plain text is converted into an encoded message called the cipher text with the help of an encryption algorithm. This cipher text is then sent over a communication channel. On the receiver side a decryption algorithm is used to recover the plain text.

Despite the above mentioned techniques being advanced and sophisticated, none of them provide a fool proof safety in communication. Steganographic techniques used deteriorate the image quality [4-5] hence presence of data in images can be easily detected by malicious nodes. On the other hand cryptographic techniques [3] has the disadvantage that if an intruder is able to figure out the key then he will be able to decrypt the data. Hence, none of the methods are completely guaranteed in a stand-alone fashion.

This paper proposes a novel scheme to provide a comparatively high security to the data. In this scheme, a combination of the above mentioned techniques offers advantages of both steganography and cryptography. The encryption methods used are: Data encryption standard (DES) algorithm [3] and Diffie-Hellman algorithm [3], whereas the size of the key implemented is 32 bit and 64 bit. The encrypted data is embedded in the images of different sizes using three different algorithms namely: Pseudorandom Substitution, Transform Domain (DCT) and Distortion. To check the efficacy of the proposal the time complexity of the process at the sender and receiver side was recorded.

The rest of the paper has been organized as follows: Section 2 provides the current steganographic techniques used in this paper, Section 3 provides the problem identification, Section 4 provides the proposed work for problem identified, Section 5 gives the simulation and results of the proposed model, Section 6 gives the conclusion followed by references.

2. STEGANOGRAPHIC TECHNIQUES USED

2.1. Pseudo Random LSB- Substitution Method

The least significant bit substitution [6-11] method is the oldest method used for steganography. A simple substitution method involves replacing the least significant bit of a first few pixels of the image with that of the bits of the data. The change incurred in the pixel value is that of only +/- 1. Therefore, the chances of these changes being noticed in the embedded image are very minor.

This method being fairly banal and is susceptible to attacks. Therefore, we have introduced a modification of the same by introducing pseudorandom substitutions. Here, instead of replacing the bits of the ordered pixels the sender chooses a series of random pixels and replaces the LSB of these bits with the data bits. The receiver must also choose the same random pixels to extract the data from the LSB of these pixels. For this purpose the sender and receiver share a key. This key is used as a seed to generate the same random numbers for embedding and extracting purpose.

This method can be further made robust by sharing a second seed which will help the sender and receiver to choose the data-bits randomly from the complete set of data bits to be embedded. Thus embedding random data bits in random pixel and as a result, improving security. Even if a hacker is able to get hold of one key the absence of the second will make his effort go vain.

This method is good for transmitting large data as the image can hold the binary data of length up till the total number of pixels of the image. Hence an RGB image can hold data as much as three

times a gray scale image without any significant distortion. One major assumption of the method is that the length of the embedded data must be known to both the receiver and the sender for successful transmission.

2.2. Distortion Technique

This technique [12-15] is similar to the substitution technique except for the fact that it is important, for the receiver and sender to have the original cover image. A pixel is chosen using the pseudorandom method explained before. Next, the data bit to be embedded is evaluated. If the binary bit is '0' then the pixel is left as it is. On the other hand when it is '1' a small value Δx is added to the pixel. This stego-image is then sent to the receiver.

The receiver subtracts the pixels of the received image from the original cover image he already has. This results in an array of Δx and 0 values. These elements are then accessed in the same pseudorandom manner. If the value is zero the bit is read as '0' and if it is Δx it is read as 1. This is altogether compiled to generate the data.

The distortion technique is faster compared to the substitution technique. It can also hold large volumes of data in accordance to the image size. But it is also more vulnerable because if a hacker has the cover image he may be able to access the data provided he knows the other parameters. And the distortion of the image is more prominent compared to the substitution methods.

2.3. Transform Domain Technique (DCT)

The distortion and substitution methods are vulnerable to any modifications in the image. The processes like cropping, compressing, image processing, etc can largely destroy the information embedded in the image. The transform domain methods [16] hide the data in the significant part of the images hence; make it more robust against these disturbances. DCT is one of the transform domain methods. This method is specifically designed to resist any changes in the secret data caused by jpg image compression and still allow successful compression. Jpeg compression can be explained with the help of the following block diagram (see Fig 1).

