International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

A Secure Message Passing Method using Multi-Layer Adaptive Video Steganography

Jeswin Roy Dcouth, K Somasundaram

Abstract*: Steganography is covert communication of a secret message hidden in a medium passed between the intended sender and receiver with no evidence that the work contains a hidden message. The paper proposes a heuristic approach in steganography to secretly embed message in the cover and make use of the Diffie-Hellman key exchange method to be passed on to a secure channel and to be extracted without being detected. Hence the proposed system is a hybrid crypto stego scehme. The study proposes a new and adaptive steganography method that provides multiple layer of security and adaptiveness in passing secret data which emphasizes on undetectability.

***Index Terms*: Steganography, Diffie-Hellman, QR code**

I. INTRODUCTION

Steganography word was originated from the Greek language. It is derived from two Greek words “stegos” and “grafia” which means “covert writing” [1]. The best approach for covert communication is to combine both cryptography and stegnographic approaches to increase the security level of the system [2].

The focus of this paper is to develop an adaptive steganography method with high security model for passing secret message embedded in the QR code and the obtained stego QR code to be embedded in the frames of the video, which uses both cryptography and steganography principles through a secure medium using Diffie–Hellman key exchange. The digital explosion has led to lack of privacy and major security issue. Valuable secret information is vulnerable to attackers in storage and through transmission over a network by unauthorized access. Adaptive and simple data hiding method [7] is often regarded to be the right way in this type of scheme.

Video stream consists of a series of sequential and equally time-spaced still image frame, sometimes it also might have an audio extension attached to it. Therefore, several image steganography techniques are valid to videos as well, which has been exploited in this paper. The advantage about image frames of the video is that it has a lot of vibrations.

Revised Manuscript Received on 30 July 2019.
***** Correspondence Author
Jeswin Roy Dcouth*, Computer Science and Engineering, Vinayaka Missions Research Foundation, Salem, India.
Dr. K Somasundaram, Computer Science and Engineering, AVIT, Vinayaka Missions Research Foundation, Chennai, India.

The obvious resolution for message protection is to have a cryptic encoding technique. Cryptography is the technique of employing a secret key to translate the comprehensible protected message to associate degree incomprehensible message (known as cipher text). Solely the user with the proper key will recover the right message without the data being disturbed or modified.

An adaptive technique normally works by the principle of understanding the statistical features of the cover before any type of modification with the secret message. The essence of many image steganography techniques are usually applicable to videos also. Hu et al. [3], Shang [4], Sherly et al. [5], extended a number of image data hiding algorithms to video.

It is a common procedure to use a single video frame to be the cover image [6] but it is bound to be detected. To transmit secret message completely and securely over the internet has become an important issue. The location and selection of the frames in the video is controlled by the selection rule. This can be either sequential or adaptive in nature. The primary goal of steganography is to design embedding functions that are statistically undetectable, providing multiple security layers which are capable of communicating practically very large payloads. The Efficiency of the proposed method was measured by Peak Signal-to-Noise Ratio (PSNR) and achieved results were compared with other steganography tools. In this paper, a multiple layer message security scheme is presented that prevents any eavesdropping. The proposed scheme is robust against any means of eavesdropping or intrusion.

A. Methodology

To build a steganography algorithmic program there are numerous factors that must be thought about before it's developed into a full-fledged system. It widely depends upon the choice of cover medium, a tangible embedding and extracting algorithmic program, embedding modification and stego key.

Selecting suitable frame approach will be by focusing on perceptibility and capacity of the cover video. Select the cover video file and convert the files into consequent image frames. Count the total image frames that has been extracted from the cover video. The embedding algorithm will determine how the covert data is embedded in the container file. The extraction algorithm will retrieve the embedded data from the container. Diffie-Hellman Key Exchange is used for secure message passing. Algorithms are based on selecting suitable frame approach by focusing on perceptibility and capacity of the cover video.

1. Diffie-Helman:

A Diffie-Hellman key exchange, also called exponential key exchange, is a method of digital encryption used to generate a shared private key exchange information across an insecure channel. For example, two users A and B to exchange the information agree on two prime numbers G and N, where N is a large prime number and G is the primitive root of N. The task of breaking the code for obtaining the secret key through intrusion is mathematically overwhelming.

