VOL. 18, NO. 4, FEBRUARY 2023 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

A ROBUST VC SCHEME FOR SECURING CLOUD DATA STORAGE

Hemalatha R. and Selvi S.
Department of Computer Science, PSG College of Arts and Science, Coimbatore, India
E-Mail: latharajiphd123@gmail.com

ABSTRACT

Visual Cryptography (VC) was created to encode images into several shares and decode them by aggregating the shares without the use of costly standard cryptanalysis. To enhance the quality and security of visual images in cloud storage, a Robust Collusion Avoidance-based Secure Signific VC (RCA-SSVC) scheme was designed, which creates the collusion-resistance Secret Image (SI) shares and embeds them into the Cover Image (CI) to prevent collusion threats. But it takes a long-time during access for users to recover the real image whenever receiving fake shares kept in the cloud by unauthorized users. Therefore, in this article, a new 2-level data protection scheme is proposed using QR code and RCA-SSVC. In this scheme, the public and private information of users are taken as QR code, which is encoded into sub-pixel blocks of all shares during the share creation phase. Also, a random permutation is applied to the created shares to disrupt the sub-pixels in a single block, which can avoid attackers from guessing the location of the Secret QR (SQR) code's pixels. During the image restoration step, the restoration process is initiated once the user identity is authenticated by reading QR code information, which is matched with the QR code embedded in the shares. So, image restoration using illegitimate shares during access is prevented. At last, the test outcomes reveal that the RCA-SSVC-QR establishes maximum confidentiality in image access from the cloud storage compared to the classical VC schemes.

Keywords: cloud storage, RCA-SSVC, QR codes, image recovery, 2-level data protection, secret shares.

INTRODUCTION

Cloud computing is a concept that enables numerous industries, financial firms, pharmacists, and public sectors to collect, examine, and establish database-driven solutions. Yet, data storage security is problematic due to numerous issues and discrepancies. Typical data losses include information recovery resilience, host activity protection, and metadata permissions. Information suppliers are worried about the quality and veracity of their information [1-2]. Cryptographic algorithms have been employed to ensure secrecy during processing and transmission. They are effective for embedding the raw data into a secret key and recovering it to obtain the real data [3-4].

These solutions demand considerable knowledge and significant practices. They also require a proper insight into cryptanalysis. VC is a cryptosystem that is used to conceal image content that the recipient can decode using the corresponding key picture [5]. The approach makes use of two sorts of images: one with scrambled pixels and one with secret information. The secret picture is split into two or more small, asymmetrical fragments that do not include the sensitive data. The secret code key can only be disclosed by merging the shares [6]. It helps VC when we are inexperienced with cryptology and extensive estimation. A shared secret is referred to as VC in cryptology. It enables people to mask secrets in multiple shares that do not characterize obscurity until they are combined. VC is particularly fit for sensitive applications such as genetic encryption, automation, steganalysis, and cryptocurrencies [7-9]. Key-free cryptography, processability, no decoding, decreased estimation costs, and delivery through FAX or email are a few of the benefits of using VC. Most recent research has used various VC approaches to achieve a range of goals [10-12].

Mary and Kumar [13] developed a unique Error Abatement Technique (EAT) that outperformed various VC strategies. It makes use of value discretization and low-error filtration techniques. The value discretization filter extracts the pixel coefficients from the grayscale SI and computes the neighboring pixel loss, which may subsequently be standardized to yield meaningful shares. Further, decreased error filter was employed to lessen created errors and remain close to important shares. Besides, (x, n) and (n, n)-SVC approaches were developed, where x was the minimum number of shares needed to restore the SI and n was the total number of shares formed. These approaches comprise share creation and reconstruction phases. In contrast, this LSB embedding and mining was prone to steganography and therefore not at all secure. Its robustness was also weakened since it is readily decrypted by extracting the image's LSBs and recovering the information in a binary sequence. The image quality may degrade according to how many pixels were modified when the embedding data includes more than one LSB.

To combat these problems, (x, n) and (n, n)-SSVC schemes [14] were developed, which replaces the LSB embedding and mining processes in the SVC method with the CSF. During the share creation step, the SI was turned into the SSI, and shares were created. The CSF then opted to choose the CI blocks, and the generated secret share values were randomly embedded with the CI blocks that were chosen. As a consequence, meaningful and semantic shares were formed. These connected CI blocks were known as shares. The produced shares were then sent to the user via the transmission channel. To recover the SI, a key share was created from the received shares during the recovery step. Nonetheless, the main issue was that this scheme was prone to collusion threats, i.e., one of the SIs was discovered through cooperation. Such findings

can be obtained when two shares collude. So, neither the produced shares were random nor were they immune to collusion in this scheme. Another issue was that its resistance to external noise was low. So, randomization and collusion resistance were essential for SSVC to be successful.

