IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, April 2025
Impact Factor: 7.67

Cryptography Based Transactions Validation in Banking Sector

Mr. S. R. Tribhuvan[1], Shubham Anil Bhusal[2], Tohid Isak Shaikh[3], Satyam Balasaheb Kolse[4], Kartik Narayan More[5]
[1,2,3,4,5]Department of Cloud Computing and Big Data
Padmashri Dr. Vitthalrao Vikhe Patil Institute of Technology and Engineering (Polytechnic), Pravaranagar

Abstract: *Conventional visual secret sharing (VSS) schemes hide secret images in shares that are either printed on transparencies or are encoded and stored in a digital form. The shares can appear as noise-like pixels or as meaningful images; but it will arouse suspicion and increase interception risk during transmission of the shares. Hence, VSS schemes suffer from a transmission risk problem for the secret itself and for the participants who are involved in the VSS scheme. To address this problem, proposed a novel technique for digitalwatermarking using a texture and also a natural-image-based VSS scheme (VSS scheme) that shares secret images via various carrier media to protect the secret and the participants during the transmission phase. Contrive the texture synthesis process into digital image to hide secret messages. In comparison to using an existing cover image to hide messages, our algorithm hides the source texture image and embeds secret messages through the process of watermarking. The natural shares can be photos or hand-painted pictures in digital form or in printed form. We also propose possible ways to hide the secret to reduce the transmission risk problem for the share. Experimental results indicate that the proposed approach is an excellent solution for solving the transmission risk problem for the VSS schemes.*

Keywords: Data Security, high security, visual secret sharing scheme, Watermarking

I. INTRODUCTION

In most of the image watermarking methods, uses the existing image as their cover medium. This leads to two drawbacks. Since the size of the cover image is fixed, embedding a large secret message will results in the distortion of the image. Thus a compromise should be made between the size of the image and the embedding capacity to improve the quality of the cover image.

In the most years no of advances have been made in the range of computerized media, and much more concern has developed with respect to watermarking for computerized media. Watermarking is a solitary system for data hiding strategies. It implants messages into a host medium keeping in mind the end aim to cover secrete messages so as not to excite doubt by a meddler. A normal technique incorporates secretive correspondences between two gatherings whose presence is unclear to a conceivable attacker and whose achievement based on upon identifying the presence of this correspondence.

The VSS scheme uses diverse media as a carrier; hence it has many possible scenarios for sharing secret images. For example, assume a dealer selects n -1 media as natural shares for sharing a secret image. To reduce the transmission risk, the dealer can choose an image that is not easily suspected as the content of the media (e.g., landscape, portrait photographs, hand-painted pictures, and flysheets). The digital shares can be stored in a participant's digital devices (e.g., digital cameras or smart phones) to reduce the risk of being suspected. The printed media (e.g., flysheets or hand-painted pictures) can be sent via postal or direct mail marketing services. In such a way, the transmission channels are also diverse, further reducing the transmission risk.

DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, April 2025
Impact Factor: 7.67

II. RELATED WORK

In this paper[1], a watermarking algorithm of color image is proposed based on Discrete Wavelet Transform, Discrete Cosine Transform and Singular Value Decomposition (DWT-DCT-SVD). First convert host color image from RGB color space to YUV color space. Then a layer ofdiscrete wavelet transform is applied to the luminance component Y, and divided the low frequency and into blocks byusing discrete cosine transform, and conducted SVD with everyblock. Finally embed watermark to the cover image.

In this paper[2], a new digital watermarking model is proposed for the medical images. An improved SMQT is used forimage enhancement and the image is being segmented usingOTSU thresholding. Discrete Wavelet Transform (DWT) andInverse DWT are used to embed and extract the watermark onthe host image. The goal of our scheme is to make thewatermarking more robust against attacks and secure the image from privacy threats.

This paper[3] presents a Wavelettransform–Singular Value Decomposition based robust zero watermarking technique for medical images to address theprivacy and security issues. Unlike conventionalwatermarking, the proposed method conserves the reliability of the cover image without bringing any artifacts and withoutany change in the critical information contained in the medicalimage. The performance of the scheme is assessed with teleophthalmological images. The simulation results reveal therobustness of the proposed technique against various imageprocessing attacks and indicate its suitability for safe exchange of medical images among remote medical practitioners.