Video for adaptive steganography is converted into frames. Users agree on the prime number and primitive root of prime number. The Prime number 'N' chosen is the largest prime number less than the total number of frames into which the video is split and 'G' is the primitive root of 'N'. The generated secret key is the location of the frame in which data is to be embedded. Finding the value of G and N is based upon the total number of frames in the cover video file.

$$Public\ Key = G^{\text{privateKey}}\ Mod\ N \qquad (1)$$

2. QR code:

A QR code consists of black squares arranged in a square grid on a white background, which can be read by an imaging device. QR code is an alphanumeric information that is encoded into a two dimensional barcode. QR code consist of black and white square grid. The first use of QR code found its way in the automobile sector and eventually found its acceptance in various industries. Typically, QR Code can encode wide variety of information such as URL, location sharing map code, PDF, business card, YouTube channel or email that can be encrypted. The primary difference between bar code and QR code is ability to hold huge amount of data by the later. Since there is an assortment of information that can be encoded in the QR Code, which typically is a black and white squares arranged in square dot background, which cannot be identified by a human eye. This requires special type of reading scanners or smart phone application to decode the information. The basic QR Code layout includes find patterns, separators, alignment patterns, timing patterns, data area, error correction and quiet space. The required data is then extracted from patterns that are present in both horizontal and vertical components of the image. The present invention embodies a technique, referred to as Secure.

3. Data Embedding at Sender Side:

The adaptability in the algorithm will occur in the selection of the frames used for data embedding and the corresponding frame number is passed to the receiver using Diffie-Hellman secure key passing method.

The cover video file is chosen for secret message passing and split into different frames based upon the payload of the cover video file. The frame position chosen for secret data embedding in the video file is selected as the secret key generated from the Diffie-Hellman algorithm where prime number chosen is closest to total number of frames per second in the message. The data to be communicated is hidden at a frame found at the position 'm' of the secret key generated using the Diffie-Hellman algorithm. The message to be transmitted is to be converted into a QR code where the size of the QR code is resized to match the size of the frame in which data is to be embedded. This QR code is embedded into the chosen frame and the frame is put back to the frame collection at location m+1 where the original frame at location m is retained. The PSNR values of all frames are calculated and it is found that PSNR of the frame containing the hidden message do not differ from those frames without message as shown in fig [3]. This provides an advantage of adaptability and undetectability. The secret key can be obtained at the receiver side for identifying the frame containing the secret message and extract the information hidden.

Data Embedding Process:

Step 1: Convert the video to embed the data into frames.
Step 2: Select the frame at location 'm' chosen using Diffie-Hellman Algortithm.
Step 3: Message M is converted into QR code.
Step 4: Resize the QR code to match the size of the frame chosen.
Step 5: Embed the data into the selected frame at m.
Step 6: Add the frame with embedded data into the collection of frames at location m+1 retaining the original frame at location m and convert to video.
Step 7: Send the video to the receiver in a secure channel.