For this purpose, a novel (n, n)-Robust Collusion Avoidance-based SSVC (RCA-SSVC) scheme [15] was developed that provides collusion resistant image shares in such a way that all shares were reliant on all other pictures, or at least the majority of the images. This characteristic ensures that information was distributed uniformly across users and protects against collusion threats. To produce shares from SIs, this scheme employs Boolean XOR operation during the share generation process. In addition, the shift-bit method was used to substitute the first four bits of all pixels with the last four bits of that pixel. It generates shares only when the earlier shares have already been generated. Though the security of the images/data was protected in the cloud storage, it takes more time for users to restore the actual information while receiving fake shares, which were stored in the cloud by illegitimate users. In other words, any information about the SI cannot be recovered from the group of shares, whose number was less than x. Likewise, when shares are entirely noisy, it was not probable to determine when they have errors incurred during archiving before adequate shares have been acquired to recover the actual image.

Hence, this paper proposes a new 2-level data protection scheme depending on QR code and RCA-SSVC. In this scheme, the public and private information of users are taken as QR code, which is encoded into sub-pixel blocks of all shares during the share creation phase. Also, a random permutation is applied to the created shares to disrupt the sub-pixels in a single block, which can avoid attackers from guessing the location of the SQR code's pixels. During the image restoration step, the restoration process is initiated once the user identity is authenticated by reading QR code information, which is matched with the QR code embedded in the shares. Thus, this RCA-SSVC-QR scheme can embed the QR code into the visual shares to prevent the users from restoring the data/image using the non-authenticated shares. Unlike prior RCA-SSVC scheme, the presented scheme integrates RCA-SSVC with QR codes, such that any one of the created share was not able to recover the actual image; but can read the QR code for authenticating user and legitimate shares. Thus, without a sufficient number of shares and verified QR codes, the actual image cannot be recovered.

The residual parts of this paper are arranged as the following: Section II presents the research on VC based on QR code strategies. Section III explains the presented scheme, while Section IV displays its effectiveness. Section V concludes this study and offers the upcoming enhancement.

LITERATURE SURVEY

Fu *et al*. [16] developed a (k, n)-VCS merged with QR codes. A probabilistic sharing scheme was used for enlarging the allowable maximum size of the SI. So, the secret sharing scheme was adopted with high relative variance. Also, the primary shares were embedded into cover QR codes by utilizing encoding redundancy. Then, all shares were meaningful and read by the typical QR code reader. But, the size of the SI was inadequate and the secret payload of QR codes was not easily improved.

Bakshi & Patel [17] presented a solution to secure telemedicine using Region-Of-Non-Interest (RONI) halftone VC without pixel expansion. Initially, the RONI of the image was mined and the Integrity Check Value (ICV) was embedded into any one of the RONI areas. Then, the embedded RONI area was halftone and shares were created for the resultant image. But it needs to consider additional data for increasing the efficiency of embedding.

Liu *et al*. [18] developed a (3,3)-threshold Visual Secret Sharing (VSS) for the QR code method, which completely uses the additional choice, offered through the color VSS and stacking. The dual covert AR code was enciphered into color shares. A dual color QR code was recreated by stacking each share. Then, the actual dual QR code was entirely recreated once the inherent preprocessing was completed in the QR code decoder. But, the safety of QR codes was not efficient and it has a high computation burden.

Zhu *et al*. [19] designed a high-capacity optical encryption method depending on the Single-shot-Ptychogrpahy Encoding (SPE) scheme and QR code. First, 2 QR codes were used as date containers, one of which was encoded into random binary images via VC. Then, the encoded images were encrypted by the SPE scheme. In contrast, its difficulty was high if the amount of SIs was high.

Xiong *et al.* [20] developed an efficient Discrete Wavelet Transform-related SI Sharing with Authentication (DWT-SISA). In this method, a CI was analyzed using DWT having a secret key of all participants, whereas the secret key was a filtration collection of DWT. After that, all t-pixel was split into a single part and the coefficients of $(t-1)$-order polynomial were substituted by the part of t-pixels to create a set of shades. Moreover, the dual ranges of all pixels in the shade were partitioned into 3 segments, which were entrenched into the 3 high-spectrum of the CI along with the validation bits once 1-point 2D-DWT depending on LSB substitution. But, the problem of revealing secrets in Shamir's polynomial SI allocation was not resolved.

Wan *et al*. [21] developed a VSS method with (n, n) threshold for discriminating covert data depending on QR codes. Initially, the covert data was enciphered into the SQR code. After that, such SQR code was entrenched into n cover QR codes. Further, the SQR code was recreated by the QR code VSS method, which conducts the stacking and XOR decryptions. But, the SQR code was not able to recreate when it contains a few errors.

