IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 6, June 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 6, June 2021||

DOI:10.15680/IJIRSET.2021.1006040

Survey Paper on Reversible Secret Image sharing schema for QR Code Applications

Kulkarni Komal [1] , Nakwal Anshu [2] , Hinge Priyanka [3] , Mhaske Nutan [4] , Prof. H.B. Jadhav [5]

Dept. of Computer Engineering, S.C.S.M.C.O.E, Savitribai Phule Pune University, Nepti, Maharashtra, India[1,2,3,4]

Professor, Dept. of Computer Engineering, S.C.S.M.C.O.E, Savitribai Phule Pune University, Nepti, Maharashtra, India [5]

ABSTRACT*:* for storage information and high-speed reading, the Fast Response (QR) code was developed. Two level storage systems are used to validate original material in a QR code for the proposed QR code authentication. Our proposal uses the preservation of documents at both public and private levels. The same standard level of QR storage is explored at the public level, and is readable to any computer that reads QR cod. The private level is built by replacing the black modules with some textured patches. It consists of information coded with an error correcting capability with the q-ary language.Q-array data increases QR code storage capability but still checks the original copy text. The resilience of the patches to the printing and scan process is responsible for this authentication. It is not possible that our steganographic solution would beat Steganalytic Algorithm. Thirdly, the reversible capacity of our system enables the recuperation of the root texture. For secrecy in picture we weave texture synthesis into steganography.

KEYWORDS: Data Security, high security, visual secret sharing scheme, QR Code, Watermarking.

I. INTRODUCTION

Increased use of internet media with a one-time login that is sent to the smartphone customer so that someone can hack information during transactions. To solve this, we use the QR 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 QR code are motivated. QR codes 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, however.
Information encoded in a QR code is always accessible to everyone, even if it is ciphered and therefore is only easily readable to authorised users just like see and understand.

QR code is unable to distinguish original document content over duplicate copy of encoded document. We encourage the standard QR code encoding ability to overcome the disadvantage.This is achieved by substituting its black modules in particular with textured patterns. These models can be designed to be susceptible to distortions due to the P&S process besides increasing storage capacity. These patterns, which do not disrupt the standard process of reading, are always seen by any QR code reader as black modules. So public information will always be available for reading even if the private information is degraded or lost in the copy.

We understand that the user's privacy information is closely linked to authentication security. The reason for this project is to considerably improve storage capacity by increasing the alphabet code q or the textured pattern size. The test results show that private data are perfectly restored. It also underlines the option.

II. RELATED WORK

A Proposed Digital Image Watermarking Based on DWT-DCT-SVD: This document offers a watermarking colour image algorithm based on the transformation of discreet waves, the transformation of discreet cosines and the decomposition of single values (DWT-DCT-SVD). Convert the first RGB colour image to YUV colour space. The low frequency is then split into blocks using the discreet cosine transform and SVD is performed with every block by a layer of discredited wavelength transformation onto the luminance component Y. Upon the cover image, finally insert watermarks.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 6, June 2021||

DOI:10.15680/IJIRSET.2021.1006040

A Digital Watermarking Approach using SMQT,OTSU, DWT and IDWT: A new digital watermarking model for medical images is proposed in this paper. For image improvement, an improved SMQT is used and the image is segmented by the OTSU threshold. The DWT and Inverse DWT are used to embed and extract watermark in the host image. The DWT is used to remove the host image. Our scheme aims to strengthen watermarking against attacks and ensure that the image is protected from privacy threats.

Lossless and Robust Digital Watermarking Scheme for Retinal Images: This paper presents a robust zero watermarking technique for medical images, based on a single value decomposition, for dealing with privacy and safety issues. The method proposed, as opposed to conventional watermarking, retains the reliability of the image cover without the introduction of artefacts or any modification to the essential information in the medical image. Telephthalmologic pictures evaluate the performance of the system. The results of the simulation show the robustness of the technique proposed in response to various image processing attacks and show its suitability for safe exchange of medical images between remote practitioners.

Unbreakable Digital Watermarking using combination of LSB and DCT: This investigation is done to find the best digital watermarking technology for safe and illegal copies of digital images. Research has also been carried out to analyse the options for dual watermarking. Different standard research papers have been studied and double watermarking with some situations has been found possible. This research motivates and provides various compounds on digital watermarking techniques for efficient watermarking output in the near future.

Property Analysis of XOR-Based Visual Cryptography: This article shows that the contrast between XVCS and OVCS is 2(k-1) times higher. The monotone property of OR reduces the visual image quality for OR-based VCS (OVCS). The contrast was therefore proposed to improve XOR-based VCS (XVCS) which uses XOR for decoding. Benefits include: Stacking the secret picture easily decodes. XVCS has a better image than OVCS reconstruction. Benefits are: More complicated is the proposed algorithm.

QR code based blind digital image watermarking with attack detection code: Present a paper that incorporates a transformed binary form of a watermark data into the cover image DWT domain and uses a unique image code for detection of image distortion. A blind key-based watermarking method. The QR code is integrated into the 1st-level DWT cover image domain attack resistant HH component and malicious interference can be detected. The advantages are: more information per bit change representation in combination with error correction functions. Increases watermark data usability and maintains stability against visually invariant data deletion attacks.The disadvantage is that the image intensity values are limited to an LSB bit in the spatial field. The spatial domain is more likely to attack and therefore cannot be used.

Distributed Secret Sharing Approach with Cheater Prevention Based on QR Code: Design a secret QR sharing approach to securely and reliably distributed privately held QR-data. The approach proposed differs from the related QR code schemes, because it uses QR features to secrete sharing and can withstand print and scanning operations. Benefits include: Minimizes the secret security risk. It is possible to approach it. It offers readability of contents, cheater detectability and an adjustable QR bar code secret handling. Benefits are: Need to enhance QR barcode security. QR technology calls for the changes to be reduced.