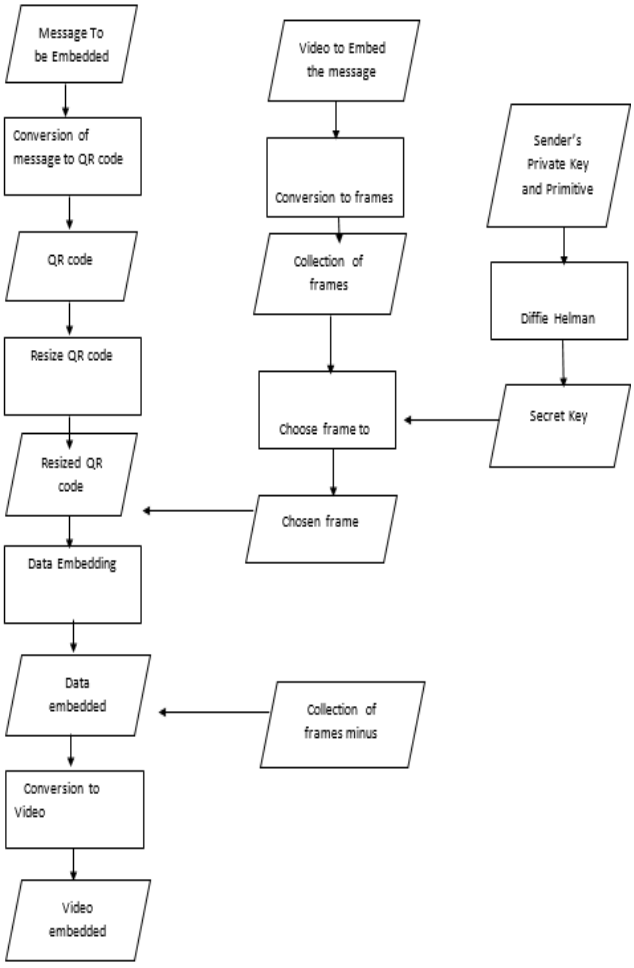

Fig 1. Data Embedding at Sender Side

4. Data Extraction at Receiver Side:

At the receiver side, the video is split into frames. The frame in which the data is embedded is identified using the secret key generated using Diffie-Hellman Algorithm. The data is extracted from the identified frame as shown in Fig [2].

Data Extraction Process:

Step 1: Convert the video into frames.

Step 2: Identify the frame at which data is embedded using Diffie-Hellman Algorithm.

Step 3: Extract the data from the frame using the identified frame and the frame previous to the data embedded frame. The frames will be extracted successfully and a stego QR code is obtained from the identified frame.

Step 4: Desteg the frame to extract QR code from the frame and decode the QR code to obtain the secret message. Along with this an added security layer of expiration limit can be set for these QR code which further enhances the security mechanism.

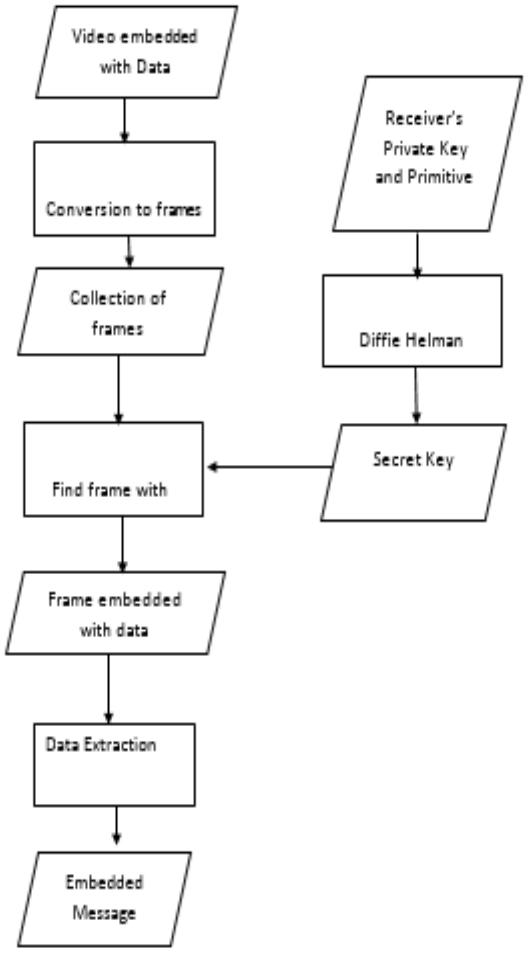

Fig 2. Data Extraction at Receiver Side

B. Experimental Analysis

The video file used to embed the secret message is split into 240 image frames as shown in table [1]. First frame is chosen as the reference image and PSNR of the remaining 239 frames are calculated. It is found that the PSNR of all 239 frames including the frame at position 185 which contains the hidden secret message does not differ much which makes the detection of the presence of secret message impossible for an intruder as shown in Fig [3].

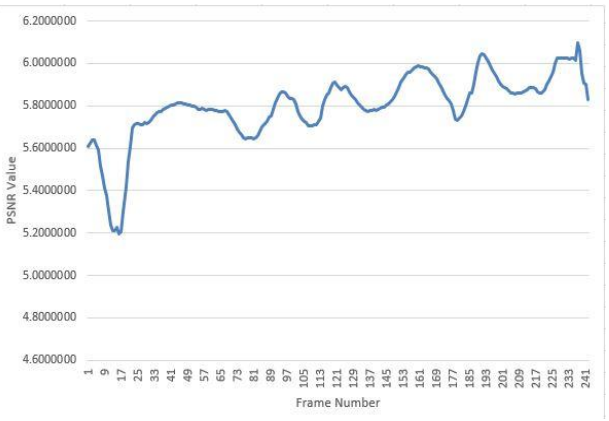

Fig 3. PSNR Values of Video Frames

II. CONCLUSION

The adaptive nature and undetectability of the proposed system makes it difficult for the attacker to identify that the communication of secret message has happened or not in the cover medium, which in true sense is the primary objective of any steganography scheme. The system presented in the work embeds information into images by slightly changing them in such a way that human eye cannot detect the transformation. Multiple layers of security has been introduced in which encoded secret message is embedded using Quick Response Code (QR) into image frames of the video. Diffie-Hellman secure key exchange is used for communicating to the receiver the frame number in which the message is hidden .

