Confidential Data Encryption And Data Retrieval Using QR Authentication System

Mrs.J.Roselin Lourd[1], Dhanushkodi.P[2], Sabanabanu.S[3], Sowmya.J[4]
[1]Head, Dept of CSE
[2, 3, 4]Dept of Computer Science
[1, 2, 3, 4] RAAK college of Engineering and technology Puducherry
[2, 3, 4]Pondicherry university Puducherry

Abstract- *The QR code cryptography with a password and sends it to the required hiding the information message QR code. Search and hiding personal information. At present, confidentiality is maintained in secure base RSA,DES and ASE method. Personal information can be securely shared with the expected person and the person can verify the information by checking its authenticity. QR codes are being used increasingly to share data for different purposes. In information communication, The QR code is most important because of its high data capacity. However, The most existing QR code systems that can use to insecure data format and encryption is rarely used for it.*

Keywords- cryptography- QR code RSA, DES and AES algorithm

I. INTRODUCTION

With the rapid development of mobile communication technology and Internet of things technology (IOT), electronic tag technology has gradually been widely used in all walks of life. Compared with one-dimensional barcodes, Quick Response (QR) code has the advantages of large information capacity, high decoding reliability, strong error correction ability, wide range of storage information, high density, high information transmission efficiency, etc. It has been widely used in many fields, such as ID identification, advertising warehousing and logistics , product traceability, e-commerce, mobile payment, etc. As the core perception technology of Internet of things and the important information entrance of the Internet, QR code has gradually penetrated into various fields of national economy and social life.

However, because of the openness of QR code encoding and decoding technology, the sensitive information transmitted by QR code is easy to be stolen, especially in the fields of O2O e-commerce, mobile payment and ID identification. This will cause security issues. To protect the sensitive information in QR code, many researchers are investigating pattern recognition technology to improve the security of sensitive information security.

II. QR CODE USING HIDING INFORMATION SECURED

In this era of digital world, with the evolution of technology and un-ending growth in digital data, there is an essential need of optimization of online data and information present in the digital world. The most important issue in data is that it should be original and correct. The authenticity of data is the most challenging issue in management of data in the internet database. In the present study we mainly focus on the authenticity of marks in a printed mark sheet.In our new mark-sheet system, we will be embedding the data digitally in form of QR Code which is itself encrypted, so that the marks obtained by the student can not be tampered, and the data embedded in the mark-sheet can be only decrypted and read from our decryption program.

METHODS USED IN HIDING INFORMARION

TTJSA encryption algorithm, which was designed by Nath et al. and is an amalgamation of three different cryptographic modules: generalized modified Vernam cipher , MSA and NJJSA for the encryption purpose of data in the QR Code. TTJSA for Encryption Purpose of the Embedded Data TTJS is a combined symmetric key cryptographic method, which is formed of generalized modified Vernam cipher, MSA and NJJSA symmetric key cryptographic methods. Brief study of the methods used in TTJSA algorithm is as follows:

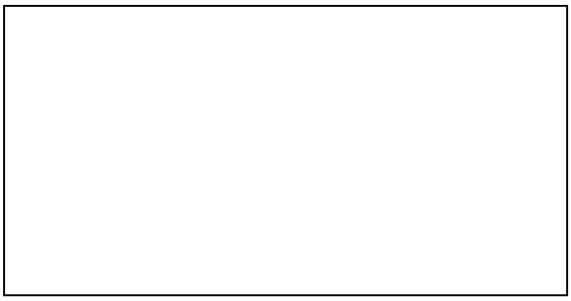
Modified Vernam Cipher In this step, we break the whole file into different small blocks (like in Block Cipher system []), where each block size should be less than or equal to 256 byes.

NJJSAA Algorithm The encryption number (=secure) and randomization number (=times) is calculated according to the method mentioned in MSA algorithm.

MSA Encryption and Decryption Algorithm Nath et al. [2] proposed a symmetric key method where they have

used a random key generator for generating the initial key and that key is used for encrypting the given source file.

V. PROBLEM IDENTIFIED

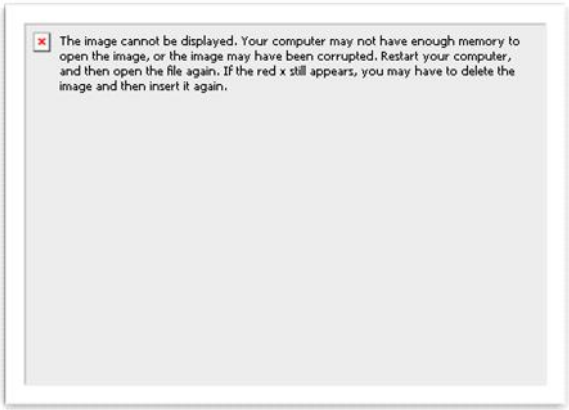


The data is embedded directly.In this system

One key to encrypt is available. In this type of encryption different keys are used for encrypting and decrypting. There is a public key that can be exchanged with anybody and a private key that is not shared.

