iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** VII **Month of publication:** July 2021

DOI: https://doi.org/10.22214/ijraset.2021.37023

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VII July 2021- Available at www.ijraset.com

Survey Paper on Secret Sharing Schema for Digital Quick Response Code Applications

Miss. Mugale Swati M[1], Prof. Late R. B[2]
[1, 2]*DBAT University, Department of CSE, M. S. Bidve Engineering College, Latur, Maharashtra, India*

Abstract: ***Due to data loss rate during communication may be high and vary from time to time. Now a days, there is the possibility to hack and change your data while you are sending from one place to another. To solve this Problem , Many Approaches are proposed to provide security to Original Message. In this paper, We Provide a survey of different Approaches used for Secure Data transmission Like VSS Scheme, Visual Cryptography, Watermarking, Stenography, etc.***
Keywords: Data Security, high security, visual secret sharing scheme, QUICK RESPONSE Code, Watermarking.

I. INTRODUCTION

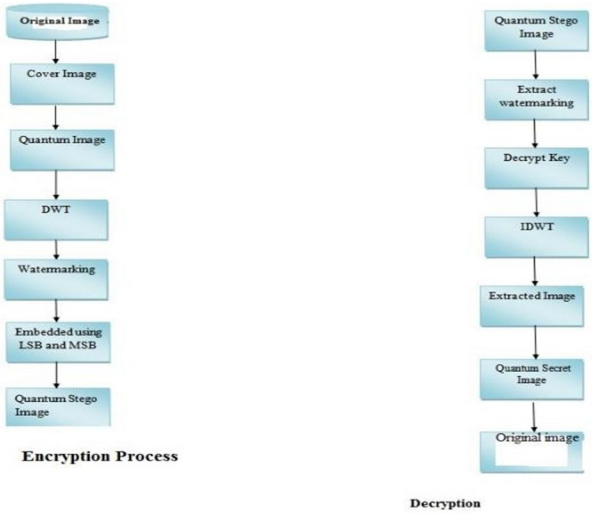
A. Overview

Increased use of internet media with a one- time login that is sent to the smart phone customer so that someone can hack information during transactions. To solve this problem use the QUICK RESPONSE code to overcome this inconvenience, because all correspondence is encrypted. This is not feasible. For private message share and document protection permission, two levels of QUICK RESPONSE code are used. QUICK RESPONSE codes has feature a high degree of encoding capability, supplemented with error correcting facilities, small size and robust to geometric distortions as they are copying data and easy to read with any computer and each person. It has certain benefits and a little inconvenience. Information encoded in a QUICK RESPONSE code is always accessible to everyone, even if it is ciphered and therefore is only easily readable to authorized users just like see and understand.
QUICK RESPONSE code is unable to distinguish original document content over duplicate copy of encoded document. To overcome this drawback used to standard QUICK RESPONSE code encoding capacity therefore, even when the private information is degraded or lost in the copy, the public information is always accessible for reading.

II. RELATED WORK

Y. Cheng and others[1] propose a visual secret sharing scheme to encode a secret QUICK RESPONSE code into Multiple shares. It transfers data into Non-Readable format of secret Quick Response code and again Quick Response code transfer into readable format by using standard Quick Response code reader and scan Using smartphones or other Quick response Scanning devices.
A.A. Abd and others[2] develop Two Approaches for data Hiding.

1) Quantum Image Steganography Firstly, Original Image is encrypted and combined into a quantum Cover image.
2) Quantum Image Watermarking To combine watermark image into quantum Carrier image without affecting the Original image.



Encryption and Decryption process[2]

Y. Li and Others[3] develop Sparse coding Approach is mainly used to find out Small set of atoms from the input signal that is Fingerprint. It helps to identify if a user is authorized or not from database. Due to this Error rate of this technique is lower.

D.HOu and others[4] develop Reversible data hiding (RDH) Approach where data is hidden in cover media that is image. It combines data in cover image by changing pixel values of image for secure communication and cover image can be recovered to its Original Image from after extraction of secret data its Original Image from its after extraction of secret data from it.

