# DESIGN AND PERFORMANCE ANALYSIS OF DIVERSE GENERIC DATA HIDING ALGORITHMS IN CRYPTOGRAPHY

K Saravanan[1], T Purusothaman[2], T Velmurugan[1] and KVN Kavitha[1]
[1]School of Electronics Engineering, Vellore Institute of Technology, Vellore, India
[2]Department of Information Technology, Government College of Technology, Coimbatore, India
E-Mail: kasisaravanan@vit.ac.in

## ABSTRACT

An effective cryptographic algorithm plays a major role in secure communications which is important for today's digital world. Network security primarily depends upon Cryptographic algorithms as its applications are. The main goal of a cryptographic algorithm is to satisfy four conditions which are Integrity, Confidentiality, Authentication and Nonrepudiation. Though there are numerous algorithms there is a chance of drudge caused due to adversaries and hence for the better security we in this paper considered few existing algorithms and on few modification we compared them through their performance level on considering few factors like encryption time, throughput, computational time and memory usage. We also added a new concept related to steganography in this paper where that technique is evaluated based on histogram level. The proposed algorithm is effective for secure communications in this digital era. In this study is made particularly for the evaluation of comparison and performances of cryptographic algorithms.

**Keywords:** cryptography, cipher text, encryption, decryption, steganography, QR code, RSA-shamir, polyalphabetic-LZW, advanced ASCII based cryptography using matrix operation.

## 1. INTRODUCTION

Today in the present world, for transmitting the data securely through a public network it is obviously indeed of cryptography. Cryptography is a technique which involves encryption of data on the sender side and decryption of cipher-text on the receiver side in a secured network. Though there exist numerous cryptographic algorithms there is somehow a chance of drudge taking place caused by the adversaries. Hence it is leading to invention of new algorithms day by day. There is a lot of research going for the advanced techniques in new cryptographic algorithms by the researchers for the sake of better security. Similarly steganography is also a data hiding technique but it differs from cryptography. Steganography is a technique to hide a message, file, video or image within another message, file, video or image. In a cryptographic algorithm, the encrypted cipher-text can't be decrypted without knowing the decryption key whereas in steganography, the message is hidden inside some other format like an image and many people don't detect the presence of a message inside it. On combining, these two produce a two level security algorithm is proposed based on it.

In this paper we evaluate the performance of the algorithms that we encounter and are compared. Firstly the performance of each and every existing algorithms that we encountered are evaluated and then on few modifications further the performances of new obtained algorithms are measured and compared internally and overall comparison takes place only for the algorithms that are obtained after modifications. Similarly for steganography algorithm the performance is evaluated with both normal image as well as QR image [10].

## 2. REVIEW OF RELATED WORK

We considered few algorithms for the performance evaluation purpose and these are explained in details which are as follows:

### 2.1 RSA-shamir algorithm

RSA is a commonly used as well as a widely adopted public key based cryptographic algorithm [1] [8] [9]. It is used by many software companies for adding security to their products. RSA has various applications like digital signatures, key exchange, encryption of smaller data blocks, etc. RSA uses an encryption block and key which are both variable in size always. Similar to RSA, Shamir secret sharing is also one of the known cryptographic algorithm. In this shamir sharing the secret is split into pieces and shared then the original secret is recovered with the help of Lagrange's polynomial. Hence Shamir secret sharing involves in two algorithms: one is sharing and the other is recovery. Now these two algorithms are combined in our paper and the performance is evaluated.

### 2.2 Polyalphabetic-LZW algorithm

Polyalphabetic cipher [1] is similar to monoalphabetic cipher where each letter in a word or a sentence is replaced or substituted with the other. The difference between mono and polyalphabetic cipher is, in monoalphabetic the same letter in a word will be substituted with other letter which will be same for both where it is easy to recover the message. But in polyalphabetic cipher, the same letter in a word will be substituted with different other letters. For example, an `a' may be represented by a 'j', 'r', or 'x' depending on where it occurs in the original message. This cipher was invented by anticipating that it may greatly confuse the cryptanalysts.

LZW is an algorithm used to compress data without any loss and this algorithm is used universally. The implementation of the algorithm is very simple and it results in high throughput when it is used in hardware implementations. The codes range from 0-255 where each code denotes an 8-bit character sequence and the codes in the range 256-4095 are assigned to sequences found as data is being encoded and those assigned codes are stored in a dictionary. At each and every stage of compression, the input data bytes are grouped together into a sequence and this grouping process continues till the next character is able to form a sequence which can't be matched to a code in the dictionary. In the output, the sequence of a code without including that character is added and the new code representing the sequence created by that character is added to the existing dictionary. Now on combining these two algorithms we evaluated the performance of the algorithm.