Tan *et al*. [22] developed a robust (k,n)-threshold XOR-ed VSS (XVSS) method depending on the QR code and the fault alteration strategy. In this method, XVSS was used to distribute a SI and create noisy shades having larger image excellence and no pixel extension. Also, the stuffing codewords of cover QR codes were substituted using the bits of shades to create strong and significant shades. Further, the SI was restored from at least $k$shadows. Conversely, the size of the SI was constrained using the amount of stuffing codewords of the cover QR code.

Huang *et al*. [23] designed an (n,n)-threshold SS method by using the fault alteration ability of QR code. In this method, a SQR code was partitioned and enciphered into n cover QR codes. The created manifest QR codes contain CI therefore that they can highly decrease the distrust of illegal persons when communicated in the open media. The SQR code was simply recreated by the XOR function while each n allowed participants to collaborate. But, it needs to analyze the homomorphism of QR codes to enhance the access structure from $(n,n)$to (k,n).

Chow *et al*. [24] presented 2 schemes of confirming the visual fidelity of image-based databases with the aid of QR codes to identify perturbations in the data. In the primary scheme, a validation string was accumulated for all images in a database. Such strings were utilized to estimate whether or not an image in the database was perturbed. In the second scheme, only a single validation string was accumulated and utilized to confirm whether a whole database was intact. But, the visual fidelity of separate images was not determined in the AVS scheme.

Pan *et al*. [25] designed 2 novel methods utilizing color XOR to completely recover the covert color image and create meaningful shares. The initial method was used to create meaningful shares. The second method was utilized to create $n-1$ significant and insignificant shares. According to the initial method, $n-1$ shares were changed to color QR codes in the subsequent method. Such color QR codes were deciphered using the normal decoder and each share was conducted with the color XOR to recover the entire covert color image. But, the decoding speed was impacted by the size of the color QR code and the quality of shares was not effective.

PROPOSED METHODOLOGY

In this section, the presented 2-level data protection scheme is explained. This presented scheme focuses on the image transmission with security and privacy considerations among users. Secure login access is provided among the users to access the cloud storage; the user has to login with authenticated QR code to access the shares and retrieve the actual image. For the data protection scheme, RCA-SSVC is applied to hidden the actual image with CI. After the user is authorized by the QR code to use the image, it needs the shares to be decoded to obtain the actual image. The block diagram of RCA-SSVC with QR code authentication is depicted in Figure-1.

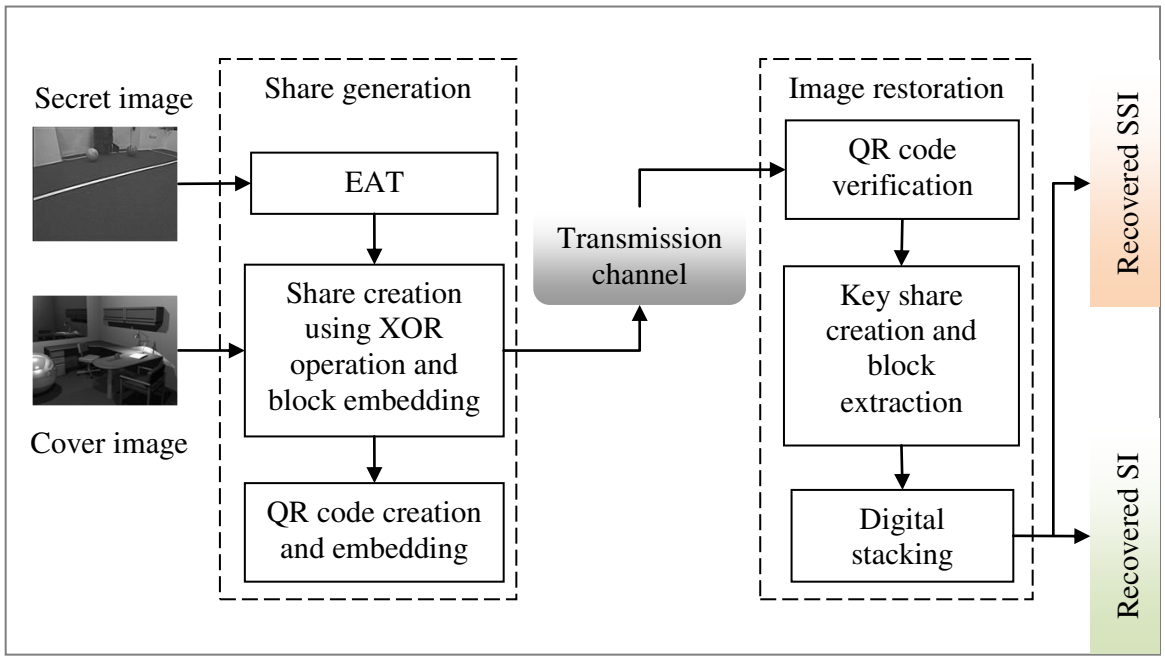

Figure-1. Block diagram of RCA-SSVC with QR code authentication for image restoration.