Higher embedding capacity, acceptable visual distortion, and the robustness against similarity transformation makes this method stronger against attacks.

Efficiency of the proposed method is measured by Peak Signal-to-Noise Ratio (PSNR) and the significantly small difference of PSNR evenly distributed over the image frames makes it imperceptible for covert communications.

TABLE I: PSNR VALUES OF VIDEO FRAMES

Frame 1 5.608002e+00	**Frame 2** 5.624124e+00	**Frame 3** 5.639633e+00	**Frame 4** 5.636825e+00	**Frame 5** 5.615670e+00	**Frame 6** 5.591409e+00	**Frame 7** 5.514193e+00	**Frame 8** 5.468643e+00
Frame 9 5.414571e+00	**Frame 10** 5.374455e+00	**Frame 11** 5.306485e+00	**Frame 12** 5.237534e+00	**Frame 13** 5.211298e+00	**Frame 14** 5.210438e+00	**Frame 15** 5.227723e+00	**Frame 16** 5.196978e+00
Frame 17 5.208420e+00	**Frame 18** 5.298770e+00	**Frame 19** 5.417001e+00	**Frame 20** 5.535818e+00	**Frame 21** 5.609766e+00	**Frame 22** 5.711303e+00	**Frame 23** 5.615670e+00	**Frame 24** 5.715047e+00
Frame 25 5.718307e+00	**Frame 26** 5.708887e+00	**Frame 27** 5.713311e+00	**Frame 28** 5.724165e+00	**Frame 29** 5.714208e+00	**Frame 30** 5.720273e+00	**Frame 31** 5.732731e+00	**Frame 32** 5.746737e+00
Frame 33 5.755591e+00	**Frame 34** 5.767216e+00	**Frame 35** 5.773068e+00	**Frame 36** 5.774448e+00	**Frame 37** 5.784640e+00	**Frame 38** 5.790330e+00	**Frame 39** 5.794009e+00	**Frame 40** 5.798206e+00
Frame 41 5.803725e+00	**Frame 42** 5.805657e+00	**Frame 43** 5.810448e+00	**Frame 44** 5.813259e+00	**Frame 45** 5.813071e+00	**Frame 46** 5.814428e+00	**Frame 47** 5.810336e+00	**Frame 48** 5.807671e+00
Frame 49 5.804999e+00	**Frame 50** 5.803380e+00	**Frame 51** 5.799622e+00	**Frame 52** 5.797617e+00	**Frame 53** 5.794851e+00	**Frame 54** 5.784581e+00	**Frame 55** 5.784472e+00	**Frame 56** 5.786232e+00
Frame 57 5.782310e+00	**Frame 58** 5.780753e+00	**Frame 59** 5.782323e+00	**Frame 60** 5.781213e+00	**Frame 61** 5.783283e+00	**Frame 62** 5.778286e+00	**Frame 63** 5.779227e+00	**Frame 64** 5.770757e+00
Frame 65 5.770739e+00	**Frame 66** 5.774263e+00	**Frame 67** 5.777118e+00	**Frame 68** 5.772635e+00	**Frame 69** 5.758179e+00	**Frame 70** 5.744676e+00	**Frame 71** 5.727216e+00	**Frame 72** 5.710442e+00
Frame 73 5.693259e+00	**Frame 74** 5.677838e+00	**Frame 75** 5.664175e+00	**Frame 76** 5.649571e+00	**Frame 77** 5.646494e+00	**Frame 78** 5.649340e+000	**Frame 79** 5.649884e+00	**Frame 80** 5.648102e+00
Frame 81 5.644313e+00	**Frame 82** 5.648302e+00	**Frame 83** 5.659756e+00	**Frame 84** 5.680136e+00	**Frame 85** 5.700924e+00	**Frame 86** 5.717575e+00	**Frame 87** 5.729242e+00	**Frame 88** 5.745565e+00
Frame 89 5.752936e+00	**Frame 90** 5.781808e+00	**Frame 91** 5.815563e+00	**Frame 92** 5.836776e+00	**Frame 93** 5.856621e+00	**Frame 94** 5.863584e+00	**Frame 95** 5.866048e+00	**Frame 96** 5.859851e+00
Frame 97 5.844300e+00	**Frame 98** 5.834504e+00	**Frame 99** 5.834449e+00	**Frame 100** 5.830384e+00	**Frame 101** 5.807957e+00	**Frame 102** 5.772278e+00	**Frame 103** 5.751162e+00	**Frame 104** 5.738549e+00
Frame 105 5.726584e+00	**Frame 106** 5.722035e+00	**Frame 107** 5.707086e+00	**Frame 108** 5.705902e+00	**Frame 109** 5.708740e+00	**Frame 110** 5.710381e+00	**Frame 111** 5.709856e+00	**Frame 112** 5.725296e+00