### 2.3 Advanced ASCII based cryptography using matrix operation

It is a new cryptography technique. It changes the data into a set of different computer codes and those codes are in turn converted into cipher-text by using a word range. This strategy additionally makes use of matrix multiplication that creates an environment where the information is safer from the intruder attacks [4]. Another strategy of this algorithm makes use of is authentication using a single id which is alphanumeric in nature and such ids are provided to each and every receiver. In the initial stage, each and every receiver is given a unique id and they are stored in the sender's database. Id's are made of 3 alphabets and one range. Then it is converted into receiver's id in ASCII form.

A word number is generated as soon as those values were summed up on the whole. The receiver gets the encrypted information and along with it he/she also gets the key and a random range set. The key received is then decrypted and it is compared with that of the receiver's id. The original information was encrypted on that basis of those two id matches. The user is identified with unique id and calculating the computer code values of the id. Then decode the palindrome's word range of information victimization.

Now on evaluating the performance of this algorithm, we will be comparing the results of the algorithms that we encountered in this paper.

### 2.4 LSB steganography

The Least Significant Bit (LSB) is a well known steganography technique used in spatial domain. The LSB denotes the lowest significant bit present in the image pixel's byte value [5]. This technique works by embedding the message in LSB positions of all the pixels in an image. Thus this technique works on the basis that the precision level in various image formats is such that it can't be seen by an average human. Thus an average human eye can't differentiate between a modified image (slight change in the colours used) from that of an original image.

This concept is practiced basically for images or videos. But we in this paper extended this concept to QR images where the original data will be compressed in the QR images and the LSB technique is performed.

## 3. DESIGN OF THE SYSTEM

The figure below gives the entire idea of cryptography system.

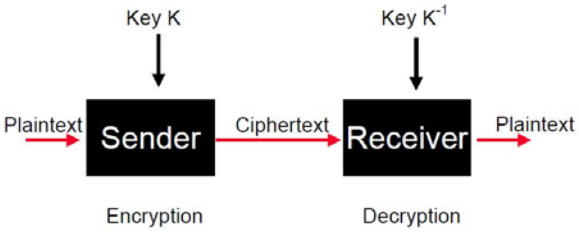

**Figure-1.** Block diagram of cryptography.

At the encryption side the plain text is encrypted depending upon the algorithm designed [3]. The key will be utilized if the algorithm is indeed with that.

The encrypted text, called as cipher text will be obtained as per the algorithm that is used. Now this cipher text will be decrypted by the receiver in order to recover the original text [7], [2].

So at the receiver side the obtained cipher text will be decrypted with the particular algorithm that is used during encryption time. So with the decoding process of that particular algorithm the cipher will be decoded by the receiver.

Thus the original text will be recovered from cipher text. All the mentioned above algorithms will follow the same procedure, the only change is the algorithm that will be using for encryption and decryption differs.

The figure below gives the idea of steganography system.

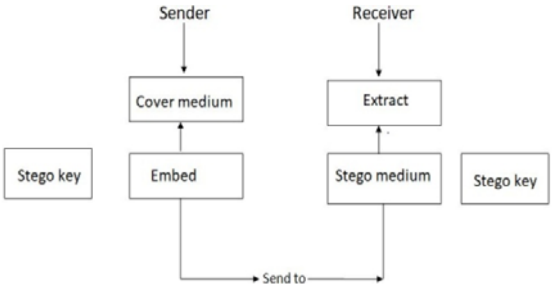

**Figure-2.** Block diagram of steganography.

The steganography system is also similar to cryptography system.

The sender embeds the data in an image using LSB technique resulting to stego-image [6]. The data can be a text file or an image or a video file etc. The obtained stego-image resembles same as the original image and hence it is not easy one to predict that there is something hidden through naked eye.

Now the obtained stego-image is sent to the receiver along with the original image and on performing decoding process of particular technique one can extract the original data.

So we used the similar technique for QR images too where initially the data will be compressed in those images.

## 4. PERFORMANCE OF ALGORITHMS IMPLEMENTED

This section deals with comparison of the algorithms based on their performance.