This research[4] is done to find the best digital watermarking technique to highly secure digital imageform the illegal copies. The research work also done toanalyze the possibilities of dual watermarking. Various standard research articles were studied and it is found that dual watermarking is possible with some situation.This research work motivates and offers different combinations on digital watermarking techniques in nearfuture for efficient output of watermarking.

The paper [5] proves that the contrast of XVCS is 2((k-1)) times greater than OVCS. The monotone property of OR operation degrades the visual quality of reconstructed image for OR-based VCS (OVCS). Accordingly, XOR-based VCS (XVCS), which uses XOR operation for decoding, was proposed to enhance the contrast. Advantages are: Easily decode the secret image by stacking operation. XVCS has better reconstructed image than OVCS. Disadvantages are: Proposed algorithm is more complicated.

In [6] paper, present a blind, key based watermarking technique, which embeds a transformed binary form of the watermark data into the DWT domain of the cover image and uses a unique image code for the detection of image distortion. The QR code is embedded into the attack resistant HH component of 1stlevel DWT domain of the cover image and to detect malicious interference by an attacker. Advantages are: More information representation per bit change combined with error correction capabilities. Increases the usability of the watermark data and maintains robustness against visually invariant data removal attacks. Disadvantages are: Limited to a LSB bit in the spatial domain of the image intensity values. Since the spatial domain is more susceptible to attacks this cannot be used.

In [7] paper, design a secret QR sharing approach to protect the private QR data with a secure and reliable distributed system. The proposed approach differs from related QR code schemes in that it uses the QR characteristics to achieve secret sharing and can resist the print-and-scan operation. Advantages are: Reduces the security risk of the secret. Approach is feasible. It provides content readability, cheater detectability, and an adjustable secret payload of the QR barcode. Disadvantages are: Need to improve the security of the QR barcode. QR technique requires reducing the modifications.

The two-level QR code (2LQR), has two public and private storage levels and can be used for document authentication [8]. 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 qr code with an error correction capacity. Advantages are: It increases the storage capacity of the classical QR code. The textured patterns used in 2LQR sensitivity to the P&S process. Disadvantages are: Need to improve the pattern recognition method. Need to increase the storage capacity of 2LQR by replacing the white modules with textured patterns.

To protect the sensitive data, [9] paper explores the characteristics of QR barcodes to design a secret hiding mechanism for the QR barcode with a higher payload compared to the past ones. For a normal scanner, a browser can only reveal the formal information from the marked QR code. Advantages are: The designed scheme is feasible to hide the secrets

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, April 2025
Impact Factor: 7.67

into a tiny QR tag as the purpose of steganography. Only the authorized user with the private key can further reveal the concealed secret successfully. Disadvantages are: Need to increase the security

III. GAP ANALYSIS

Sr. No	Author, Title and Journal Name	Technique Used	Advantages	Disadvantages	Refer Points
1	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.	XOR-based VCS (XVCS)	Easily decode the secret image by stacking operation. XVCS has better reconstructed image than OVCS.	More complicated.	This paper proves that the contrast of XVCS is $2^{(k-1)}$times greater than OVCS.Accordingly, XOR- based VCS (XVCS), which uses XOR operation for decoding, was proposed to enhance the contrast.
2	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.	Watermarking tech -nique for QR code	More information representation per bit change combined with error correction capabilities. Increases the usability of the watermark data and maintains robustness against visually invariant data removal attacks.	Limited to a LSB bit in the spatial domain of the image intensity values. Since the spatial domain is more susceptible to attacks this cannot be used.	The QR code is embedded into the attack resistant HH component of 1stlevel DWT domain of the cover image and to detect malicious interference by an attacker.
3	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.	A secret QR sharing scheme	Reduces the security risk of the secret. Approach is feasible. It provides content readability, cheater detectability, and an adjustable secret payload of the QR barcode.	Need to improve the security of the QR barcode. QR technique requires reducing the modifications.	The proposed approach differs from related QR code schemes in that it uses the QR characteristics to achieve secret sharing and can resist the print-and-scan operation.
4	I. 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.	Two-level QR code	It increases the storage capacity of the classical QR code. The textured patterns used in 2LQR sensitivity to the P&S process.	Need to improve the pattern recognition method. Need to increase the storage capacity of 2LQR by replacing the	The two-level QR code (2LQR), has two public and private storage levels and can be used for document authentication.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, April 2025
Impact Factor: 7.67