Also, the schematic representation of this presented scheme is depicted in Figure-2. By utilizing this scheme, the image is encoded with the RCA-SSVC of the shared image and the encoded image is accumulated in the cloud storage. For the image that is accumulated in the cloud storage to be utilized, the user should authenticate QR code. Using the identical scheme at the recipient end, if the recipient has the authenticated QR matched with the QR code embedded in each share, they are permitted to

access the image and restore the actual image that is stored before the encoding task in the cloud data storage.

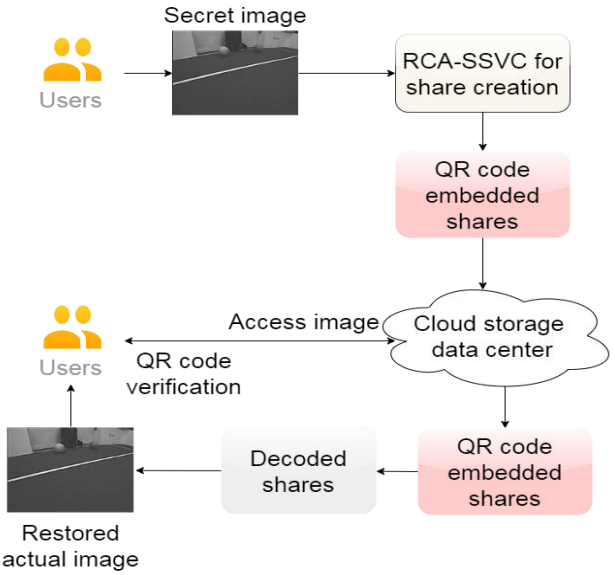

Figure-2. Schematic representation of presented cloud storage and image restoration security.

Compared to the many VC schemes, it satisfies (n, n) RCA-SSVC, whereas n denotes the number of shares generated to secure the data storage and access. The aim of this scheme is to resolve the access authentication issue of the public and private information of a group. The public information is accessible for anyone in the group, whereas the private information can only be obtained by the particular trusted person. To combat the access authentication during image restoration, this scheme is designed, which performs 3 primary processes: share creation, QR code embedding and image restoration.

During share creation, n number of SIs is encoded to generate n random share images $\{S_{i,j}^1, S_{i,j}^2, \dots, S_{i,j}^n\}$. To generate l^{th} share, XOR function is applied for primary $l-1$ shares and accumulated in z. Also, z is modified by executing XOR function with the $l+1^{th}, l+2^{th}, \dots, l^{th}$ actual images. Then, shift-bit algorithm on z is performed to substitute the initial 4 bits of all pixels with the final 4 bits of that pixel in each share. Moreover, XOR is employed on the resulting pictures to produce the final share pictures [15].

Embedding User QR Code with Visual Shares

Consider $U = \{1,2, \dots, n\}$ refers to the group of users, $PU_i = \{pu_1, \dots, pu_p\}$ is the public information of participant $i, (i = 1, \dots, n)$ and p denotes the amount of public data about the user (e.g. name, gender, age, etc.), $PR_i = \{pr_1, \dots, pr_r\}$ is the private information of participant $i, (i = 1, \dots, n)$ and r indicates the amount of private data about the user (e.g. IP address, etc.). During this phase, PU_i and PR_i of each user is initially encoded into QR code as Q_{xy}^i, respectively, where $x, (x = 1, \dots, p)$ is the number of rows and $y, (x = 1, \dots, r)$ is the number of columns in the QR code. After that, the secret sharing method considers the n visual shares and $n-1$ QR codes as inputs to provide n QR code embedded shares. Figure 3 illustrates the secret sharing process, wherein 4 visual shares and 4 QR codes are considered in this study to generate 4 QR-embedded shares.

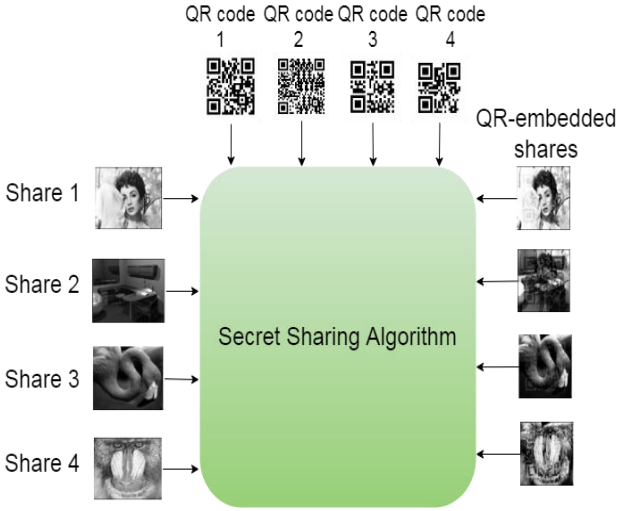

Figure-3. Sharing process of visual shares and QR code information.