VI. PROPOSED SYSTEM

The system that has been proposed with basic methods is used for video steganography is AES method, DES & RSA Network. The data or information contains the flow of secret communication with the quality of data. The steganography involves the sender side and receiver side way of communication. And there are many steganography tools and file formats that existed. QR code is the Quick Response code.Before the QR code there are some authentication methods are available that are User name and password, Bar code, Finger prints ,Face identity. But user name and password are not providing more security. And the Bar codes have some limitations like bar code only stored up to 20 digits. Bar codes are only readable in one direction. Also when it gets damage it is not readable.



METHODOLOGY

This paper was done using algorithms (“AES, DES network, and RSA logic”). The algorithms are applied for better results, quality of videos, and secured communication. The methodology process through steps:

Step 1: Trace the video stream files.
Step 2: Upload sample text or image to embed in video files. Embedding Method:
Step 3: Grab any video file and upload a secret message in the video stream file.
Step 4: It displays the results of stegno video file. Extraction Procedure:
Step 5: The process of applying using LSB, neural network and fuzzy logic.
Step 6: This step shows, hidden data in a video stream file.
Step 7: It shows the results of PSNR & MSE.
Step 8: MSE and PSNR values are defined.

VI. FUTURE SCOPE

Cryptograpy techniques have been achieved the three techniques are AES, RES and DES to hiding information. And the existing techniques act in payload, capacity, the other lacks robustness. All the major file formats have several methods and week points respectively this paper steganography done with good results and to use advanced steganography & good precision rates, &successfully tested PSNR and MSE data values. Future work of steganography applications wants to use the new algorithms, in the use of more quantization vector and to ensure the security of others.

VII. CONCLUSION

In modern days, the usage of data is increasing and the ways of forging data is increasing as well. Authenticity and validity of data is a very important issue nowadays. Information ,especially confidential information. It replaces sensitive information on paper documents with QR Codes and let only the registered user decode it with our system. of, QR Code Verification and QR Code Validation. QR Code generation part, QR Code decoding part, QR Code verification part, QR Code validation part and also RSA Key generation part, learnt about different attributes of 2D codes, especially QR Code and also learnt about cryptography, especially asymmetric cryptography like RSA public key cryptography and RSA digital signature. By using the web application, secure encrypted QR Code can be generated and then, this QR code can be decoded by means of confidential information verification.

REFERENCES

[1] Kumar, A &pooja, K. (2010). "STEGANOGRAPHY-A DATA HIDING TECHNIQUE." International Journal of Computer Applications, 9(7), 19-23.

[2] Bhargava, S., &Mukhija, M. (2019). HIDE IMAGE AND TEXT USING LSB, DWT AND RSA BASED ON IMAGE STEGANOGRAPHY. ICTACT Journal on Image &Video Processing, 9(3).

[3] Gutub, A., Al-Qahtani, A., &Tabakh, A. (2009, May). TRIPLE-A: SECURE RGB IMAGE STEGANOGRAPHY BASED ON RANDOMIZATION. In 2009 IEEE/ACS International Conference on Computer Systems and Applications(pp. 400-403).IEEE.

[4] Srilakshmi, P., Himabindu, C., Chaitanya, N., Muralidhar, S. V., Sumanth, M. V., &Vinay, K. (2018). TEXT EMBEDDING USING IMAGE STEGANOGRAPHY IN SPATIAL DOMAIN. International Journal of Engineering & Technology, 7(3.6), 14.

[5] Krishnaveni, N. (2018). IMAGE STEGANOGRAPHYUSING LSB EMBEDDING WITH CHAOS. International Journal of Pure and Applied Mathematics, 118(8), 505-509.

[6] Morkel, T., Eloff, J. H., & Olivier, M. S. (2005, June). AN OVERVIEWOF IMAGE STEGANOGRAPHY. In ISSA (pp. 1-11).

[7] Kaur, S., Bansal, S., &Bansal, R. K. (2014, March). STEGANOGRAPHY AND CLASSIFICATION OF IMAGE STEGANOGRAPHY TECHNIQUES. In 2014 International Conference on Computing for Sustainable Global Development (INDIACom)(pp. 870-875). IEEE.