Frame 113 5.741472e+00	**Frame 114** 5.800449e+00	**Frame 115** 5.830463e+00	**Frame 116** 5.848784e+00	**Frame 117** 5.861603e+00	**Frame 118** 5.885642e+00	**Frame 119** 5.905266e+00	**Frame 120** 5.910086e+00
Frame 121 5.898939e+00	**Frame 122** 5.886633e+00	**Frame 123** 5.876627e+00	**Frame 124** 5.886406e+00	**Frame 125** 5.892611e+00	**Frame 126** 5.885926e+00	**Frame 127** 5.867287e+00	**Frame 128** 5.850481e+00
Frame 129 5.838341e+00	**Frame 130** 5.828650e+00	**Frame 131** 5.812790e+00	**Frame 132** 5.802151e+00	**Frame 133** 5.792034e+00	**Frame 134** 5.784655e+00	**Frame 135** 5.776546e+00	**Frame 136** 5.774574e+00
Frame 137 5.776769e+00	**Frame 138** 5.776825e+00	**Frame 139** 5.781063e+00	**Frame 140** 5.778298e+00	**Frame 141** 5.784851e+00	**Frame 142** 5.786264e+00	**Frame 143** 5.791519e+00	**Frame 144** 5.794070e+00
Frame 145 5.804335e+00	**Frame 146** 5.807005e+00	**Frame 147** 5.817836e+00	**Frame 148** 5.830022e+00	**Frame 149** 5.842948e+00	**Frame 150** 5.863991e+00	**Frame 151** 5.887511e+00	**Frame 152** 5.911281e+00
Frame 153 5.932400e+00	**Frame 154** 5.947149e+00	**Frame 155** 5.956370e+00	**Frame 156** 5.960839e+00	**Frame 157** 5.966744e+00	**Frame 158** 5.978961e+00	**Frame 159** 5.986421e+00	**Frame 160** 5.988691e+00
Frame 161 5.986830e+00	**Frame 162** 5.984409e+00	**Frame 163** 5.980157e+00	**Frame 164** 5.978935e+00	**Frame 165** 5.972630e+00	**Frame 166** 5.958737e+00	**Frame 167** 5.950490e+00	**Frame 168** 5.938741e+00
Frame 169 5.925787e+00	**Frame 170** 5.909121e+00	**Frame 171** 5.891705e+00	**Frame 172** 5.871765e+00	**Frame 173** 5.852662e+00	**Frame 174** 5.836988e+00	**Frame 175** 5.822792e+00	**Frame 176** 5.807199e+00
Frame 177 5.778108e+00	**Frame 178** 5.738861e+00	**Frame 179** 5.733172e+00	**Frame 180** 5.741787e+00	**Frame 181** 5.751985e+00	**Frame 182** 5.771146e+00	**Frame 183** 5.800575e+00	**Frame 184** 5.828463e+00
Frame 185 5.862029e+00	**Frame 186** 5.860955e+00	**Frame 187** 5.903815e+00	**Frame 188** 5.958789e+00	**Frame 189** 6.004449e+00	**Frame 190** 6.036868e+00	**Frame 191** 6.046055e+00	**Frame 192** 6.040195e+00
Frame 193 6.024438e+00	**Frame 194** 6.008906e+00	**Frame 195** 5.987787e+00	**Frame 196** 5.968786e+00	**Frame 197** 5.955616e+00	**Frame 198** 5.935671e+00	**Frame 199** 5.918134e+00	**Frame 200** 5.902089e+00
Frame 201 5.892285e+00	**Frame 202** 5.888075e+00	**Frame 203** 5.881523e+00	**Frame 204** 5.871839e+00	**Frame 205** 5.862422e+00	**Frame 206** 5.859106e+00	**Frame 207** 5.854579e+00	**Frame 208** 5.859388e+00
Frame 209 5.858999e+00	**Frame 210** 5.861493e+00	**Frame 211** 5.866730e+00	**Frame 212** 5.871747e+00	**Frame 213** 5.878120e+00	**Frame 214** 5.885462e+00	**Frame 215** 5.885781e+00	**Frame 216** 5.884269e+00
Frame 217 5.879040e+00	**Frame 218** 5.866223e+00	**Frame 219** 5.861383e+00	**Frame 220** 5.858624e+00	**Frame 221** 5.874846e+00	**Frame 222** 5.901542e+00	**Frame 223** 5.919416e+00	**Frame 224** 5.937340e+00
Frame 225 5.960115e+00	**Frame 226** 6.002480e+00	**Frame 227** 6.025789e+00	**Frame 228** 6.026097e+00	**Frame 229** 6.026732e+00	**Frame 230** 6.026612e+00	**Frame 231** 6.024926e+00	**Frame 232** 6.027211e+00
Frame 233 6.022238e+00	**Frame 234** 6.023174e+00	**Frame 235** 6.025698e+00	**Frame 236** 6.015993e+00	**Frame 237** 6.095534e+00	**Frame 238** 6.063140e+00	**Frame 239** 5.953661e+00	**Frame 240** 5.904634e+00