Secret Sharing Algorithm

If the QR code and visual shares contain the equal dimension $a \times b$, then n pixels of each visual share and $n-1$ pixels of each QR code at the equal coordinate are encoded into $4(n+1)$ sub-pixels of n shares. The algorithm for secret sharing process is presented below.

Algorithm for Secret Sharing-based QR-embedded Share Generation

Input: n shares, n QR codes, dimension $a \times b$

Output: QR-embedded shares $QS_1, QS_2, \dots, QS_n$

Begin

i. Initialize $i = 1, j = 1$; //i, j: the row and column of QR codes/shares, respectively.

ii. $\left(\mathrm{QS_f}(2\mathrm{i}-1,2\mathrm{j}), \mathrm{QS_f}(2\mathrm{i}-1,2\mathrm{j})\right) = \left(\mathrm{Q_f}(\mathrm{i},\mathrm{j}), \mathrm{Q_f}(\mathrm{i},\mathrm{j})\right)$, where $1 \le f \le n$; //S_f: visual shares

iii. $\left(QS_n(2i, 2j-1), QS_n(2i, 2j)\right) = (0,1) or (1,0)$ randomly with the equal probability 0.5;

iv. $(\ [\![\mathrm{QS}]\!]\_\mathrm{f}(2\mathrm{i}, 2\mathrm{j}-1),\ [\![\mathrm{QS}]\!]\_\mathrm{f}(2\mathrm{i}, 2\mathrm{j})\ ) =$

$$\begin{cases} \mathrm{QS_n}(2\mathrm{i}-1,2\mathrm{j}-1), \mathrm{QS_n}(2\mathrm{i}, 2\mathrm{j}), & \mathrm{Q_f}(\mathrm{i},\mathrm{j}) = 0 \\ \mathrm{QS_n}(2\mathrm{i}, 2\mathrm{j}-1), \mathrm{QS_n}(2\mathrm{i}, 2\mathrm{j}) & \mathrm{Q_f}(\mathrm{i},\mathrm{j}) = 1' \end{cases}$$

$$1 \le f \le n$$

v. Create a random permutation matrix M_{perm}, which is utilized to permute the 4 sub-pixels in $n+1$ shares in the same order.

vi. Consider $j = j+1$, when $j \le b$, go to Step ii; or else return back to Step v.

vii. Consider $i = i+1$, when $i \le a$, go to Step ii; or else the algorithm terminates.

Once all the QR-embedded shares are created, those are encoded with the CI blocks chosen by the CSF to produce the meaningful shares. These are accumulated in

the cloud storage data server and further accessed by the users via communication medium.

Image Restoration

During this phase, the user initially accesses the different QR-embedded shares from the cloud storage. After obtaining all the shares of a particular image, user can authenticate the QR code embedded in each share to confirm whether the shares are provided by the legitimate users or not. If the QR codes in all shares are verified properly, then the user can extract the appropriate shares and decode them to restore the actual image [15] efficiently. This ensures that the decoding of the unwanted or illegitimate shares from the cloud storage for accessing and restoring original image by any user.

EXPERIMENTAL RESULTS

In this section, the efficiency of (n,n) RCA-SSVC-QR scheme is measured via testing it in MATLAB 2017b. Also, the efficiency is compared with the (k,n)-VCS-QR [16], (3,3)-threshold VSS-QR [18], (k,n)-threshold XVSS-QR [22], (n,n)-threshold SS-QR [23], (x,n) and (n,n) SVC [13], (x,n), (n,n) SSVC methods [14] and (n,n) RCA-SSVC [15]. The comparative study is conducted regarding the PSNR, Mean Squared Error (MSE), Mean Absolute Error (MAE), Universal Image Quality Index (UIQI) and Structural Similarity Index (SSIM). In this scrutiny, 4 grayscale SI of distinct types and 4 CIs of size 512×512 are selected randomly. The SI is sent to the recipient through splitting them into 4 shares, which are masked in 4 CIs.

MSE: It is the average error between the restored SI and the true SI. The lower the MSE value, the less degraded the restored SI.

$$MSE = \frac{\sum_{M,N}[SI_{m,n} - RSI_{m,n}]^2}{M \times N} \quad (1)$$

In Equation (1), M, N define the total rows and columns in the SI, $SI_{m,n}$ denotes the actual SI at m^{th} row and n^{th} column and $RSI_{m,n}$ denotes the restored SI at m^{th} row and n^{th} column.

PSNR: It is the ratio of the decoded SI to the true SI. The greater the PSNR, the greater the precision of the restored SI.

$$PSNR = 10 \log_{10} \left(\frac{SI_{max}^2}{MSE} \right) \quad (2)$$

In Equation (2), SI_{max} indicates the highest number of pixels in the SI.

