

Data Security by a Hybrid Mechanism

Priya Rawat¹, Nidhi Gupta², Suman Dagar³

M.Tech Scholar, ECE, NGF College Of Engineering, Palwal, Haryana-121102, India¹

Assistant Professor, ECE, NGF College Of Engineering, Palwal, Haryana-121102, India²

HOD, ECE, NGF College Of Engineering, Palwal, Haryana-121102 India³

Abstract: With the growing internet technology, the number of intruders trying to steal the confidential information has grown exponentially. In the recent past, hybrid mechanisms that use steganography mechanism to hide the encrypted data are proposed. The salient features that these hybrid security mechanisms should possess are high Peak Signal to Noise Ratio (PSNR), data embedding capacity, entropy and low computational time. This thesis also proposes a hybrid security mechanism that emphasizes on embedding capacity and entropy. To improve randomness, the use of chaos process wherever possible is done while for improving embedding capacity the steganography process employed is Improved Bit Plane Complex Steganography (IBPCS). In addition, for efficiency improvement hierarchical visual cryptography is used. The scheme is implemented in MATLAB-10 and several performance metrics are used to evaluate the efficacy of proposed technique in comparison with others in literature. The results show that the proposed mechanism has high embedding capacity and high security with moderate decrease in PSNR value.

Keywords: Steganography, Cryptography, IBPCS, MATLAB

INTRODUCTION

As the technology is advancing, the use of internet is growing and hence, the hacker finds it more appropriate to intercept the data by applying various attacks. So researchers continuously search and develop novel security mechanism to curb these attacks. Two most prominent solutions are cryptography and steganography. Cryptography can be defined as the encoding of secret data into a form which can be read by the intended user only. Cryptography is classified into two categories: Symmetric key cryptography and Asymmetric key cryptography. In symmetric key cryptography, same key is used for encryption at sender side and for decryption at receiver side. While in asymmetric key cryptography, also known as public key cryptography, two different keys i.e. one public and one private is used. Public key is known to all and it is used for encryption while private key is known only to the intended recipient used for decryption. Schemes based on former are considered to be faster as compared to those based on later who in contrast provide more security. On the other hand, steganography doesn't encode the data rather it hides the data into a cover media which can be an image, video etc. It can be broadly classified into two domains: Spatial (Time) domain and Transform (Frequency) domain. Spatial domain techniques preserve picture quality and have high PSNR value but are not robust, while transform domain techniques provide robustness with the drawback of poor picture quality. Using any of the above two techniques standalone is not sufficient, as the attacks have grown more sophisticated. So, researchers have combined both of these to form hybrid security mechanism. This mechanism encodes as well as hides the secret data which makes it more difficult for the intruder to retrieve the original secret data. In this paper, a new hybrid mechanism has been proposed which tries to inculcate the advantages of both cryptography and steganography. The rest of the paper is organized as follows: Section 1.2 gives the detailed analysis of previously developed hybrid approaches and the objectives taken into consideration while section 1.1 discusses the proposed approach.

1. MAJOR CHALLENGES AND ISSUES

Researchers have tried different combinations of various techniques to have optimized results in terms of various parameters like security, robustness, time complexity, size etc.

After analyzing, it is found that different hybrid mechanisms lead to different strengths and some overheads. Some are better in terms of security and some in terms of time complexity but there is no security mechanism which has very high embedding capacity. Though Divya Chaudhary et. al. [36] has applied Huffman compression technique to increase size of embedding data still there is a need for such a mechanism which can further increase embedding capacity. Also, there is no focus on entropy in any mechanism which in turn increases the unpredictability of data. The literature shows that employing visual cryptography improves confidentiality of data with marginal increase in time complexity as discussed by Divya Chaudhary et.al. [36]. This technique can further be improved by the use of hierarchical visual

cryptography instead of plain Visual cryptography. So, a novel hybrid security mechanism has been proposed which serves the following objectives:

- To have high data embedding capacity.
- To preserve picture quality.
- To have high Entropy.
- To have high PSNR value.
- To have high privacy and security.

1.1 PROPOSED TECHNIQUE

The proposed technique is described in Figure 1.1. Here the secret message i.e. plain text is first compressed through a compression technique, which reduces the size or number of data bits and then a cryptographic technique is applied on the compressed data to encrypt the data. After that a spatial domain steganography technique is applied on this encrypted data to hide it into a cover image which finally generates the stego image.