Two-Level QR Code for Private Message Sharing and Document Authentication: The two-tier QR (2LQR) code, has two levels of public and private storage that can be used for authentication of documents. The public level is identical to the standard level of storage QR code, so any conventional QR code application is easy to read. The private level was built by substituting certain textures of the black modules. It is made up of information encoded with an error correction capability using qr code. Benefits include: It increases the classic QR code's storage capacity. The textured patterns used in 2LQR P&S sensitivity.

High payload secret hiding technology for QR codes: Paper explores the features of QR barcodes to design an enclosed QR Barcoding secret hiding mechanism that is more payloaded in comparison with previous ones to protect sensitive data. For a normal scanner, the formal information from the marked QR code can only be disclosed by a browser. The advantages are: the scheme designed is possible for steganography to hide the secrets into a small QR tag. The covered secret can only be disclosed successfully by the authorised user with the private key. Benefits are: Need to improve safety.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 6, June 2021||

DOI:10.15680/IJIRSET.2021.1006040

III. PROPOSED APPROACHES

The proposed system works to ensure data security by securely transmitting data across social media that keeps the data concealed within the texture image. This system is therefore designed for maintaining a high level of data transmission or network image security. In the proposed work, the QR code and the watermark are used to hide the secret message in the image. Efficient (n, n)-VSS scale encryption/decryption algorithms are also developed using image sharing coverage. Digital and printed media are the proposed algorithms applicable. There is also discussion of possible ways to hide the resulting share. The proposed NVSS scheme not only has a high level of user friendliness and manageability, but also reduces transmission risk and enhances the security of participants and shares.

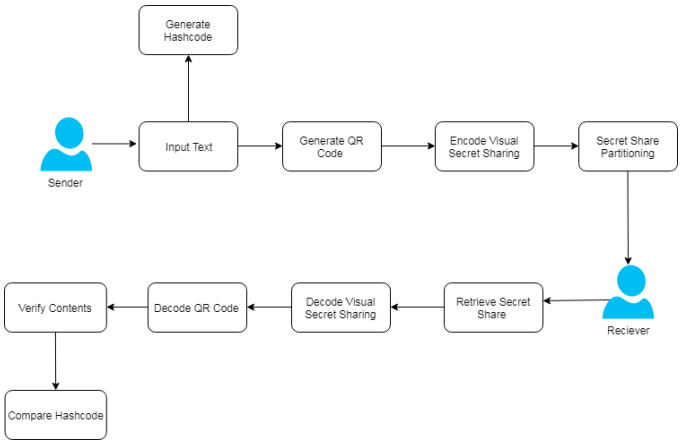

Figure. System Architecture

IV. CONCLUSION

The message and the picture are loaded with GUI. The process of Watermarking is used to hide the secret image message and also to extract the secret texture image message from our system. The recipient extracts a secret message. The methodology proposed uses watermarking for hiding data in the image that inputs the texture image pattern to hide text. The proposed VSS scheme can effectively reduce the risk of transmission and ensure that shareholdings and the secret image are user-friendly.

REFERENCES

1. 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).
2. Shaekh Hasan Shoron,MonamyIslam,BiprojitMondal,JiaUddin,"A Digital Watermarking Approach using SMQT,OTSU, DWT and IDWT"IEEE Conference 2018.
3. Abhilasha Singh, 2 Malay Kishore Dutta," Lossless and Robust Digital Watermarking Schemefor Retinal Images" International Conference on "Computational Intelligence and Communication Technology" (CICT 2018)
4. Etti Mathur, Manish Mathuria," Unbreakable Digital Watermarking using combination of LSB and DCT" International Conference on Electronics, Communication and Aerospace Technology ICECA 2017
5. 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.
6. P. P. Thulasidharan, M. S. Nair, "QR 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.
7. P. Y. Lin, "Distributed Secret Sharing Approach with Cheater Prevention Based on QR Code," IEEE Transactions on Industrial Informatics, vol. 12, no. 1, pp. 384-392, 2016.
8. Tkachenko, W. Puech, C. Destruel, et al., "Two-Level QR Code for Private Message Sharing and Document Authentication," IEEE Transactions on Information Forensics & Security, vol. 11, no. 13, pp. 571-583, 2016.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 6, June 2021||

DOI:10.15680/IJIRSET.2021.1006040

9. P. Y. Lin, Y. H. Chen, "High payload secret hiding technology for QR codes," Eurasip Journal on Image & Video Processing, vol. 2017, no. 1, pp. 14, 2017.
10. F. Liu, Guo T: Privacy protection display implementation method based on visual passwords. CN Patent App. CN 201410542752, 2015.
11. S J Shyu, M C Chen, "Minimizing Pixel Expansion in Visual Cryptographic Scheme for General Access Structures," IEEE Transactions on Circuits & Systems for Video Technology, vol. 25, no. 9, pp.1-1,2015.
12. H. D. Yuan, "Secret sharing with multi-cover adaptive steganography," Information Sciences, vol. 254, pp. 197–212, 2014.
13. J. Weir, W. Q. Yan, "Authenticating Visual Cryptography Shares Using 2D Barcodes," in Digital Forensics and Watermarking. Berlin, German: Springer Berlin Heidelberg, 2011, pp. 196-210.
14. G. Wang, F. Liu, W. Q. Yan, "2D Barcodes for visual cryptography," Multimedia Tools and Applications, vol. 2, pp. 1-19, 2016.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details