REFERENCES

1. Das R, Tuithung T (2012) A novel steganography method for image based on Huffman Encoding. In: 3rd National Conference on Emerging Trends and Applications in Computer Science (NCETACS) 1418
2. Mercuri RT (2004) The many colors of multimedia security. Commun of the ACM 47(12):2529
3. Hu S, KinTak U (2011) A Novel Video Steganography Based on Non-uniform Rectangular Partition. In: IEEE 14th International Conference on Computational Science and Engineering (CSE) 5761
4. Shang Y (2007) A new invertible data hiding in compressed videos or images. In: Third International Conference on Natural Computation (ICNC) 576580
5. Sherly AP, Amritha PP (2010) A Compressed Video Steganog- raphy using TPVD. Int J of Database Manag Syst 2 (3). doi:5121/ijdms.2010.2307 67
6. Yugeshwari Kakde, Priyanka Gonnade, Prashant Dahiwale, Audio-Video steganography, in IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems [Online]. pp. 1-6. 2015.

7. Liao Y-C, Chen C-H, Shih TK, Tang NC (2009) Data hiding in video using adaptive LSB. In: Joint Conferences on Pervasive Computing (JCPC) 185190
8. Hamid N, Yahya A, Ahmad RB, Al-Qershi OM(2012) Image steganography techniques: an overview. Int JComput Sci Secur (IJCSS) 6(3):p168p187
9. Herodotus, The History December 17 2014, [Online]. Available: https://ebooks.adelaide.edu.au/h/herodotus/h4/complete.html
10. W. Luo, F. Huang, J. Huang, Edge adaptive image steganography based on LSB matching revisited, IEEE Trans Inform Forensics Secure, 5 (2) (2010), pp. 201214.
11. Sadek, M.M., Khalifa, A.S. & Mostafa, M.G.M. Multimed Tools Appl (2015) 74: 7063. https://doi.org/10.1007/s11042-014-1952-z
12. Shang Y (2007) A new invertible data hiding in compressed videos or images. In: Third International Conference on Natural Computation (ICNC) 576–580
13. R. M. Bani-Hani, Y. A. Wahsheh and M. B. Al-Sarhan, "Secure QR code system," 2014 10th International Conference on Innovations in Information Technology (IIT), Al Ain, 2014, pp. 1-6. doi: 10.1109/INNOVATIONS.2014.6985772
14. Nan Li, "Research on Diffie-Hellman key exchange protocol," 2010 2nd International Conference on Computer Engineering and Technology, Chengdu, 2010, pp. V4-634-V4-637. doi: 10.1109/ICCET.2010.5485276
15. S. Goyal, S. Yadav and M. Mathuria, "Exploring concept of QR code and its benefits in digital education system," 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Jaipur, 2016, pp. 1141-1147. doi: 10.1109/ICACCI.2016.7732198