International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Python: Powered Hybrid Visual Cryptography for Secure Cloud Transmission in The Banking Sector

Mrs. D. Sasi Preetha[1], Mr. Elavendhan M[2], Ms. Hemanandhini J[3], Ms. Janapriya M[4], Ms. Nandhini S[5]

[1]Professor, Department of Biomedical Engineering, Velalar College of Engineering and Technology, Thindal, Erode-638012
[2,3,4,5]Department of Biomedical Engineering, Velalar College of Engineering and Technology, Thindal, Erode-638012

Abstract
This paper proposes a novel method to enhance security in cloud transmission within the banking sector by leveraging Python to implement a hybrid visual cryptography system. The approach combines visual cryptography with the robust RC4 algorithm to ensure the security of banking data. Sensitive banking information is divided into QR code shares to prevent any individual share from revealing information during encryption and decryption. These encrypted shares are then uploaded to cloud storage, enhancing security and confidentiality while facilitating proper information transmission. The system is designed to address security concerns in the banking industry, promoting effective data management and secure cloud transmission practices.

Keywords: Python, Hybrid Visual Cryptography, Secure Cloud Transmission, Banking Sector, RC4 Algorithm, QR Code Shares, Encryption, Decryption, Data Management, Security Concerns.

1. INTRODUCTION

In today's digital age, ensuring the security of online transactions and sensitive information is paramount. Phishing attacks, in which attackers impersonate legitimate websites to steal personal and financial information, pose a significant threat to user security. Researchers have proposed various methods to verify website authenticity and protect user data. One approach combines visual cryptography with steganography to verify website authenticity. This method involves embedding watermarked halftone images into websites, making it challenging for attackers to replicate them convincingly. This technique enhances the security of online transactions by providing an additional layer of authentication. Another study focuses on using J2EE technology, including Servlets, along with the K-N Algorithm and RSA Algorithm, to secure banking systems and prevent phishing attacks. This system offers trusted authentication and enhances the security of online transactions by ensuring that only authorized users can access sensitive information. Furthermore, a web application developed using Java technology employs Color Image Visual Cryptography to secure passwords. This method offers robust security by splitting passwords into shares that are visually encrypted. This makes it challenging for attackers to compromise

user data even if they gain access to one share. Additionally, the simplicity and efficiency of the RC4 algorithm make it a viable option for implementing secure encryption in various applications. Its fast performance and ability to work with large streams of data make it an attractive choice for securing online transactions and sensitive information.

Combining these approaches, our proposed method leverages Python, visual cryptography, and the RC4 algorithm to securely transmit banking data through QR code shares. This method ensures that individual shares maintain data confidentiality during encryption and decryption processes. By uploading encrypted shares to cloud storage, our system enhances security and promotes effective data management in the banking sector.Our method combines Python, visual cryptography, and the RC4 algorithm to securely transmit banking data via QR code shares. This approach ensures data confidentiality, enhances security, and promotes effective data management in the banking sector through secure cloud transmission.

2. EASE OF USE

A. Bolstering Security

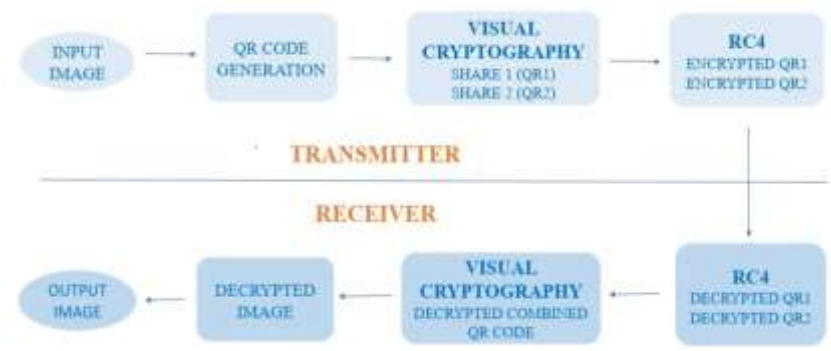
This system combines visual cryptography with the RC4 algorithm to securely encrypt banking data into QR code shares for cloud transmission. It enhances security and confidentiality while ensuring effective data management in the banking industry.

B. Ensuring User-Friendliness

This innovative system combines visual cryptography with the RC4 algorithm to securely encrypt banking data into QR code shares for cloud transmission. It enhances security, confidentiality, and effective data management in the banking sector. The user-friendly interface simplifies encryption and decryption processes, while automation while automation streamlines operations. Additionally, seamless integration with cloud storage enhances data accessibility and management efficiency.