MAE: It is the average deviation of the pixel range between the regenerated and the real SI.

$$MAE = \frac{\sum_{M,N}|RSI_{m,n} - SI_{m,n}|}{M \times N} \quad (3)$$

UIQI: It is calculated according to the brightness, clarity and contour.

$$UIQI(a,b) = \frac{4\mu_a \mu_b \sigma_{ab}}{(\mu_a^2 + \mu_b^2)(\sigma_a^2 + \sigma_b^2)} \quad (4)$$

In Equation (5), μ_a, μ_b are the mean ranges of real (a) and restored (b) images σ_a, σ_b are the standard variance of real and restored pictures and σ_{ab} is the covariance of both pictures.

SSIM: It is calculated according to the brightness, texture and smoothness.

$$SSIM(a,b) = \frac{(2\mu_a \mu_b + c_1)(2\sigma_{ab} + c_2)}{(\mu_a^2 + \mu_b^2 + c_1)(\sigma_a^2 + \sigma_b^2 + c_2)} \quad (5)$$

In Equation (5), c_1 and c_2 are the constants. The range of UIQI and SSIM are $[-1,1]$ where 1 represents the true and restored SI is not viable to discriminate for all pixels.

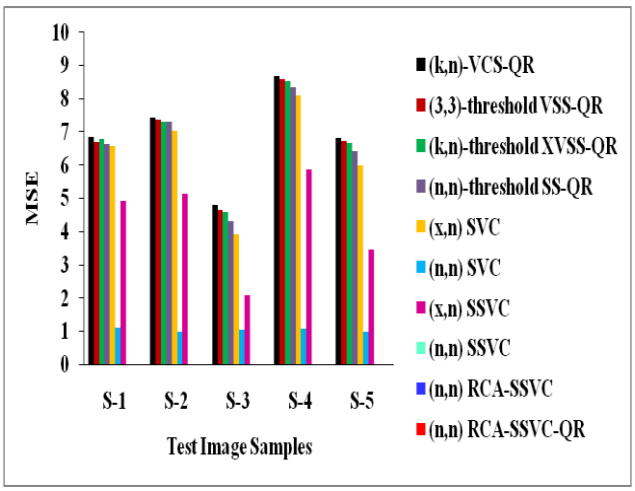

Figure-4. MSE vs. different test images.

Figure-4 portrays the MSE outcomes achieved by the different VCs with QR code schemes applied on 5 unique test samples. This analysis indicates that the (n,n) RCA-SSVC-QR scheme realizes the zero MSE than all other schemes, which signifies that the restored and actual SIs are analogous with no pixel degradation.

Similarly, Figure-5 illustrates the PSNR outcomes realized by the different VCs with QR code schemes tested on 5 samples. It observes that the (n,n) RCA-SSVC-QR scheme gives an average PSNR of about 57.34dB, which is 38.88% higher than all other schemes because of preventing pixel losses and decoding illegitimate shares for restored SI.

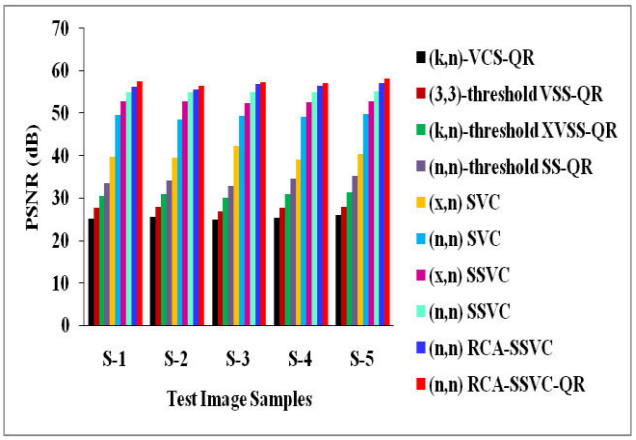

Figure-5. PSNR vs. different test images.

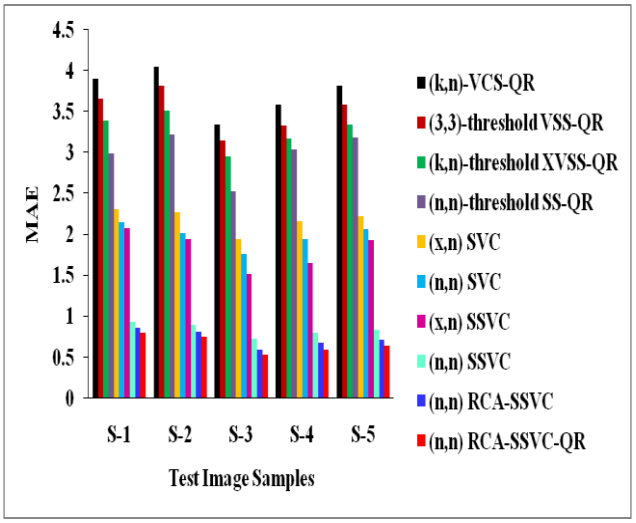

Figure-6. MAE vs. different test images.