In this paper[5] develop Watermarking algorithm of color image based on Discrete-Wavelet Transform, Discrete Cosine Transform and Singular Value Decomposition(DWT-DCT-SVD).Firstly, Convert Original color image from Red Green Blue(RGB) color into YUV color space after that it divides into blocks and apply SVD with every blocks and then finally Combines Watermark to Cover image, we got Original Image. It helps to detect invisible data and solve common Watermark attacks.

Shaekh Hasan Shoron and Others[6] develop approach giving Security from Unauthorized user. Firstly, Original image is processed using Successive- Mean-Quantization transform(SMQT) which uses OTSU for image parts, after that Watermark is
Combined in image using Discrete- Wavelet- Transform(DWT).
Finally, Watermark is extracted from Original image by executing inverse operation of combining process.

In this paper [7] develop Wavelet Domain to generate Unique identity code from Structure images which is combined with patient ID to generate watermark.
This technique is used for Unique identification, authentication and integrity Verification of images.

EttiMathur and Others[8] to secure data by hiding some information in such a way that information can not be detected without having Knowledge about the Watermarking scheme.
Least Significant Bit(LSB) pixel values of image are converted into binary bits using Discrete Cosine Transform(DCT) can measure an original image into cosine waveform and inverse Discrete cosine transform to got Original image.

In this paper[9] develop an approach that allows pictures,text,etc to be encrypted in such a way that decryption can be performed by a human visual System. A(k,n)visual Cryptography Scheme(VCS) encrypts a secret image into n images distributed among n participants.XOR based visual Cryptography Scheme(VCS),which uses XOR operation for decoding was created Secure Communication.

P. Y. Lin and others[11]proves that Quick Response code has large data capacity and high speed scanning .It uses Quick Response Features to get secret sharing ,printing and scanning operation.
The data can be divided into parts and apply Quick Response tags on those parts and allow access to that data only to authorized users.
Browsers can read that Original data which has Quick response tag, it helps to reduce Security risk.

In this paper[12] Quick Response code that has two storage levels and can be used for document authentication. This new rich QR code, named two- level QR code, has public and private storage levels. The public level is the same as the standard QR code storage level therefore, it is readable by any classical QR code application. The private level is constructed by replacing the black modules by specific textured patterns. It consists of information encoded using q-array code with an error correction capacity. The results show a perfect restoration of private information.

To protect the sensitive data, this paper[13] explores the characteristics of QR barcodes to design a secret hiding mechanism for the QR barcode with a higher payload. For a normal scanner, a browser can only reveal the formal information from the marked QR code. The authorized user/scanner can reveal the sensitive data from the marked QR tag. The results demonstrate a satisfactory secret payload and the feasibility of this scheme.

In this paper[14] develop an approach to what extent such an external attacker can identify the specific actions that a user is performing on mobile apps.
Mobile devices can be maliciously exploited to violate the privacy of people. The apps installed on a smartphone can reveal much information about a user, such as their medical conditions or religious beliefs. Additionally, the presence or absence of particular apps on a smartphone can inform an adversary who is intent on attacking the device.

In this paper[15] show that a passive eavesdropper can feasibly identify smartphone apps by fingerprinting the network traffic that they send. Although packet size and direction is still leaked from encrypted connections. This system used machine learning techniques to identify smartphone apps from this side-channel data.
This strategies is used to enable app classification system to identify and mitigate the effect of ambiguous traffic, i.e., traffic in common among apps such as advertisement traffic.