At the receiver side, reverse operation is performed to extract the original information. As shown in Figure 1.2, the stego image is first processed with inverse steganography technique. Then the data obtained from this is applied with inverse cryptography technique to decrypt the data and finally, with inverse compression this decrypted data is uncompressed to retrieve the secret data i.e. plain text.

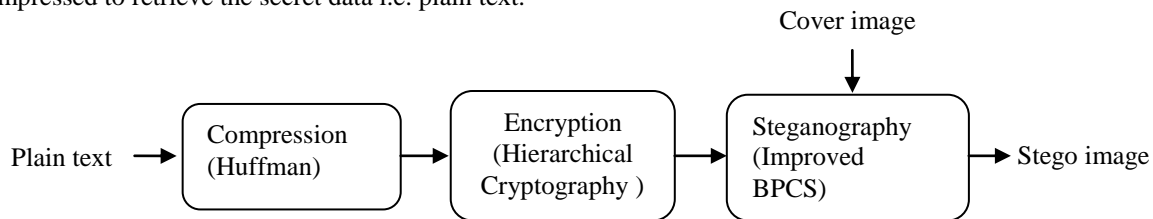


Figure 1.1 Block diagram of proposed technique at sender side

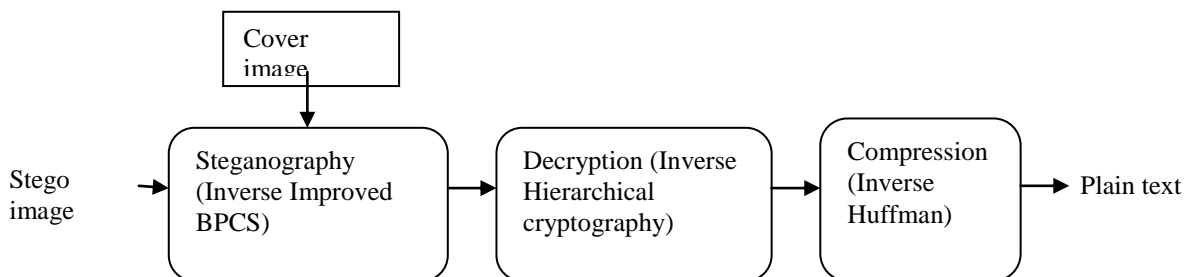


Figure 1.2 Block diagram of proposed technique at receiver side

1.1.1 Compression Technique used

As shown in Figure 1.2, compression technique employed in proposed mechanism is Huffman compression. The purpose of using this first stage is to compress or reduce the size of data to be transmitted so that amount of secret data to be encrypted and finally embedded in the cover image gets increased which in turn increases embedding capacity. Huffman coding is used in this paper.

1.1.2 Cryptography Technique used

After first step of compression next block in proposed mechanism is a cryptography technique. In a three layer security mechanism this is second layer. Here hierarchical visual cryptography technique is chosen for encryption/decryption of data [33] because it is very simple technique with low time complexity and high security. In this scheme, data is first converted into 2 shares (see Figure 1.3) where a share is defined as a component of data which contains partial information and seems as a noise i.e. meaningless to unauthorized users. Here first share i.e. share1 is generated by using random numbers. In proposed mechanism, these random values are generated by chaotic function which increases the unpredictability of random numbers. The way of generation of random number using chaotic function is explained. And the second share i.e. share2 is generated by using share1 and the data i.e. if data bit is 1, compliment of share1 is written into share2 else bit of share1 is copied into share2.