On the basis of performance of different algorithms for encrypting text files, the proposed algorithm uses Polyalphabetic-LZW, RSA-Shamir and Advanced Ascii based Cryptography using Matrix Operation and their performances are evaluated using various parameters like memory usage, encryption time, computational time and throughput. Similarly the LSB technique for normal images as well as QR images is compared through histogram level of the graphs.

The prime factor is encryption time and it is calculated for those algorithms. It is the time taken in forming a cipher-text from a plain text. When those three algorithms were compared it showed that Polyalphabetic-LZW takes more encryption time whereas RSA-Shamir takes less encryption time compared to other two. The memory usage by each and every algorithm is to be considered as a memory byte level. Advanced ASCII based Cryptography using Matrix Operation algorithm takes larger memory than other two. Next the computation time is computed and we see that RSA-Shamir takes minimum time.

Throughput of encryption is calculated which is defined as the ratio of total plain text in bytes encrypted to the encryption time in seconds. Hence on computing for all the algorithms we find RSA-Shamir has more throughput and hence it can transmit large amount of data if required.

The simulation results show that RSA-Shamir has better performance when compared with rest algorithms in all test cases.

For steganography system the histogram level of images is compared and on observing QR images has better security as well as better performance.

## 5. SIMULATION RESULTS

This section deals about the results which were obtained when the algorithms were implemented by MATLAB simulation. Comparison of the algorithms through different parameters is computed and the values are listed in the following tables along with the diagrams required.

**Table-1.** Encryption time.

| **Size of file in bytes** | **RSA-shamir encryption time** (in seconds) | **Polyalphabetic -LZW encryption time** (in seconds) | **Advanced ASCII based cryptograph y encryption time** (in seconds) |
|---|---|---|---|
| 12 | 0.053155 | 0.073355 | 0.093495 |
| 16 | 0.070124 | 0.164475 | 0.111289 |
| 40 | 0.073227 | 0.422462 | 0.11530 |

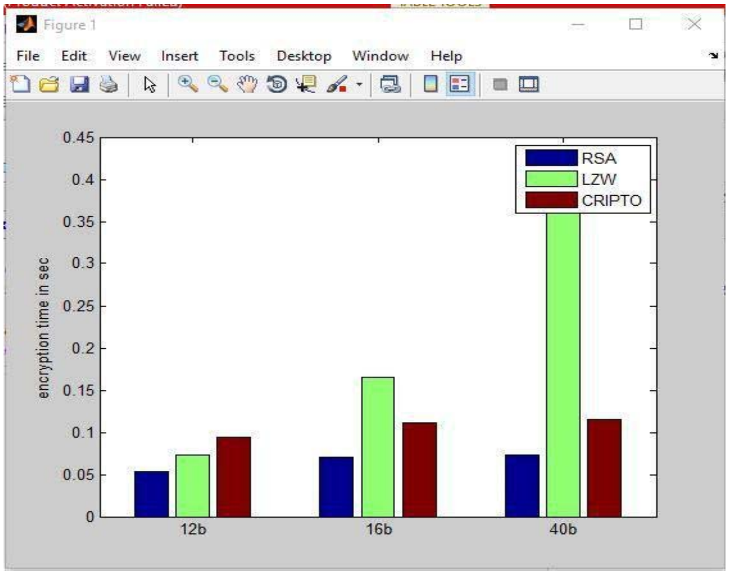

**Figure-3.** Encryption time analysis.

Figure-3 shows the result of encryption time analysis of three algorithms of different size of text files. It is observed that RSA-Shamir takes less time for encrypting the text compared to other two.

In Table-2, a comparison of memory usage by those three algorithms for different file sizes is shown below.

**Table-2.** Memory usage.

| **File size** (Bytes) | **RSA-shamir memory usage** (KB) | **Polyalphabetic-LZW memory usage** (KB) | **Advance ASCII based cryptography memory usage** (KB) |
|---|---|---|---|
| 12 | 647540.736 | 620638.208 | 663236.608 |
| 16 | 647569.408 | 630722.560 | 652947.456 |
| 40 | 650383.36 | 632385.536 | 653168.64 |