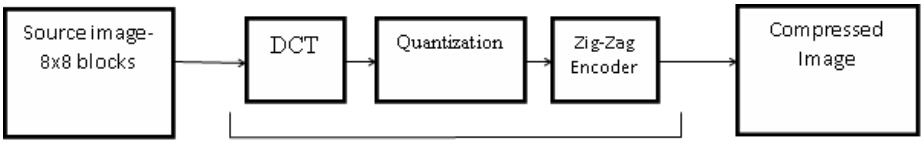

Figure 1. Jpeg Compression

2.3.1. JPEG Compression

The Quantization matrix used at the step of quantization is the most important element of the process. It is a standard matrix given by:

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

Referring to this matrix, the sender and receiver agree on the two indices (j1, k1) and (j2, k2) (say). These are chosen such that the coefficients at these indices correspond to the cosine function with middle frequencies. This ensures that the information is stored in the significant parts of the image. According to the above shown matrix the positions (5, 2) and (4, 3) or (2, 3) and (4, 1) are favorable for this operation.

The image is divided into an array of 2 dimensional matrices of the magnitude 8x8. The DCT operation is performed on these matrices to obtain another set of 8x8 matrices (say D).

Starting with the first block and the first data bit, we check if the data bit is '1' or '0'. Next, compare the magnitude of coefficients at the chosen indices. If D (j1, k1)>D (j2, k2) and the bit to be embedded is '1' then the indices are left as it is. Else to embed '0' the coefficient values are swapped. Alternately if D (j1, k1) <D (j2, k2) and the bit to be embedded is '1' then the coefficients are swapped whereas for '0' they are left as it is. Also this algorithm ensures that |D (j1, k1)- D (j2, k2)|>x, where x>0.

This is done by increasing the value of the larger coefficient and by further decreasing that of the smaller to maintain a constant difference between the two.

The factor of distortion depends upon the constant x and the location of the coefficient. This method causes visibly more distortion that the previous two methods and also consumes more time. Moreover the capacity of a particular sized image is fixed. If we try to embed the data more than its capacity the secret data is lost due to superimposition. Yet, it is the most robust method for obtaining compressed images and to perform other manipulations without losing the embedded secret data. The security can be improved by choosing the blocks and data in the pseudorandom manner.

3. PROBLEM IDENTIFICATION

Neither steganography nor cryptography is standalone solution to provide security in communication networks. In steganography the presence of data can be easily detected by observing distortion in the cover image. On the other hand cryptographic techniques can fail in scenario of key disclosure by nodes having rogue intentions. In our opinion if the data embedded in the image is encrypted, the confidentiality of the data would be maintained even if it is extracted by an intruder node. Thus it would be beneficial if the secret data is encrypted before applying steganography. Some researchers who have previously worked in this direction 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.

Shailender Gupta et. al. [18] 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.

This paper has been inspired from the above mentioned literature. This paper focuses on embedding a text file in the image unlike Sujay narayanas et. al. attempt which was centrally based on the idea of hiding an image in a cover image. Moreover Shailender guptas et. al. used only 32 bit key for the purpose of encryption and decryption and uses only LSB substitution steganographic technique. The idea proposed in the current paper is an improvement over this work.

4. THE PROPOSED SCHEME

4.1. Sender side

The sender side process is depicted in figure 2. The secret message called the plain text is converted into cipher test using one of the two mentioned algorithms i.e. DES or Diffie-Helman using a 32 bit or 64 bit. This cipher text is then converted to bits. These bits are embedded into a cover image using one of the three steganographic techniques namely pseudorandom substitution, Transform Domain (DCT) or Distortion. The resultant encrypted stego-image is sent over a channel.

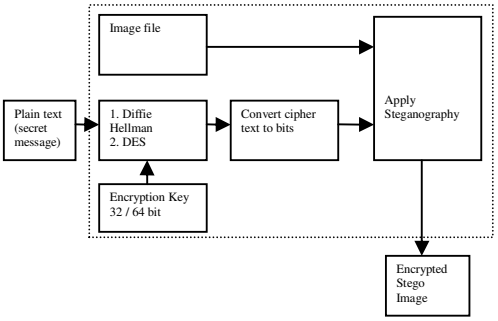

Figure 2. Block diagram of proposed scheme at sender side

4.2. Receiver side

The complete process at the receiver side is depicted in figure 3. The received encrypted stego-image is subjected to steganographic extraction process and decryption technique corresponding to the techniques used at transmitter side to recover the plain text.