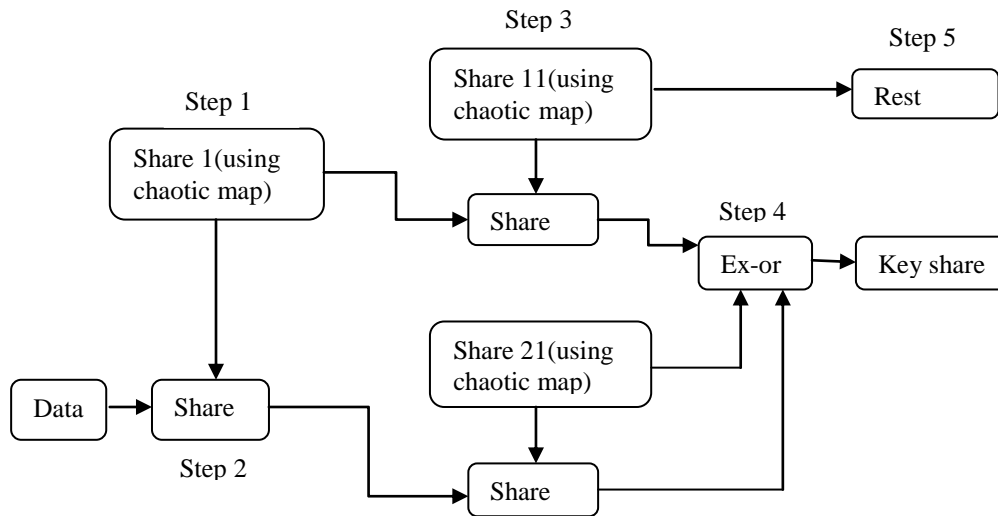


Figure 1.3 Hierarchical cryptography encryption technique

1.1.3 Chaotic Map:

A chaotic map is that which deals with non linear dynamical values where dynamical means the value changes over time based on its current state. This map includes generation of random sequence for various 1D and 2D discrete maps based on mathematical equations and relations i.e. Logistic map, Cubic map, Ricker's map, Sin map, Henon map, Gingerbreadman map, Burgers' map, Tinkerbell map, etc.

1.1.4 Steganography Technique used

In the proposal, third layer of security is introduced by the steganography technique. Here Improved BPCS (Bit Plane Complexity Segmentation) which is a spatial domain steganography technique [9] is used to hide/embed the data into the cover image is. This technique is chosen for its very special feature of high embedding capacity. As all other techniques have limited embedding capacity, the said scheme nourishes this property. In this scheme, data is embedded into noise like regions which cannot be differentiated by human eye.

If the image is RGB i.e. coloured image then eight bit planes are formed for each R, G and B planes. Therefore, total 24 bit planes are generated for a coloured image. Now, each of the bit planes is divided into 8x8 size blocks. Then complexity of each block is calculated. Complexity is defined as the maximum number of adjacent pixel changes in that block and is denoted by Cmax. A parameter α is also calculated by using the chaotic map i.e. Logistic map equation, which has been defined earlier, then the product of these two parameters i.e. $\alpha.C_{max}$ is called threshold complexity.