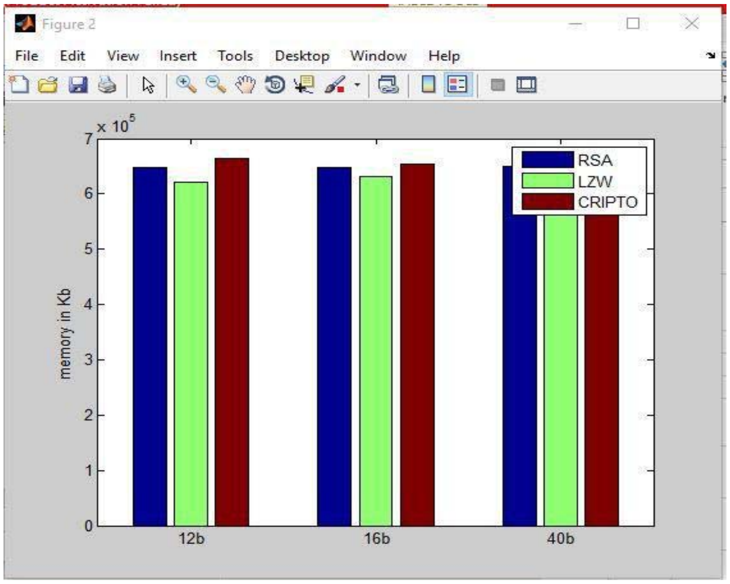

**Figure-4.** Memory usage analysis.

Figure-4 shows the memory usage analysis of the encountered algorithms of different size of text. It is observed that almost in all cases Advance ASCII based Cryptography takes more memory compared to the rest.

Next, comparison of computation time is shown in the following Table-3.

**Table-3.** Computation time.

| **File size** (Bytes) | **RSA-shamir computation time** (sec) | **Polyalphabetic-LZW computation time** (sec) | **Advance ASCII based cryptography computation time** (sec) |
|---|---|---|---|
| 12 | 0.085152 | 0.073693 | 0.209230 |
| 16 | 0.097601 | 0.165430 | 0.168913 |
| 40 | 0.14212 | 0.425768 | 0.187894 |

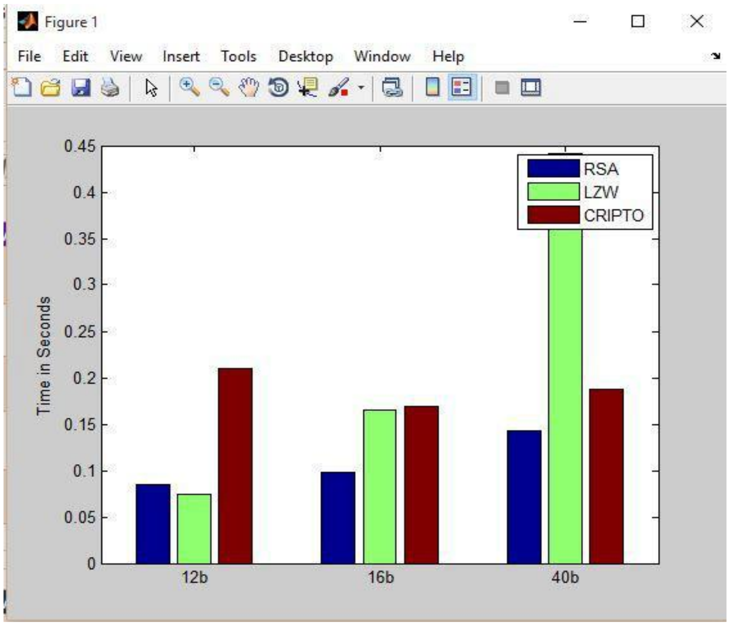

**Figure-5.** Computation time analysis.

Figure-5 shows the result of analysis of computation time of all the algorithms of different sizes of text and we observe that RSA-Shamir takes less computation time and hence it is better than other two.

Next, comparison of throughput of encryption is shown in the following Table-4.

**Table-4.** Throughput analysis.

| File size (Bytes) | RSA-shamir throughput (bytes/sec) | Polyalphabetic-LZW throughput (bytes/sec) | Advance ASCII based cryptography throughput (bytes/sec) |
|---|---|---|---|
| 12 | 225.75 | 163 | 128.35 |
| 16 | 228.16 | 97.27 | 143.76 |
| 40 | 546.2 | 94.638 | 346.92 |