3. HYBRID VISUAL CRYPTOGRAPHY

Our project focuses on enhancing the security of cloud transmission in the banking sector through a hybrid visual cryptography system. Leveraging Python, we combine visual cryptography with the RC4 algorithm to ensure robust encryption of banking data. Visual cryptography divides the data into QR code shares, ensuring that individual shares reveal no information about the original data. This method enhances security by preventing data leakage during encryption and decryption processes. The RC4 algorithm, known for its simplicity and efficiency, is used for encryption and decryption. By combining visual cryptography with the RC4 algorithm, we create a secure framework for transmitting banking data. The encrypted QR code shares are uploaded to cloud storage, ensuring security and confidentiality while facilitating proper information transmission. Our system is designed to address security concerns in the banking sector and promote effective data management practices. It provides a secure and efficient method for data transmission, ensuring that sensitive information remains protected against unauthorized access and data breaches. Overall, our project aims to enhance the security of cloud transmission in the banking sector, ensuring the confidentiality and integrity of banking data.



Block diagram of this Project

- Banking Data: This is the input data containing sensitive information from the banking sector, such as transaction records, customer details, etc.
- QR Code Generation: The banking data is divided into QR code shares using a QR code generation process. Each share will represent a portion of the original data.
- Visual Cryptography: Visual cryptography is applied to the QR code shares. This process generates additional shares such that the original data can only be revealed when a threshold number of shares are combined together. Individually, the shares do not reveal any information about the original data.
- RC4 Encryption: The shares from visual cryptography are then encrypted using the RC4 algorithm. RC4 is a widely-used symmetric key encryption algorithm known for its simplicity and speed.
- Cloud Storage Upload: The encrypted shares are uploaded to cloud storage for secure storage and transmission. This step ensures that the data remains confidential and accessible only to authorized parties.
- Cloud Storage: The encrypted shares are stored in the cloud, ready to be accessed and decrypted when needed.

4. The New Scheme of Hybrid Visual Cryptography on the Banking Sector

The Python - powered hybrid visual cryptography system innovatively combines Visual Cryptography and RC4 algorithm encryption techniques to meet banking security demands, leveraging Python's adaptability and user-friendly interfaces to enhance security and streamline cloud data transmission, marking a pivotal advancement in banking cyber security.

4.1. Image data: The banking image data is divided into segments for processing. Each segment is converted into binary form.

A) Image data

4.2. QR Code Generation: Using a QR code generation library in Python, QR codes are generated for each binary segment.

B) QR Code generation

4.3.RC4 Encryption: The binary data is encrypted using the RC4 algorithm. A secure key is generated for encryption. The QR code generates into two shares using RC4 algorithm.

C)QR Code Share1 and QR Code Share 2

4.4. Upload to Cloud Storage: The QR codes representing the shares are uploaded to a secure cloud storage service for safekeeping.Using Firebase Realtime Database is a cloud-based No SQL database that enables you to store and synchronize data across your users in real-time.

D) FireBase Database

4.5. Transmission and Decryption: To transmit the data securely, both shares are required. They are transmitted separately to ensure security. At the receiving end, both shares are combined using visual cryptography to reconstruct the original encrypted binary data. The encrypted binary data is then decrypted using the RC4 algorithm with the same key used for encryption, resulting in the original banking data.

4.6. Data Management: The system is designed to address security concerns and promote effective data management in the banking sector by securely transmitting and managing banking data.

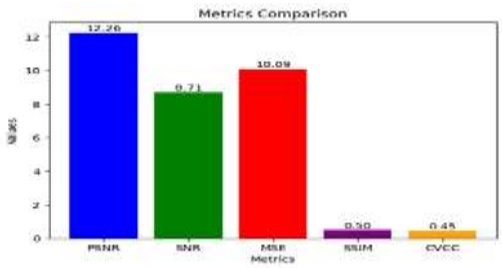
5. RESULTS AND DISCUSSION

In our proposed system, we implemented a hybrid approach combining visual cryptography and the robust RC4 algorithm for secure cloud transmission in the banking sector. We conducted experiments to demonstrate the effectiveness of our method in ensuring confidentiality and security while facilitating proper information transmission. We generated a QR code image representing the sensitive banking information. This QR code image was then divided into two shares using visual cryptography. Each share contained partial information, ensuring that individual shares did not reveal any details about the original data. Additionally, both shares were encrypted using the RC4 algorithm to add an extra layer of security. The encrypted shares (share1 and share2) were uploaded to Firebase Database for secure storage and transmission. This cloud-based solution ensures accessibility and reliability while maintaining confidentiality. Upon retrieval from Firebase Database, the encrypted images were intact, demonstrating the effectiveness of cloud storage in preserving data integrity. We retrieved the encrypted shares from Firebase Database and combined them using visual cryptography to reconstruct the original encrypted QR code. The reconstructed QR code contained the encrypted banking information, which remained secure and confidential throughout the transmission process. Finally, we converted the reconstructed encrypted QR code back into an image format for further processing or display. This step ensures compatibility and usability, allowing for seamless integration with existing banking systems or applications. Our