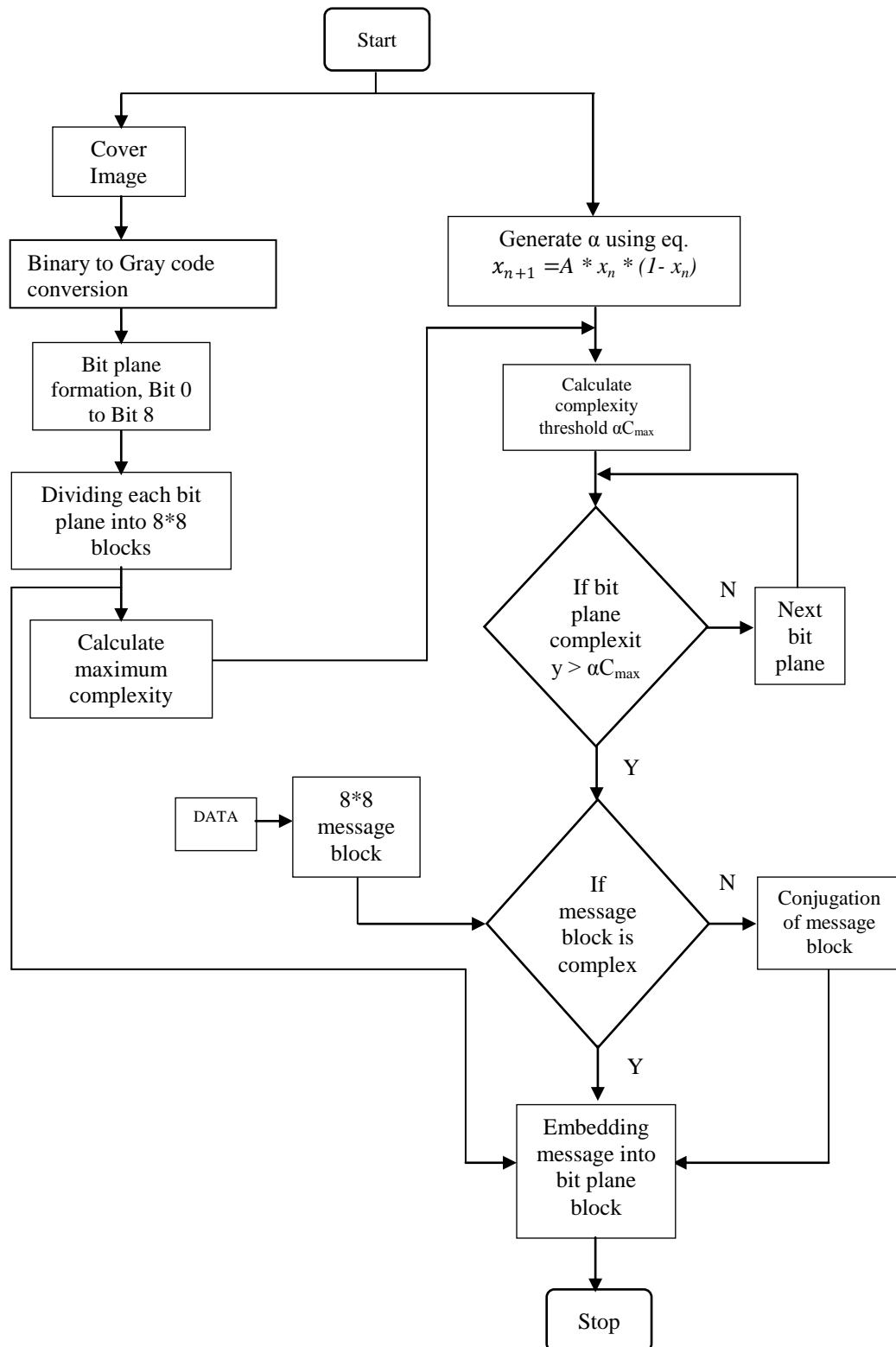


Figure 4.4 Flowchart of Improved BPCS

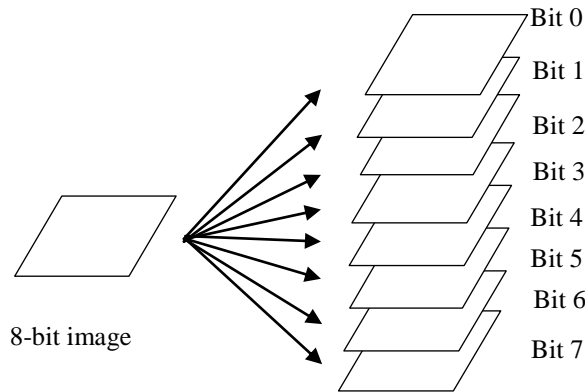


Figure 4.5 Dividing of bits to form bit planes

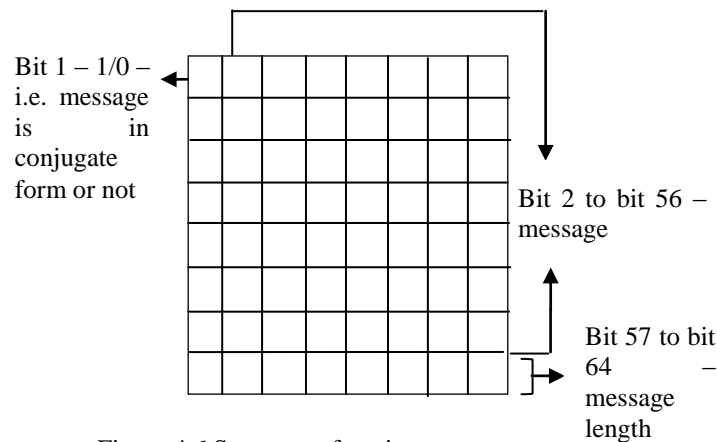


Figure 4.6 Structure of conjugate map

As shown in Figure 4.6, first bit i.e. bit 1 of conjugate map contains the information about whether this block is also conjugated or not. And from second bit position i.e. from bit 2 to bit 56, conjugate status of message blocks is stored i.e. if the block is conjugated, 1 is stored at that place else 0 is stored. This process continues for each message block. The last row of this map block i.e. bit 57 to bit 64 contains information regarding the length or size of data. First conjugate map is embedded into the cover image and then message blocks so that while extracting the message blocks at the receiver side, their conjugate status and size is known in advance. In this technique, first a basic threshold for each bit plane is set, then some incremental value is added in it to make it dynamic threshold. This threshold is not constant even in the same bit plane.

2. SIMULATION SERUP PARAMETERS

The experiments are carried out on a personal computer. Table 2.1 provides the specifications and set up parameters.

Table 2.1 Set up Parameters

Processor	Core-i3 1.7GHz RAM 4GB
Image size	64*64 128*128 256*256 512*512 1024*1024
Image type	.jpg
Simulation tool	MATLAB 7.14.0.739 64 bit (win 64)
Software version	2010
Text used for embedding	“ABCDEFABCDEFABCD”

Huffman encoding	Number of symbols n=26 Alphabets used are 'A to Z'
Hierarchical visual cryptography	Number of share in which data is divided=4
Threshold parameter α used in BPCS technique	$\alpha = A * xn * (1 - xn)$ Where A=3.7 and xn=0.4

2.2 SNAPSHOTS (PERCEPTUAL QUALITY)

Comparison of various images after applying the different approaches is given in Figure 5.1.
























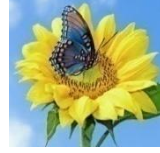






Original image	Image after applying Peipei Shi et. al. Method	Image after applying Piyush Marwaha et.al. method	Image after applying Md. Rashedul et.al. method	Image after applying Divya Chaudhary et. al. method	Image after applying Proposed technique
					
					
					
					
					