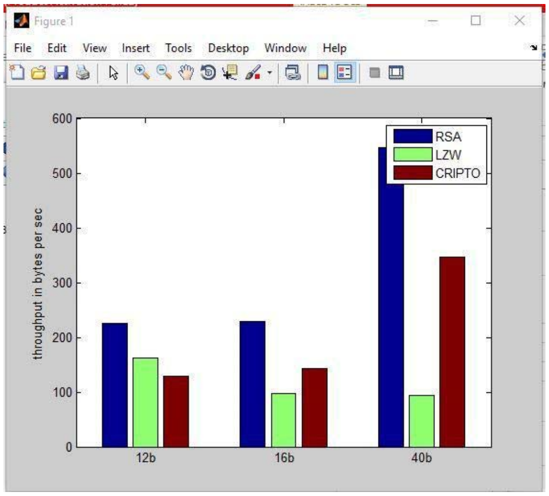

**Figure-6.** Throughput analysis.

Figure-6 shows the result on analysis of throughput encryption of all three algorithms of different size of texts and we observe that RSA-Shamir has more throughputs and hence it can transfer more data.

Now the comparison is for steganography technique and this is shown in the following figures below. (Figure-6)

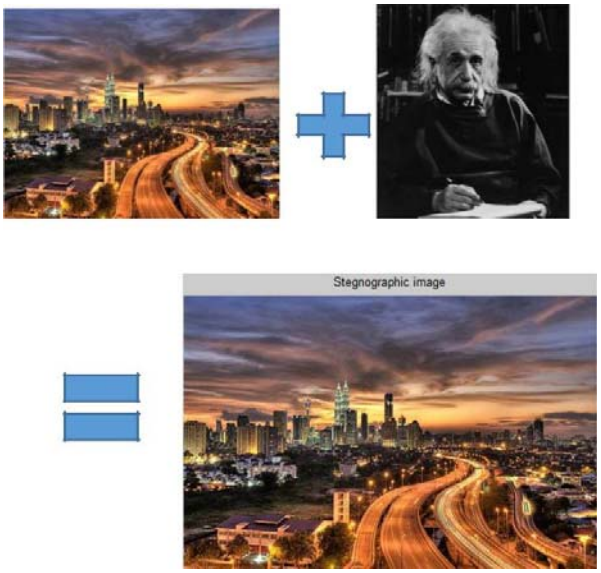

**Figure-7.** Generating stegnographic image.

Now observe the histogram levels of the above Figures.

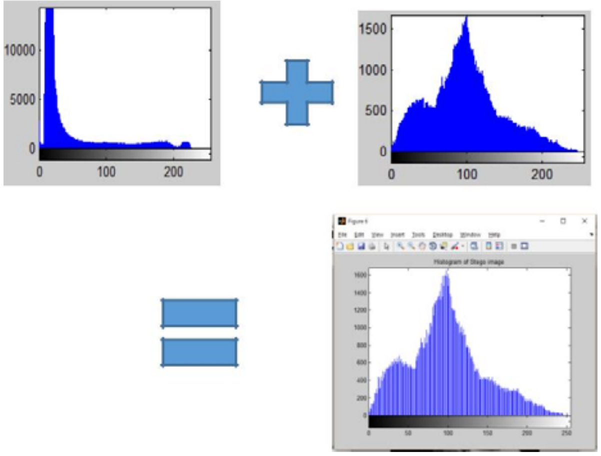

**Figure-8.** The histogram levels.

The LSB technique is performed for the above images and we also observe the histogram levels of that particular image and we see that there are sharp and smooth curves present which differs slightly between original image and stego-image and hence it will be easy for the intruders to recover the data.

Hence we approached the concept of QR images and we see the following results shown below in the figure.

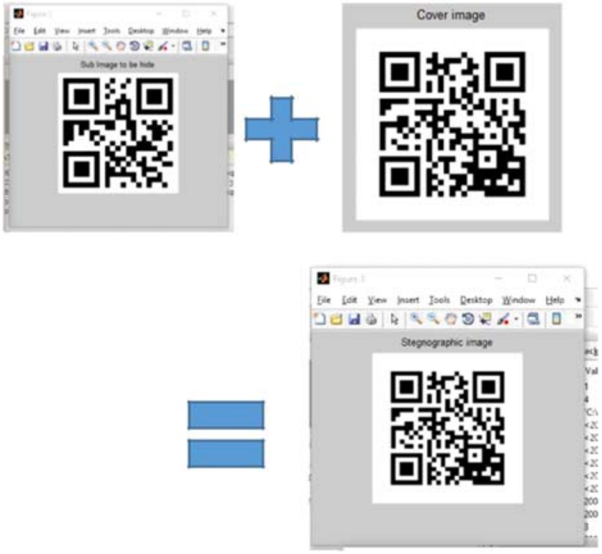

**Figure-9.** The stegnograhic image generation using QR image.

Now we see the histogram levels of these above QR images shown below.