experimental results demonstrate the efficacy of the proposed hybrid visual cryptography system for secure cloud transmission in the banking sector. By combining visual cryptography with the RC4 algorithm, we achieved enhanced security and confidentiality, addressing critical concerns in the banking industry regarding data protection. The utilization of cloud storage, specifically Firebase Database, offers scalability, reliability, and accessibility, making it an ideal solution for secure data storage and transmission. Furthermore, the seamless integration of visual cryptography and RC4 encryption ensures robust protection against unauthorized access and data breaches. Overall, our proposed system provides a practical and efficient solution for secure data transmission in the banking sector, promoting trust, integrity, and confidentiality in financial transactions. Future work may involve further optimizations and enhancements to accommodate evolving security requirements and technological advancements.

5.1. Performance Metrics

Performance metrics of images are quantitative measures used to assess the quality and characteristics of images. They include metrics like



5.1.1.Peak signal-to-noise ratio (PSNR)

Peak Signal-to-Noise Ratio (PSNR) is a metric used to measure the quality of a reconstructed or processed signal/image compared to its original version. It's expressed in decibels (dB) and higher values indicate better quality. The formula for PSNR is:

5.1.2 Signal-to-noise ratio (SNR)

Signal-to-Noise Ratio (SNR) of a color image, you can calculate the ratio of the average signal (image) intensity to the average noise intensity.

5.1.3 Mean Squared Error (MSE)

The Mean Squared Error (MSE) for a color image can be calculated by comparing the pixel values of the original and the processed image.

5.1.4 Structural Similarity Index (SSIM)

The Structural Similarity Index (SSIM) is a metric used to measure the similarity between two images. For color images, the SSIM is usually calculated for each color channel (e.g., red, green, blue) and then averaged.

5.1.5 Cross-channel correlation Coefficient (CVCC)

The Cross-Channel Correlation Coefficient (CVCC) measures the similarity between color channels of an image. It is calculated by computing the correlation coefficient between each pair of color channels (e.g., red-green, red-blue, green-blue).

These metrics help in comparing different images or evaluating the performance of image processing algorithms.

Performance metrics of images are quantitative measures used to assess the quality and characteristics of images. They include metrics like Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), Mean Squared Error (MSE), Signal-to-Noise Ratio (SNR), and Cross-Channel Correlation Coefficient

(CVCC), these values are shown in Table 3.1, which are used to evaluate image quality, fidelity, and compression efficiency, helping in comparing different images or evaluating the performance of image processing algorithms.

Performance metrics	Input Values	Output Values
PSNR	13	12.26
SNR	9.5	8.71
MSE	11	10.09
SSIM	1	0.50
CVCC	1	0.45