Figure 2.1 Snapshots

As per results of visual analysis, it is not possible to identify the presence of any type of information in the image. Both images are seems to be alike. Results for this parameter are comparable for all other techniques.

3. RESULTS

Encrypted code Analysis

Table 3.1 Code Assessment

Cryptography Technique	Original Secret	Encrypted Data	Decrypted Data
Proposed technique	ABCDEFABCDEFABCD	İ Đ (Key Share) . ã ; P (Rest Share)	ABCDEFABCDEFABCD
Divya Chaudhary et. al.	ABCDEFABCDEFABCD	Üaá@ (Share1) >x@,À (Share2)	ABCDEFABCDEFABCD
Md. Rashedul et. al.	ABCDEFABCDEFABCD	÷üjðK@hTMØ	ABCDEFABCDEFABCD
Piyush Marwaha et. al.	ABCDEFABCDEFABCD	++sC rÄP^«@{A	ABCDEFABCDEFABCD

After analyzing table 3.1, it is observed that encrypted result of all the techniques is in unreadable form which proves that all the compared mechanisms are successful in this test. Hence, by visual inspection, there is no possibility to detect the information by the hacker. If any technique fails in this test, comparison of any other analysis has no worth. Also, it can be observed from the above table that the proposed technique and Divya Chaudhary et. al.[36] has compressed data as well due to usage of Huffman compression which makes these techniques more efficient and complex.

3.2 Key Space Analysis

Table 3.2 Key Space Analysis

Techniques	Proposed technique	Divya Chaudhary et. al.	Md. Rashedul et. al.	Piyush Marwaha et. al.	Peipei Shi et. al.
Key size	Same as data length(say l)	Same as data length(say l)	128 bits	64 bits	No key
Key space	2^l	2^l	2^{128}	2^{64}	-

A good encryption scheme should have a large key space as it is directly related with brute force attack. As the key size increases, possibility of this attack decreases. Table 3.2 depicts that key size for the proposed technique and Divya Chaudhary et. al.[36] is not fixed, it is varying with data length. For a large amount of data, the key size will be very large and hence the key space which ultimately increases the resistance to brute force attacks. This result makes this technique more secure for bigger size of secret data.