Figure-6 demonstrates the MAE outcomes achieved by the different VCs with QR code schemes employed on 5 unique test images. It addresses that the (n,n) RCA-SSVC-QR scheme decreases the average MAE by about 66.8%, which is 71.5% less than all other schemes, which means that the presented scheme can prevent pixel errors and counterfeit shares uploaded to the cloud storage for accurate SI recovery.

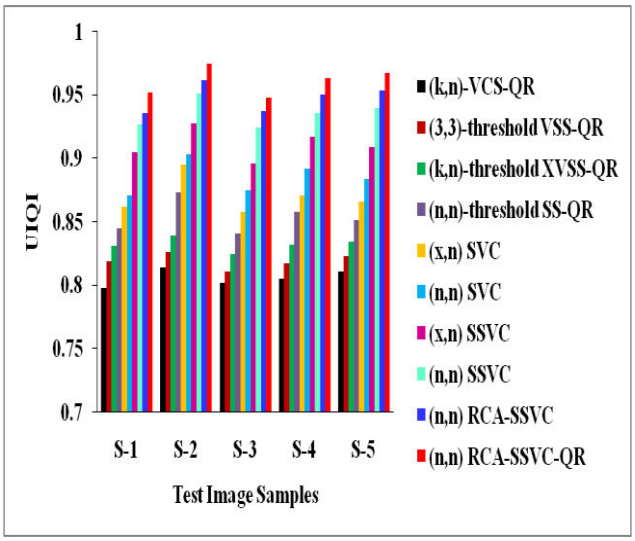

Figure 7. UIQI vs. different test images.

Figure-7 portrays the UIQI outcomes realized by the different VCs with QR code schemes tested on 5 samples. It signifies that the (n,n) RCA-SSVC-QR scheme has an average UIQI of 0.961, which is 10.03% greater than all other VC schemes. This defines that the presented scheme avoids accessing and decoding the false shares from the cloud storage for restoring actual SI.

Figure-8 depicts the SSIM achieved for the different VCs with QR code schemes tested on 5 samples. It clarifies that the (n,n) RCA-SSVC-QR scheme has an average SSIM of 0.918, which is 9.55% higher than all other VC schemes. This indicates that the presented scheme can efficiently restore the actual SI by decoding the authenticated shares from cloud storage without any pixel or information losses.

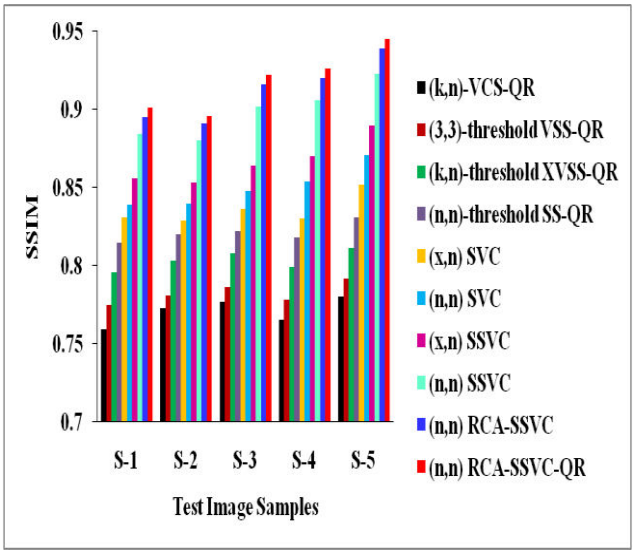

Figure-8. SSIM vs. different test images.

CONCLUSIONS

In this study, a novel 2-level data security method was presented based on QR codes and RCA-SSVC. First,

the public and private information of users was used as a QR code, which was encoded into sub-pixel blocks of all shares during the share creation phase. In addition, a random permutation was performed to the QR-embedded shares to disrupt the sub-pixels in a single block, preventing attackers from determining the position of the SQR code's pixels. During the image restoration step, the restoration process begins once the user's identity was verified by reading QR code information that matches the QR code embedded in each share. Therefore, image restoration from unauthorized shares stored in the cloud storage during access was disallowed. Finally, the experimental findings proved that the RCA-SSVC-QR has 0 mean MSE, 56.46dB mean PSNR, 0.736 mean MAE, 0.9478 mean UIQI and 0.9122 mean SSIM compared to the other VC schemes for cloud storage security.

REFERENCES

[1] Yang P., Xiong N. and Ren J. 2020. Data security and privacy protection for cloud storage: a survey. IEEE Access. 8: 131723-131740.