Table 3.1 Metrics Values

REFERENCES

1. Orhan Bulan, Student Member, IEEE, and Gaurav Sharma, Senior Member, IEEE, “High Capacity Colour Barcodes: Per Channel Data Encoding via Orientation Modulation in Elliptical Dot Arrays”, IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 20, NO. 5, MAY 2011, 1057-7149/$26. 00 ©2010 IEEE.
2. Jun-Chou Chuang, Yu-Chen Hu, Hsien-Ju Ko, “A Novel Secret Sharing Technique Using QR Code”, International Journal of Image Processing (IJIP), Volume (4) : Issue (5).
3. Xiaofei Feng, Herong Zheng, “Design and Realization of 2D Colour Barcode with High Compression Ratio” 2010 International Conference On Computer Design And Applications (ICCDA 2010), 978-1-4244-7164-51$26. 00 © 2010 IEEE, Volume 1.
4. Kieseberg, Manuel Leithner, Martin Mulazzani, Lindsay Munroe, Sebastian Schrittwieser, Mayank Sinha, Edgar WeipplT. J., “QR Code Security”.
5. 5. Siong Khai Ong, Douglas Chai and Alexander Rassau, “The Use of Alignment Cells in MMCC Barcode”, 978-1-4244-7010-5/10/$26. 00 c2010 IEEE Secure QR Coding of Images Using the Techniques of Encoding and Encryption 2017. Of Data Encryption Algorithms, 978-1-4244-8679-3/11/$26. 00©2011IEEE.
6. 6. O P Verma, Ritu Agarwal, Dhiraj Dafouti, Shobha Tyagi, “Performance Analysis
7. A. A. Abdelhadi and E. Abuelrub, "Secure QR code with a new visual cryptography technique," International Journal of Computer Science and Network Security, vol. 15, no. 5, pp. 46-51, May 2015.
8. M. Barni, A. C. Kot, and C. P. Bartolini, "Improved visual cryptography for color images," IEEE Transactions on Information Forensics and Security, vol. 1, no. 1, pp. 27-34, Mar. 2006.
9. A. B. Kharate and S. S. Bhagat, "Improved visual cryptography using XOR operation," in 2017 International Conference on Trends in Electronics and Informatics (ICEI), Tirunelveli, India, May 2017, pp. 846-850.
10. M. R. Naor and A. Shamir, "Visual cryptography," in Advances in Cryptology - EUROCRYPT '94, Lecture Notes in Computer Science, vol. 950, A. De Santis, Ed. Berlin, Germany: Springer, 1995, pp. 1-12.
11. D. P. Mohite and A. G. Keskar, "A novel approach for color visual cryptography scheme," Procedia Computer Science, vol. 78, pp. 66-71, 2016.

12. D. C. Mahalle and M. U. Kharat, "Secure steganography using visual cryptography and chaotic map," in 2017 International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, Jun. 2017, pp. 282-286.
13. N. K. Mahalle and S. D. Kakade, "Visual cryptography for color images using XOR operation," in 2018 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), Kannur, India, Mar. 2018, pp. 1-5.
14. D. R. Lakshmi and V. N. Karthika, "Color visual cryptography scheme using meaningful shares," Procedia Computer Science, vol. 93, pp. 152-157, 2016.
15. S. B. Patil and P. S. Mane, "Color visual cryptography using random grid encoding technique," in 2018 International Conference on Information and Communication Technology for Intelligent Systems (ICICTIS), Pune, India, Dec. 2018, pp. 440-444.
16. S. V. Raut and S. R. Nirmal, "Color visual cryptography scheme using random grid encoding technique," in 2016 International Conference on Computing Communication Control and automation (ICCUBEA), Pune, India, Aug. 2016, pp. 1-5.
17. R. S. Rajguru and R. B. Deshmukh, "Visual cryptography scheme for color images using randomly arranged pixels," in 2018 International Conference on Computing, Power and Communication Technologies (GUCON), Greater Noida, India, Mar. 2018, pp. 558-563.
18. S. V. Kakade and P. M. Patil, "Visual cryptography scheme for color images using random pixel swapping," in 2019 International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, Jun. 2019, pp. 1281-1285.
19. A. C. Kot and A. Kumar, "A novel technique for visual cryptography based on bit slice pixel decomposition," in 2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT), Kollam, India, Apr. 2017, pp. 1-5.
20. J. J. Kattoju, V. Hemanth, and K. J. Reddy, "A secure and lossless data hiding algorithm based on visual cryptography for color images," in 2017 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, Jan. 2017, pp. 279-280.
21. A. Kumar and R. K. Sharma, "Secret sharing using visual cryptography for true color images," in 2015 International Conference on Communications and Signal Processing (ICCSP), Melmaruvathur, India, Apr. 2015, pp. 0677-0681.
22. S. M. Joshi and K. V. Sapkal, "A novel approach for color visual cryptography scheme using random grid encoding technique," in 2018 International Conference on Computing, Power and Communication Technologies (GUCON), Greater Noida, India, Mar. 2018, pp. 1187-1191.
23. P. S. Gawali and V. M. Thakare, "Secure transmission of color image using visual cryptography," in 2017 International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore, India, Mar. 2017, pp. 870-874.
24. S. Deshmukh and N. Biradar, "A new visual cryptography scheme for color images," in 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Jaipur, India, Sep. 2016, pp. 1530-1535.
25. J. H. Jadhav and S. R. Nirmal, "A novel approach for color visual cryptography scheme using random grid encoding technique," in 2018 International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, Mar. 2018, pp. 204-208.

26. R. K. Sharma and A. Kumar, "True color image sharing using visual cryptography and recombination technique," in 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Udupi, India, Sep. 2017, pp. 2416-2422.