4. CONCLUSION

In this thesis work a secure hybrid mechanism has been proposed for communication network which not only uses steganography and cryptography but also uses Huffman coding for increasing the embedding capacity. Our proposed mechanism is better in terms of various parameters than other author's work mentioned in the literature. On comparison, it is found that our mechanism is better from the above two in terms of various parameters as can be seen from the Table 4.1:

- The proposed mechanism has good picture quality.
- Since our mechanism uses hierarchical visual cryptographic mechanism using chaotic map, therefore its entropy is high.
- Our mechanism has highest embedding capacity since it uses BPCS steganography which has high embedding capacity and Huffman coding also has been used for data compression.
- Our proposed mechanism provides much more security with increased complexity.

Table 4.1 Overall Comparisons

Parameters	Divya Chaudhary et. al.	Md. Rashedul et. al.	Piyush Marwaha et. al.	Peipei Shi et. al.	Proposed technique
Encrypted Code	Unreadable and compressed	Unreadable	Unreadable	Unreadable	Unreadable and compressed
Key Space	Large and varying	Small and fixed	Small and fixed	No key space as there is no key	Large and varying
Correlation Coefficient	Higher	High	Highest	Highest	Highest
UIQI	Higher	High	Highest	Highest	Highest
PSNR	Highest	Higher	Lowest	Low	High
Embedding Capacity	Higher	Low	Low	High	Highest
Entropy	Higher	Low	Low	High	Highest

As per inspection it is concluded that, till now there is no hybrid mechanism which emphasizes on both embedding capacity and entropy which are also important parameters for any security technique. Also all other results are comparable with other mechanisms i.e. with no overheads required parameters are enhanced.

5. FUTURE SCOPE

Currently, the proposed scheme has moderate value of PSNR, which can further be increased by using a more efficient technique with the proposed one at the cost of high time complexity to achieve higher PSNR value.

REFERENCES

- [1] Nentawe Y. Goshwe, "Data Encryption and Decryption Using RSA Algorithm in a Network Environment", in proceedings of International Journal of Computer Science and Network Security, Vol. 13, Issue 7, pp 9-13, 2013.
- [2] Md. Rashedul Islam, Ayasha Siddiq, Md. Palash Uddin, Ashish 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.
- [3] Pye Pye Aung, Tun Min Naing, "A Novel Secure Combination Technique of Steganography and Cryptography", in International Journal of Information Technology, /modelling and Computing (IJITMC), Vol. 2, pp 55-62, 2014.
- [4] Shingote Parshuram N., Syed Akhter Hussain, Bhujpal Pallavi M., "Advanced Security using Cryptography and LSB Matching Steganography", in International Journal of Computer and Electronics Research, Vol. 3, pp 52-55, 2014.
- [5] Md. Jakir Hossain, "Information-Hiding Using Image Steganography With Pseudorandom Permutation" in proceedings of Bangladesh Research Publications Journal, Vol. 9, Issue 3, pp 215-225, 2014.
- [6] Pallavi Vijay Chavan, Dr. Mohammad Atique, Dr. Latesh Malik, "Design and Implementation of Hierarchical Visual Cryptography with Expansionless Shares" in proceedings of International Journal of Network Security & Its Applications, Vol. 6, No. 1, 2014.
- [7] Mahmoud E. Hodeish, Dr. V. T. Humbe, "State-of-the-Art Visual Cryptography Schemes" in proceedings of International Journal of Electronics Communication and Computer Engineering, Vol. 5, Issue 2, pp 412-420, 2014.
- [8] Vinish Alikkal, Dr. T. Senthil Prakash, Ajmal Hussain, "Enhanced Hierarchical Design for Visual Cryptography-Overview" in proceedings of International Journal on Engineering Technology and Sciences, Vol. 2, Issue 4, 2015.
- [9] Divya Chaudhary, Shailender Gupta, Manju Kumari, "A Novel Hybrid Security mechanism for Data Communication Networks" accepted for publication in Inderscience Journal, 2015.
- [10] Yamini Jain, Gaurav Sharma, Gaurav Anand, Sangeeta Dhall, "A Hybrid Security Mechanism based on DCT and Visual Cryptography for Data Communication Networks" accepted for publication in CSI-2015 Journal.
- [11] <https://securelist.com/analysis/publications/66978/mobile-cyber-threats-a-joint-study-by-kaspersky-lab-and-interpol/>