[2] Seth B., Dalal S., Jaglan V., Le D. N., Mohan S. and Srivastava G. 2020. Integrating encryption techniques for secure data storage in the cloud. Transactions on Emerging Telecommunications Technologies .1-24.

[3] Sarosh P., Parah S. A., Bhat G. M., Heidari A. A. and Muhammad K. 2021. Secret sharing-based personal health records management for the internet of health things. Sustainable Cities and Society. 74: 103129.

[4] Pandey D., George S., Aremu B., WariyaS.and Pandey B. K. 2021. Critical review on integration of encryption, steganography, IOT and artificial intelligence for the secure transmission of stego images. Scientific Research Journal of Engineering and Computer Science. 1(1): 33-36.

[5] Brindha K. and Jeyanthi N. 2015. Secured document sharing using visual cryptography in cloud data storage. Cybernetics and Information Technologies. 15(4): 111-123.

[6] Adee R. and Mouratidis H. 2022. A dynamic four-step data security model for data in cloud computing based on cryptography and steganography. Sensors. 22(3): 1-23.

[7] Ibrahim D. R., Teh J. S.and Abdullah R. 2021. An overview of visual cryptography techniques. Multimedia Tools and Applications. 80(21): 31927-31952.

[8] Mohan J. and Rajesh R. 2021. Enhancing home security through visual cryptography. Microprocessors and Microsystems.80: 1-30.

[9] Jisha T. E. and Monoth T. 2020. Recent research advances in black and white visual cryptography schemes. Soft Computing for Problem Solving. 479-492.

[10] Gurunathan K. and Rajagopalan, S. P. 2020. A stegano-visual cryptography technique for multimedia security. Multimedia Tools and Applications. 79(5): 3893-3911.

[11] Salim M. Z., Abboud A. J. and Yildirim R. 2022. A visual cryptography-based watermarking approach for the detection and localization of image forgery. Electronics. 11(1): 1-22.

[12] Wu X., Yao P. and An N. 2021. Extended XOR-based visual cryptography schemes by integer linear program. Signal Processing. 186: 1-14.

[13] Mary G. S. and Kumar S. M. 2020. Secure grayscale image communication using significant visual cryptography scheme in real time applications. Multimedia Tools and Applications. 79(15): 10363-10382.

[14] Hemalatha R. and Selvi S. 2021. Improving security of visual cryptography by contrast sensitivity function. Vidyabharati International Interdisciplinary Research Journal, Special Issue on Recent Research Trends in Management, Science and Technology. 1322-1330.

[15] Hemalatha R. and Selvi S. 2022. Robust collusion avoidance-secure signific VC scheme. International Journal of Intelligence Engineering & Systems. 15(4): 565-574.

[16] Fu Z., Cheng Y. and Yu B. 2018. Visual cryptography scheme with meaningful shares based on QR codes. IEEE Access. 6: 59567-59574.

[17] Bakshi A. and Patel A. K. 2019. Secure telemedicine using RONI halftoned visual cryptography without pixel expansion. Journal of Information Security and Applications. 46: 281-295.

[18] Liu T., Yan B. and Pan J. S. 2019. Color visual secret sharing for QR code with perfect module reconstruction. Applied Sciences. 9(21): 1-20.

[19] Zhu Y., Xu W. and Shi Y. 2019. High-capacity encryption system based on single-shot-ptychography encoding and QR code. Optics Communications.435: 426-432.

[20] Xiong L., Zhong X. and Yang C. N. 2020. DWT-SISA: a secure and effective discrete wavelet transform-based secret image sharing with authentication. Signal Processing. 173: 1-23.

[21] Wan S., Qi L., Yang G., Lu Y., Yan X. and Li L. 2020. Visual secret sharing scheme with (n, n) threshold for selective secret content based on QR codes. Multimedia Tools and Applications. 793. 2789-2811.

[22] Tan L., Lu Y., Yan X., Liu L. and Zhou X. 2020. XOR-ed visual secret sharing scheme with robust and meaningful shadows based on QR codes. Multimedia Tools and Applications. 79(9): 5719-5741.

[23] Huang P. C., Chang C. C., Li Y. H. and Liu Y. 2021. Enhanced (n, n)-threshold QR code secret sharing scheme based on error correction mechanism. Journal of Information Security and Applications. 58: 1-9.

[24] Chow Y. W., Susilo W., Wang J., Buckland R., Baek J., Kim J. and Li N. 2021. Utilizing QR codes to verify the visual fidelity of image datasets for machine learning. Journal of Network and Computer Applications. 173: 1-11.

[25] Pan J. S., Liu T., Yang H. M., Yan B., Chu S. C., and Zhu, T. 2022. Visual cryptography scheme for secret color images with color QR codes. Journal of Visual Communication and Image Representation. 82: 1-8.