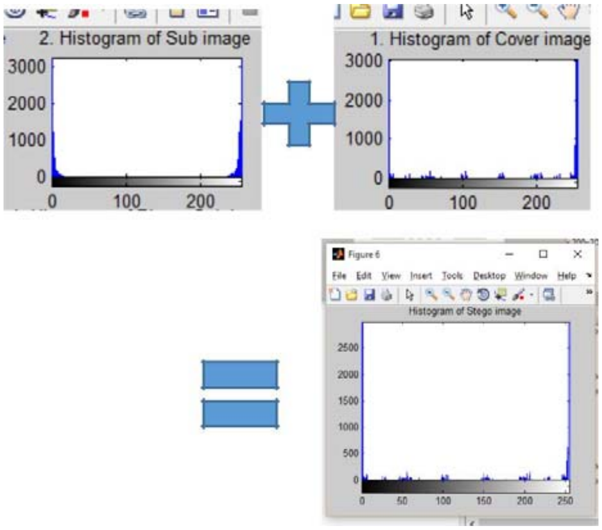

**Figure-10.** Shows the histogram levels of the QR images.

We observe that from above histogram levels of QR images is that both original image as well as stego-image histogram levels are almost same and it is not easy for an intruder to classify original image as well as stego image and cannot recover the data.

## 6. CONCLUSIONS

In this paper we studied various cryptographic algorithms as well as performed few analysis test on these algorithms and we concluded that all the algorithms will have respective advantages as well as disadvantages. So in similar way on performing analysis test on considering few parameters like encryption time, computation time, memory usage and throughput RSA-Shamir algorithm is better in terms of all cases except memory usage. Polyalphabetic-LZW is almost a worse case but for an intruder to decode it takes lot of time.

When come to LSB technique of steganography between normal images and QR images it is better to use QR images as it clearly observed from the histogram levels that QR images provide better security.

In future this work can be extended for images or audio data or videos files. Also focus can be given over decreasing the memory usage and improving the encryption time for a particular file size.

## ACKNOWLEDGEMENTS

The authors gratefully acknowledge the authorities of VIT University for the facilities offered to carry out this work.

## REFERENCES

[1] W. Stallings. 2005. Cryptography and Network Security, Prentice Hall, First Edition.

[2] Diaasalama, Abdul Kader, Mohiy Hadhoud. 2011. Studying the Effect of Most Common Encryption Algorithms. International Arab Journal of e-technology. 2(1): 1-10.

[3] S.P. Deepa, S. Kannimuthu, V. Keerthika. 2011. Data Security using colors and Armstrong numbers. Journal of Electronis and Communication Engineering. 9(1): 13-18

[4] Sanket A. Ubhad, Nilesh Chaubey, Shyam P. Dubey. 2015. Advanced ASCII Based Cryptography Using Matrix Operation, Palindrome Range, Unique id. IJCSMC. 4(8): 66-71.

[5] M. Ram Mohan Reddy, S.S. Divya. 2012. Hiding text in audio using multiple lsb steganography and provide security using cryptography. International Journal of Scientific Technology Research. 1(6): 68-70.

[6] Teoh Suk Kuan, Rosziati Ibrahim. 2011. Steganography algorithm to hide secret message inside an image. Computer Technology and Application, 2: 102-108.

[7] Diaasalama Abd Elminaam, Hatem Mohamad Abdual Kader, Mohly Mohamed Hadhoud. 2010. Evaluation the Performance of Symmetric Encryption Algorithms. International journal of network security. 10(3): 216-222.

[8] Shashi Mehrotra Seth, Rajan Mishra. 2011. Comparative Analysis of Encryption Algorithms for Data Communication. IJCST. 2(2): 292-294.

[9] R. L. Rivest, A. Shamir, A. Adleman. 1978. A method for obtaining digital signature and public key cryptosystem. Communications of the ACM. 21(2): 120-126.

[10] K. Saranya, R. S. Reminaa, S. Subhitsha. 2016. Modern applications of QR - Code for Security. IEEE International Conference on Engineering and Technology. 3: 173-177.