				white modules with textured patterns.	
5	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.	Secret hiding for QR barcodes.	1.The designed scheme is feasible to hide the secrets into a tiny QR tag as the purpose of steganography.	1. Need to increase the security	To protect the sensitive data, this paper explores the characteristics of QR barcodes to design a secret hiding mechanism for the QR barcode with a higher payload compared to the past ones.

IV. PROPOSED APPROACHES

Proposed system working to facilitate the data security in getting secure transmission of data over social media which maintain the data hiding inside texture image. Hence this system is suitable for maintaining high level security for data transmission or image preservation in the network.

In proposed work, watermarking is used to hide the secret message in image and also extract the secret message from texture image.

Also we develop efficient encryption/decryption algorithms for the (*n, n*) -VSS scheme using cover image's shares. The Proposed algorithms are applicable to digital and printed media. The possible ways to hide the generated share are also discussed. 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.

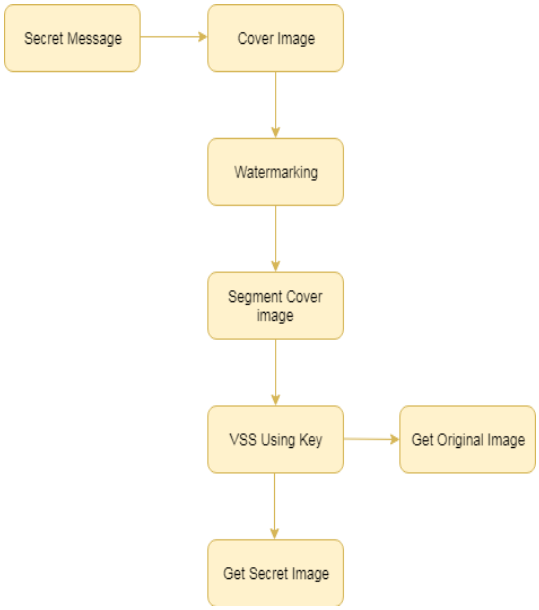
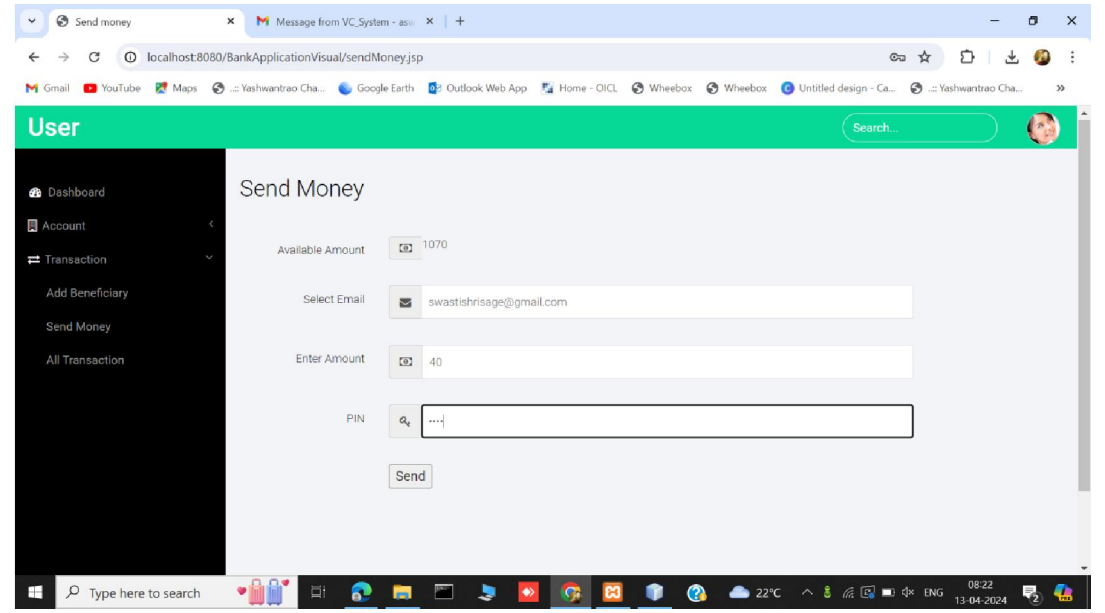
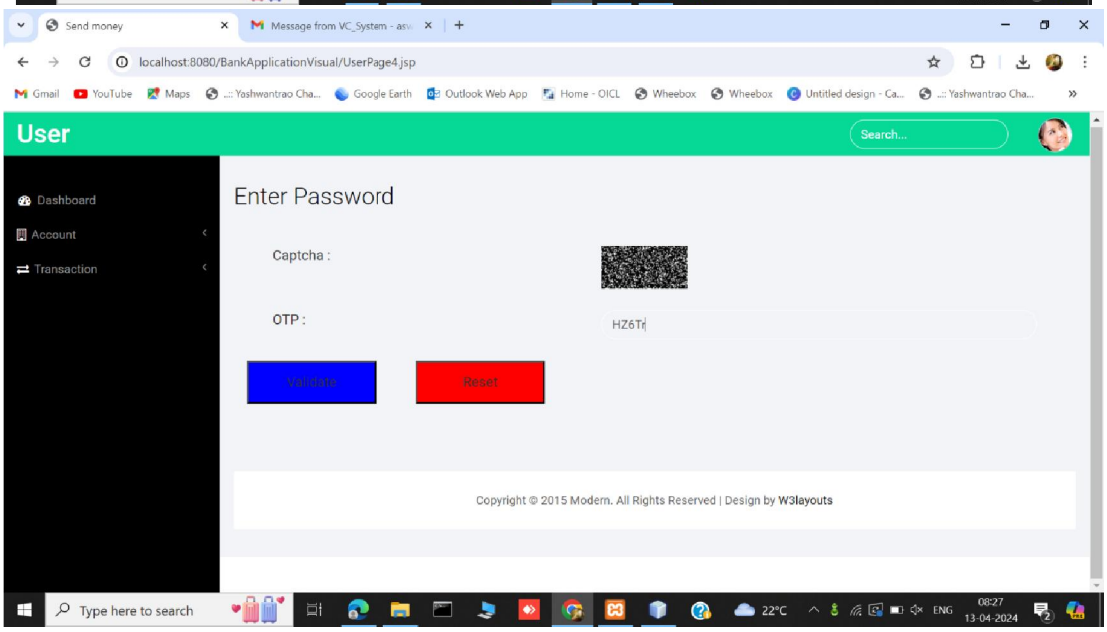


Fig. 1 Flow Diagram

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, April 2025
Impact Factor: 7.67

V. RESULT





VI. CONCLUSION

The message and image is loaded by using GUI format. Watermarking process is used to hide the secret message in image and also extract the secret message from texture image in our system. Secret message will extract by receiver. Proposed methodology uses watermarking for hiding data inside the image which input the texture image pattern for hiding text in the data. The proposed VSS scheme can effectively reduce transmission risk and provide the highest level of user friendliness for shares and for secret image

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, April 2025
Impact Factor: 7.67

REFERENCES

[1] 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.
[2] 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.
[3] 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.
[4] I. 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.
[5] 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.
[6] F. Liu, Guo T: Privacy protection display implementation method based on visual passwords. CN Patent App. CN 201410542752, 2015.
[7] 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.
[8] H. D. Yuan, "Secret sharing with multi-cover adaptive steganography," Information Sciences, vol. 254, pp. 197–212, 2014.
[9] 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.
[10] G. Wang, F. Liu, W. Q. Yan, "2D Barcodes for visual cryptography