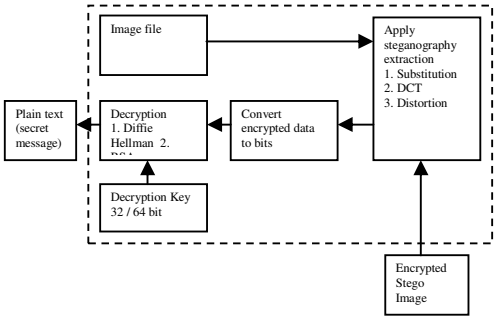

Figure 3. Block diagram of proposed scheme at receiver side

5. SIMULATION AND RESULTS

5.1. Performance metrics

The following parameters were used to record the results:

- **Time complexity**- Defined as the total time taken by the sender side to encrypt and embed the secret message in the cover image, combined with the time taken by the receiver to extract and decrypt the secret message from the transmitted image.
- **Qualitative comparison of images**- The original cover image and the modified images (after cryptography and steganography) were placed side by side and subjected to visual inspection.

5.2. Simulation setup

A simulator was designed in MATLAB 7.12.0 to simulate various combinations of the cryptographic and steganographic techniques at different key and image sizes. The simulation setup parameters used are as shown below:

Table 1. Setup parameters.

Component	Parameter	Value of parameter
Steganography	Techniques	Substitution, Distortion, DCT
	Image Size	• 1024x1024 • 1536x1536 • 2048x2048 • 3072x3072 • 4096x4096 • 5120x5120
	Plain text size	1 K Byte
Cryptography	Technique	Diffie Hellman Key = Gxy mod (P) Where for **32 Bit** p = 2863311530, g=112557 x=637, y=597 **64 Bit** p= 768614336404564650, g=112557 x=637, y=597

		DES Key(k)=4294967295 (32 bit) Key(k)=18446744073709551615(64 bit)
Processor	Type	i5-64 bit
	RAM:	2 GB
	speed:	2370 MHz

5.3. Simulation results

This section is dedicated to depicting the impact of the combination of the steganographic and cryptographic techniques on images of various sizes. Before discussing time complexities two important things should be kept in mind:

- The time shown in all cases is the total time elapsed on the sender and receiver side. It does not include time elapsed in transfer of information from source to destination.
- The time complexities in case of Diffie- Helman (combined with stego techniques) include the time of key calculation on the receiver as well as the sender side.

5.3.1. Results of Steganography and 32 bit cryptography

5.3.1.1. Qualitative results

Figure 4 depicts the effect of combination of Steganography and Cryptography (32 bit) on the quality of the cover image (1024x1024). It can be observed that:

- Pseudorandom Substitution combined with Diffie-Helman produces best qualitative result followed by pseudorandom substitution with DES.
- DCT combined with DES produces the worst qualitative result.

In the similar manner, the impact of this scheme on images of different size i.e. 1536x1536, 2048x2048, 3072x3072, 4096x4096 pixels was recorded.

Figure 4(a). Original Image

Figure 4 (b). Result of applying DCT

Figure 4(c). Result of applying Distortion

Figure 4 (d). Result of applying Substitution

Figure 4(e). Result of DES plus DCT

Figure 4(f). Result of Diffie-Helman plus DCT

Figure 4(g). Result of DES plus Substitution

Figure 4(h). Result of Diffie-Helman plus Substitution

Figure 4(i). Result of DES plus Distortion

Figure 4(j). Result of Diffie-Helman plus Distortion

Figure 4. Impact of proposed technique on images (Image size = 1024X1024 pixels)

5.3.1.2. Qualitative results

Figure 5 depicts the total time taken by a complete process of the combination including the time on sender and receiver side. It can be observed that:

- Distortion combined with DES has minimum time complexity
- DCT combined with Diffie-Helman has maximum time complexity
- Time complexity for all the combinations increases with an increase in the image size.