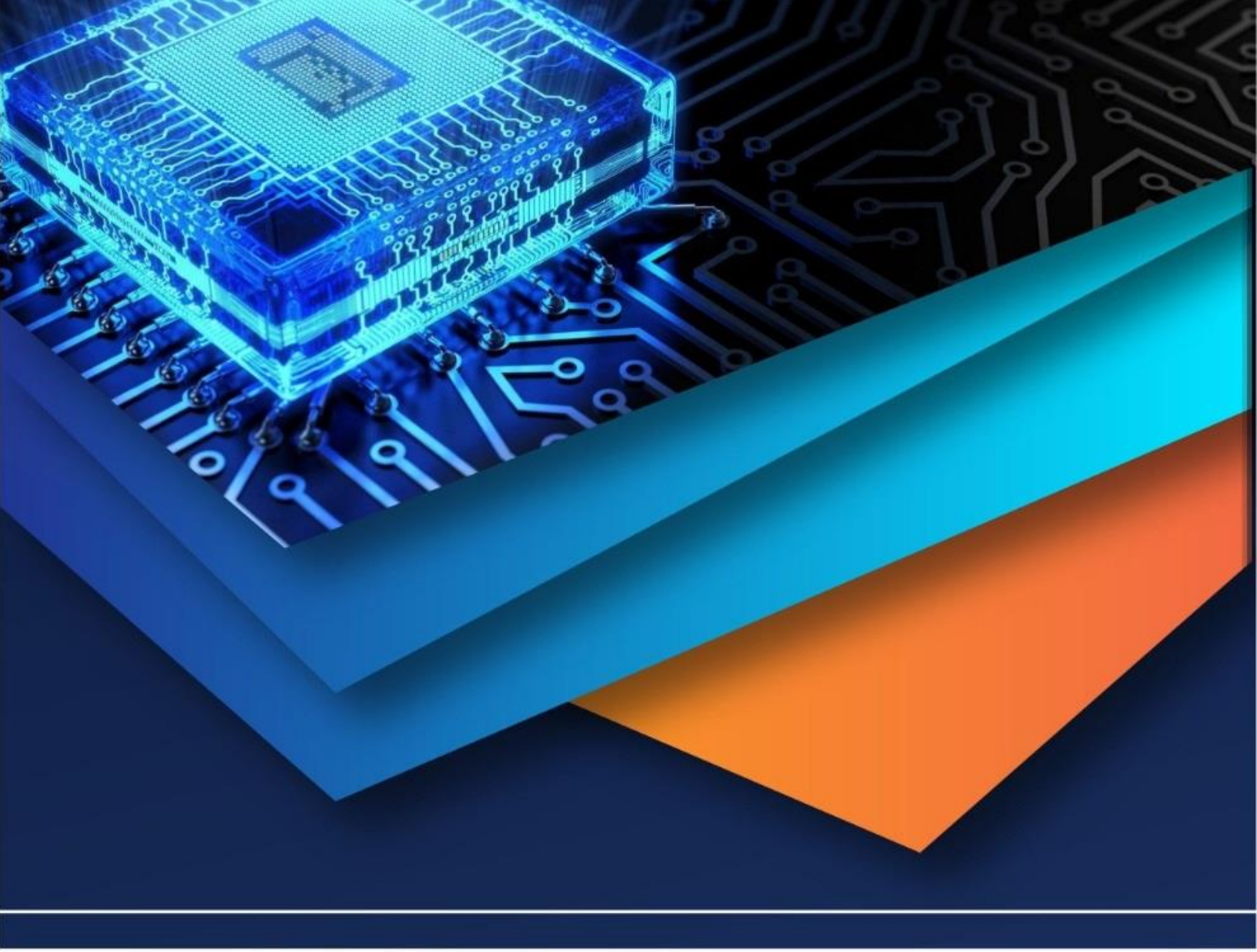
III. CONCLUSION

In this paper we review approaches on existing techniques for secure data transmission. so for that purpose, different approaches used like VSS scheme, Reversible Data Hiding scheme and watermarking scheme that helps to encode a secret Quick Response code into Multiple shares, to maintain Security during communication. Above Described approaches can effectively reduce the transmission and maintain security of data during transmission.