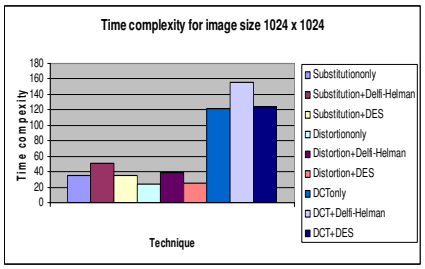

Figure 5(a). Time Complexity (1024X1024 pixel)

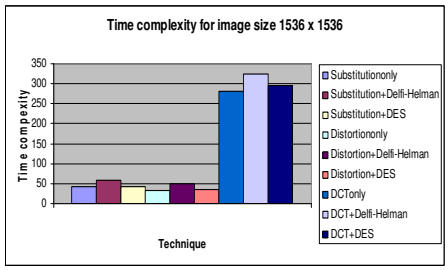

Figure 5(b). Time Complexity (1536X1536 pixel)

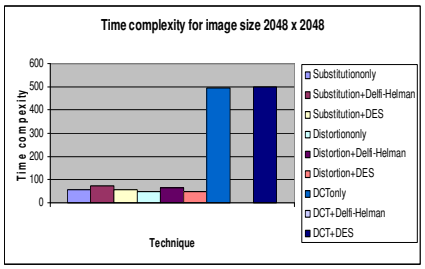

Figure 5(c). Time Complexity (2048X2048 pixel)

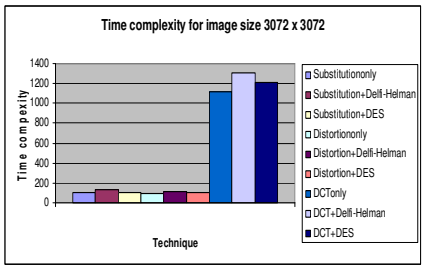

Figure 5(d). Time Complexity (3072X3072 pixel)

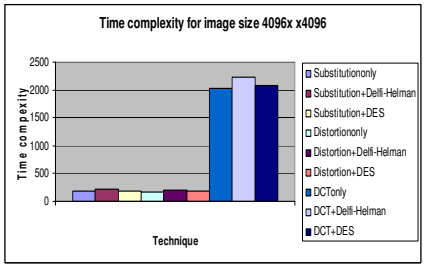

Figure 5(f). Time Complexity (4096X4096 pixel)

Figure 5. Impact on Time complexity of Proposed Technique

5.3.2. Results of Steganography and 64 bit cryptography

5.3.2.1. Qualitative result

Figure 6 depicts the effect of combination of Steganography and Cryptography (64 bit) on the quality of the cover image (2048x2048). It can be observed that:

- Pseudorandom Substitution combined with Diffie-Helman produces best qualitative result followed by pseudorandom substitution with DES.
- DCT combined with DES produces the worst qualitative result.

In the similar manner, the impact of this scheme on images of different size i.e. 3072x3072, 4096x4096, 5120x5120 pixels was recorded.

Figure 6(a). Original image

Figure 6(b). Result of applying DCT only

Figure 6(c). Result of applying Distortion

Figure 6(d). Result of applying Substitution

Figure 6(e). Result of a DES plus Substitution

Figure 6(f). Result of Diffie-Helman plus Substitution

Figure 6. Impact of proposed technique on images (Image size = 3072X3072 pixels)

5.3.2.2. Results of time complexity

Figure 7 depicts the total time taken by a complete process of the combination including the time on sender and receiver side. It can be observed that:

- Distortion combined with DES has minimum time complexity
- DCT combined with Diffie-Helman has maximum time complexity
- Time complexity for all the combinations increases with an increase in the image size

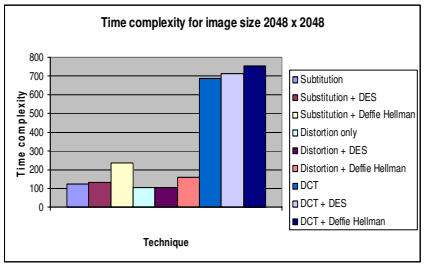

Figure 7(a). Time Complexity (2048X2048 pixel)

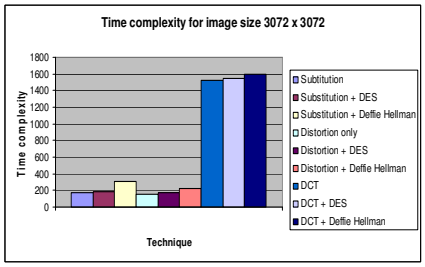

Figure 7(b). Time Complexity (3072x3072 pixel)

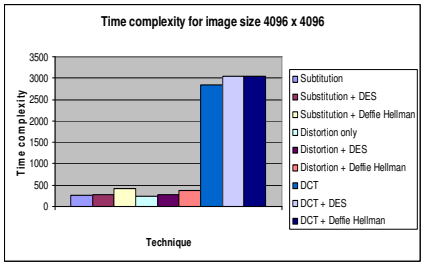

Figure 7(c). Time Complexity (4096x4096 pixel)

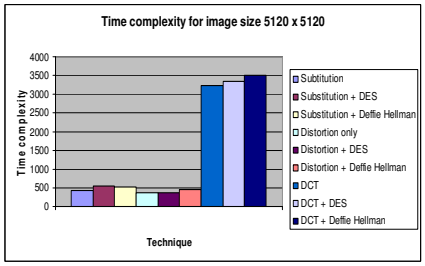

Figure 7(d). Time Complexity (5120X5120 pixel)

Figure 7. Impact on Time complexity of Proposed Technique

6. CONCLUSION

In this paper a new scheme of combining steganography and cryptography has been proposed. Where steganography eliminates any chances of detection of hidden data being present in the cover image, text, etc., cryptography ensures data confidentiality by changing the very form of data. Thus the hybrid approach ensures a higher degree of data security compared to either of the techniques applied alone. After analysing the results of the application of the proposal it can be concluded:

- The time complexity of this hybrid process is much more than that of pure steganography.
- As the size of the key used for encryption and decryption increases time complexity further increases.
- There is no major effect on the process of steganography on adding it to cryptography because the data being embedded is in the form of bits in either case.
- On increasing the size of the image used as a cover, the time complexity increases even more.
- DCT Combined with Diffie-Helman has the highest time complexity in comparison to any other proposed combination.
- The pseudorandom substitution combined with any cryptographic technique provides least distortion in image quality.

These results can be very useful to researchers who wish to use both steganography and cryptography to secure data in communication networks.

ACKNOWLEDGEMENTS

The authors would like to thank everyone, just everyone!

REFERENCES

[1] Neil F. Johnson and Sushil 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] Clair, Bryan, "Steganography: How to Send a Secret Message", 8 Nov. 2001 www.strangehorizons.com/2001/20011008/steganography.shtml.

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

[4] Rhodas, G. B., "Method and Apparatus Responsive to a Code Signal Conveyed Through a Graphic Image", U.S. Patent 5,710,834, 1998.

[5] Swanson, M. D., 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] Bender, W., D. Gruhl, and N. Morimoto, "Techniques for data hiding", IBM Systems Journal , vol. 35, no. 3/4, 1996, pp. 131-336.

[7] Moller. S.A., 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] Gruhl, D., 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] Kurak, C., and J. McHughes, "A Cautionary Note On Image Downgrading", in IEEE Computer Security Applications Conference 1992, Proceedings, IEEE Press, 1992, pp. 153-159.

[10] Van Schyndel, R. G., 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] Johnson, N. F., and S. Jajodia, "Exploring Steganography: Seeing the Unseen", IEEE Computer, vol. 31, no. 2, 1998, pp. 26-34.

[12] Maxemchuk, N. F., "Electronic Document Distribution", AT&T Technical Journal, September/October 1994, pp. 73-80.

[13] Low, S. H., et al., \Document Marking and Identifications Using Both Line and Word Shifting," in Proceedings of Infocom'95, 1995, pp. 853-860.

[14] Low, S. H., 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] Low, S. H., 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] Rhodas, G. B., "Method and Apparatus Responsive to a Code Signal Conveyed Through a Graphic Image", U.S. Patent 5,710,834, 1998.

[17] Sujay Nararayana and Gaurav 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, December 2010.

[18] Shailender Gupta, Ankur Goyal And Bharat Bhushan, "Information Hiding Using Least Significant Steganography and Cryptography", I. J Modern Education and Computer Science, vol. 6, pp. no. 27-34, IJMECS-2012.