It is observed that the secure data transmission based approaches cannot give confirmation about delivery of data and it cannot provide accuracy of message at receiver side. More successful approaches need to be invented to address the current difficulties of secure data transmission and accuracy of data.

REFERENCES

[1] Y. Cheng, Z. Fu, and B. Yu, ―Improved visual secret sharing scheme for QUICK RESPONSE code applications,‖ IEEE Trans. Inf. Forensics Security, vol. 13, no. 9, pp. 2393–2403, Sep. 2018.
[2] A. A. Abd El-Latif, B. Abd-El-Atty, M. S. Hossain, M. A. Rahman, A. Alamri, and B.Gupta, ―Efficient quantum information hiding for remote medical image sharing,‖ IEEE Access, vol. 6, pp. 21075–21083, 2018.
[3] Y. Li and L. Guo, ―Robust image fingerprinting via distortion-resistant sparse coding,‖ IEEE Signal Process. Lett., vol. 25, no. 1, pp. 140–144, Jan. 2018.
[4] D. Hou, W. Zhang, J. Liu, S. Zhou, D. Chen, and N. Yu, ―Emerging applications of reversible data hiding,‖ in Proc. 2nd Int. Conf. Image Graph. Process. (ICIGP), Singapore, Feb. 2019, pp. 105– 109.
[5] Yuqi He, Yan Hu,"A Proposed Digital Image Watermarking Based on DWT-DCT- SVD"2018 2nd IEEE Advanced Information Management,Communicates,Electronic and Automation Control Conference(IMCEC 2018).
[6] ShaekhHasan Shoron, MonamyIslam, BiprojitMondal,JiaU ddin,"A Digital Watermarking Approach using SMQT,OTSU, DWT and IDWT"IEEE Conference 2018.
[7] Abhilasha Singh, 2 Malay Kishore Dutta,‖ Lossless and Robust Digital Watermarking Schemefor Retinal Images‖ International Conference on "Computational Intelligence and Communication Technology" (CICT 2018). RESPONSE Code,‖ IEEE Transactions on Industrial Informatics, vol. 12, no. 1, pp. 384-392, 2016.
[8] EttiMathur, Manish Mathuria,‖ Unbreakable Video Processing, vol. 2017, no. 1, pp. 14, 2017. Digital Watermarking using combination of LSB and DCT‖ International Conference on Electronics, Communication and Aerospace Technology ICECA 2017
[9] C. N. Yang, D. S. Wang, ―Property Analysis of XOR-Based Visual Cryptography,‖ IEEE Transactions on Circuits & Systems for Video Technology, vol. 24, no. 12 pp. 189- 197, 2014.
[10] P. P. Thulasidharan, M. S. Nair, ―QUICK RESPONSE code based blind digital image watermarking with attack detection code,‖ AEU - International Journal of Electronics and Communications, vol. 69, no. 7, pp. 1074-1084, 2015.
[11] P. Y. Lin, ―Distributed Secret Sharing Approach with Cheater Prevention Based on QUICK
[12] Tkachenko, W. Puech, C. Destruel, et al., ―Two- Level QUICK RESPONSE Code for Private Message Sharing and Document Authentication,‖ IEEE Transactions on Information Forensics & Security, vol. 11, no. 13, pp. 571-583, 2016.
[13] P. Y. Lin, Y. H. Chen, ―High payload secret hiding technology for QUICK RESPONSE codes,‖ Eurasip Journal on Image &
[14] M. Conti, L. V. Mancini, R. Spolaor, and N. V. Verde, ―Analyzing android encrypted network traffic to identify user actions,‖ IEEE Transactions on Information Forensics and Security, vol. 11, no. 1, pp. 114–125, Jan 2016
[15] V. F. Taylor, R. Spolaor, M. Conti, and I. Martinovic, ―Robust smartphone app identification via encrypted network traffic analysis,‖ IEEE Transactions on Information Forensics and Security, vol. 13, no. 1, pp.63–78, Jan 2018.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY