Received: May 6, 2022. Revised: June 14, 2022.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Robust Collusion Avoidance-Secure Signific VC Scheme

Hemalatha Rangaswamy[1]* **Selvi Sellappan[1]**

[1]*Department of Computer Science, PSG College of Arts & Science, Coimbatore, India*
* Corresponding author's Email: latharajiphd123@gmail.com

Abstract: Visual Cryptography (VC) was developed to encrypt images into numerous shares and decrypt them by grouping the shares without the need for expensive traditional cryptosystems. The Secure Signific VC (SSVC) scheme was intended to use a Contrast Sensitive Function (CSF) for deciding on Cover Image (CI) blocks to be embedded with the secret shares. However, this scheme was prone to collusion attacks and distortions in the images. To solve this, randomness and collusion avoidance are essential for SSVC to be valuable. Hence, this article proposes a new Robust Collusion Avoidance-based SSVC (RCA-SSVC) scheme to create the collusion-resistant Secret Image (SI) shares effectively and avoid the risk of collusion. This scheme is designed in a manner such that each share is dependent on every other image or at least most of the images. This characteristic ensures that data is distributed uniformly across users and protects against collusion threats. During the share creation stage, a Boolean XOR function and a shift-bit algorithm are introduced to create multiple shares from SIs. This algorithm creates the shares only if the prior shares had been previously created. These created shares are embedded with the CI blocks chosen by CSF and sent to the individuals via a transfer channel. Further, the actual SI is retrieved from the received shares during the restoration stage. Finally, the results of the experiments show that the RCA-SSVC achieves an average Mean Square Error (MSE) of 0, mean Peak Signal-to-Noise Ratio (PSNR) of 56.48dB, average Mean Absolute Error (MAE) of 0.736, mean Universal Image Quality Index (UIQI) of 0.9478, mean Structural Similarity Index (SSIM) of 0.9122 and 0.9sec time complexity compared to the traditional VC schemes.

Keywords: VC, SSVC, Multiple secret sharing, Collusion avoidance, XOR function, Shift-bit algorithm.

1. Introduction

Cloud computing is a technological advancement that makes it possible for many enterprises, banks, health practitioners, and government organizations to gather, analyze, and implement database-driven applications. However, cloud storage protection is difficult since there are several problems and inconsistencies. The most common data breaches are database retrieval stability, server operation defense, and metadata access control [1, 2]. Data providers are concerned about the security and validity of their data. Crypto technologies are used to assure confidentiality during collection and distribution. They are capable of encoding the original message into a stream cipher and decoding it to get the actual message [3, 4].

Indeed, such technologies need a great amount of estimation as well as crucial administrative procedures. They also need a clear idea of cryptosystems. VC is a type of encryption used to hide image data that will be decrypted by the client using the associated key image [5]. The method employs two types of images: one with randomized pixels and the other with sensitive data. The hidden image is divided into two or more tiny, asymmetrical segments, omitting the encryption keys. Only by combining the shares can the hidden secret key be revealed [6]. This simplifies VC if we are unfamiliar with cryptography and complex analysis. In cryptography, VC is a shared secret. It helps individuals to conceal secrets in various shares that do not define secrecy until they are placed collectively. VC is primarily suited for high-sensitivity applications like biological authentication,

remote monitoring, steganography, and digital wallets [7-9].

The use of VC has several advantages, including a key-free cryptosystem, processability, no deciphering, lower estimate costs, and distribution via FAX or email. In recent years, several studies have employed different VC techniques for a variety of objectives [10-12].

Mary and Kumar [13] created a novel Error Abatement Technique (EAT) to achieve substantial shares among several VC techniques. It employs value discretization and low-error filtration methods. The value discretization filter separates the pixel coefficients from the grayscale SI and calculates the adjacent pixel loss, which may then be regularised to produce meaningful shares. In addition, reduced error filtration was used to reduce generated mistakes and get nearer to relevant shares. In addition, the SVC technique, which includes share creation and reconstruction phases, was created. However, this LSB embedding and mining was subject to steganography and was not at all secured. Its resilience was also reduced because it can be easily deciphered by extracting the picture's LSBs and retrieving the contents in a binary sequence. If the embedding information contained more than one LSB, the photo quality may suffer depending on how many pixels were altered.

As a result, the SSVC scheme [14] was developed which substitutes the CSF for the LSB embedding and mining operations in the SVC approach. The SI was converted into the SSI and shares were produced during the share creation stage. The CSF then decided to select the blocks of the CI and the produced secret share values were randomly embedded with the selected blocks of CIs. As a result, semantic and meaningful shares were generated. These integrated CI blocks were referred to as shares. The generated shares were then transmitted to the user through the transmission channel. In the reconstruction stage, a key share was produced from the received shares to rebuild the SI.

But, the major concern is that this approach was vulnerable to collusion attacks i.e., one of the SIs was uncovered by collusion. These outcomes may be acquired when two shares collude. As a result, in this approach, neither the created shares are random nor collusion resistant. Another problem is that its robustness to external noise is not high. Accordingly, randomness and collusion resistance are required for SSVC to be successful. Therefore, in this paper, a new Robust Collusion Avoidance-based SSVC (RCA-SSVC) scheme is proposed which offers the collusion resistant image shares in such a way that each share is dependent on every other image or at least most of the images. This property maintains uniformity when distributing data between users and defends against collusion attacks. In this scheme, Boolean XOR functionality is employed during the share creation phase to create the shares from SIs. Also, the shift-bit algorithm is used to replace the initial 4 bits of each pixel with the final 4 bits of that pixel. This algorithm creates the shares only if the prior shares had been previously created. This new RCA-SSVC takes less time and minimizes the chance of collusion.

The residual portions of this paper are prepared as the following: Section 2 reviews the studies and other work related to the VC methods. Section 3 explains the proposed methodology and Section 4 illustrates its experimental results. Section 5 concludes the entire work.

2. Literature survey

An optimized confidential VC [15] was adopted for brain MRI images. Initially, the images were divided into blocks using the discrete wavelet transform. The Gaussian-based cuckoo search algorithm was applied to decide the best position for all blocks. Also, the dual shares were produced from the hidden image. After that, the hidden shares were embedded into the related positions of the blocks. Finally, the real image was reproduced on the recipient side.

The sharing map and pooling method was discussed [16] to recreate the shares using the confidential image sharing method. The confidential image and halftone binary CIs were used to generate relevant grayscale shares using the sharing map. Also, the filtration was added for appropriate shared values, which produces the most significant bit of pixel in all shares equal to a bit in the corresponding binary cover.

A novel robust image watermarking technique was developed [17] depending on block categorization and VC. First, the actual image was decomposed into non-overlapping blocks. After, canny edge detection and Support Vector Machine (SVM) classification were applied to organize these blocks into smooth and non-smooth labels. The VC scheme was applied to produce a master share based on the block categorization and an owner share by the master share with a binary watermark. Then, the watermark was retrieved via stacking the master share and the owner share to authenticate the ownership of the image.

A dimension-invariant VC approach was developed [18] for grayscale images underpinned by the Efficient Direct Binary Search (EDBS)

algorithm wherein the multi-pixel encryption VC sharing was integrated into the EDBS halftone task. By using local optimizations and global iterations, the optimum restored image was acquired. Moreover, the image data was mined probabilistically by the inverse mapping in the codebook to improve the restored image quality.

An enhanced High-quality and Printer-friendly (HP)-based VC approach was developed [19] that recovers confidential photos with better quality and removes pixel expansion. An image block was enciphered to remove pixel expansion. A higher quality was achieved via highly analyzing the association between the confidential and share blocks.

A Probabilistic VC (PVC) approach designed [20] for threshold access frameworks depending on the Deterministic VC (DVC) and categorize the probabilistic methods into online and offline concerns the reference mode of sharing column vectors. A Modified Leading Diagonal Sorting with Probabilistic VC (MLDS-PVC) was developed [21] to encode the clinical images with share images and upload them to the cloud server for restoration.

A copyright defence technique depending on Curvelet Transform and Extensive VC (CT-EVC) was developed [22] for color images. In this technique, the Curvelet inter-level coefficients were utilized to generate a master share and watermark which helps to generate the ownership share based on the codebook. Also, the copyright was proven by retrieving the watermark by XOR-superimposition of master and ownership shares. Moreover, the relevant shares were generated by Baker's map to scramble the watermark and the host image.

2.1 Problem definition

From the literature survey, the problems in the VC methods are summarized as:

- Some of the methods have a high computational difficulty due to the more operations and were not appropriate for more images.
- A portion of the data about actual confidential images may vanish in the restored image because of the intensity change.
- The security of image recovery was not efficient due to the encoding of diagonal elements, which may be easily decoded by the attackers.
- If the image shares rely on multiple owners, then the computation burden was very high.
- Most methods were prone to different attacks, due to the less uncertainty (randomness) in the shares stored in the cloud.

2.2 Research contribution

The SSVC based on CSF and LSB embedding schemes was susceptible to collusion attacks. Also, its robustness was not effective while external noise exist. To combat these challenges, randomness and collusion resistance are necessary for the SSVC system.

From this perspective, the major contributions of this research are:

- Boolean XOR function is applied during the share generation to produce multiple shares from SIs.
- Shift-bit algorithm is used for substituting the primary 4 bits of all pixels with the last 4 bits of that pixel.
- So, the shares are generated only when the prior shares have been early generated and thus the chance of collusion is prevented.

3. Proposed methodology

In this section, the RCA-SSVC scheme is explained briefly. This scheme has 2 major phases: share creation and recovery phases. Compared to the SSVC, it encourages (n, n) VC where n is the amount of shares produced, to solve the problem of robustness against collusion risks. It encrypts N number of SIs to create N number of random shares.

The framework of RCA-SSVC is portrayed in Fig. 1. Also, Table 1 lists the notations used in this study.

3.1 Share creation phase

During this phase, the SI is converted to the Signific SI (SSI) with the help of value discretization and reduced error filtration methods to produce the shares. In this RCA-SSVC scheme, n number of $\{SI_{i,j}^1, SI_{i,j}^2, \dots, SI_{i,j}^n\}$ are encoded in a manner to create n random share images $\{S_{i,j}^1, S_{i,j}^2, \dots, S_{i,j}^n\}$. This scheme is utilized for any number of SIs without exposing data in separate shares. As shown in Algorithm 1, to create l^{th} share, XOR function is applied for primary $l-1$shares and accumulated in z. For each iteration, z is initialized with a range 0. Also, z is modified by executing XOR function with the $l+1^{th}, l+2^{th}$, real images $\{SI_{i,j}^{l+1}, SI_{i,j}^{l+2}, \dots, SI_{i,j}^n\}$. After that, shift-bit algorithm on z is executed in which the initial 4 bits

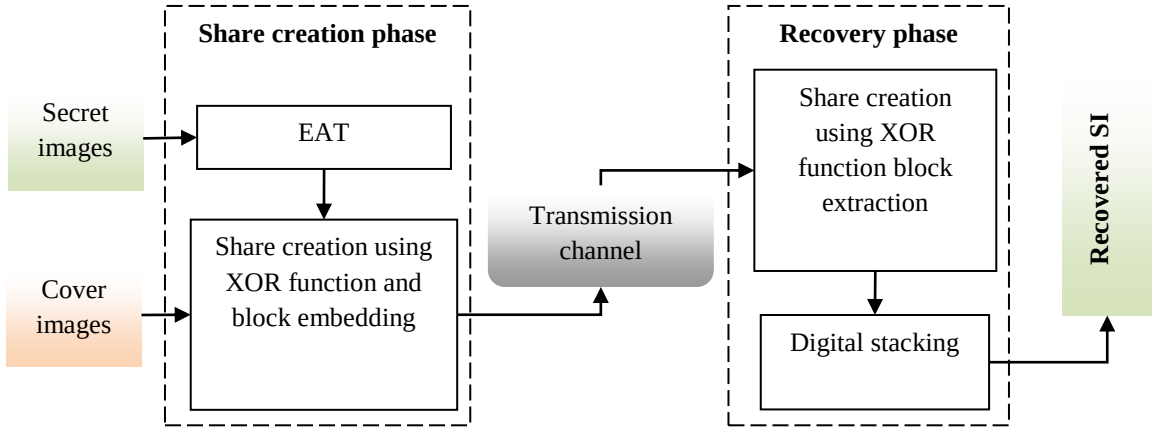

Figure. 1 Framework of RCA-SSVC scheme

Table 1. Lists of notations

Notations	Description
n	Amount of shares produced
$SI_{i,j}^{n}$	Number of secret images
$S_{i,j}^{n}$	Number of share images
$\oplus$	XOR operator
G	Grayscale image
G'	Bits replaced image
M	Total rows in the secret image
N	Total columns in the secret image
$SI_{m,n}$	Secret image at m^{th} row and n^{th} column
$RSI_{m,n}$	Recovered secret image at m^{th} row and n^{th} column
SI_{max}	Maximum number of pixels in the secret image
μ_a	Mean value of real secret image
μ_b	Mean value of recovered secret image
σ_a	Standard deviation of real image
σ_b	Standard deviation of recovered secret image
σ_{ab}	Covariance of real and recovered secret images
c_1, c_2	Constants

of all pixels are replaced with the final 4 bits of that pixel. Then, XOR is applied on the output with $SI_{i,j}^{l}$ to create the ultimate $S_{i,j}^{l}$. It is noticed that $S_{i,j}^{l}$ is created only if the prior shares $S_{i,j}^{1}, S_{i,j}^{2}, \dots, S_{i,j}^{l-1}$ had been previously created. The processes in share creation phase are illustrated in Fig. 2.

Algorithm 1: *Share Creation (Encoding)*

Input: Secret image, $SI_{i,j} = \{SI_{i,j}^{1}, SI_{i,j}^{2}, \dots, SI_{i,j}^{n}\}$

$\boldsymbol{for}(l \in \{1, \dots, n\})$
  $z \leftarrow 0$;
  $\boldsymbol{for}(m \in \{1, \dots, l-1\})$
    $z \leftarrow z \oplus S_{i,j}^{m}$;
    $\boldsymbol{for}(m \in \{l+1, l+2, \dots, n\})$
      $z \leftarrow z \oplus SI_{i,j}^{m}$;
  $S_{i,j}^{l} \leftarrow SI_{i,j}^{l} \oplus Shift\ bit(z)$;
  $\boldsymbol{end\ for}$
 $\boldsymbol{end\ for}$
$\boldsymbol{end\ for}$

Return $S_{i,j}$

Output: Shares, $S_{i,j} = \{S_{i,j}^{1}, S_{i,j}^{2}, \dots, S_{i,j}^{n}\}$

Algorithm 1 presented in a manner such that all shares are dependent on each other image or at least most of the images. This characteristic preserves uniformity when distributing data between users and avoiding collusion risks.

After creating the final shares, those are embedded with the CI blocks decided by the CSF to produce the meaningful shares. These are conveyed to the clients through transfer channels.

3.2 Recovery phase

The reconstruction process comprises level-by-level functionalities executed on the share images for extracting the entire encoded data of SIs present in shares. Fig. 3 illustrates the processes in the recovery phase.

In this process, the CI blocks and random shares are mined by the CSF from the accepted shares at the recipient side. Then, extracted n shares are provided as input and n restored images are created as output. Each n share image is essential to efficiently reconstruct each n SIs. The decoding process is akin to the encoding process. It iteratively grows and restores $SI_{i,j}^{n}, SI_{i,j}^{n-1}, \dots, SI_{i,j}^{1}$, correspondingly. For instance, to decide l^{th} SI, the process is described in Algorithm 2 as:

1. First, XOR of the primary l created shares is considered and accumulated in z.
2. Then, XOR for the real images that have been effectively restored, i.e., from $l+1, l+2, \dots, n$ and z is executed.

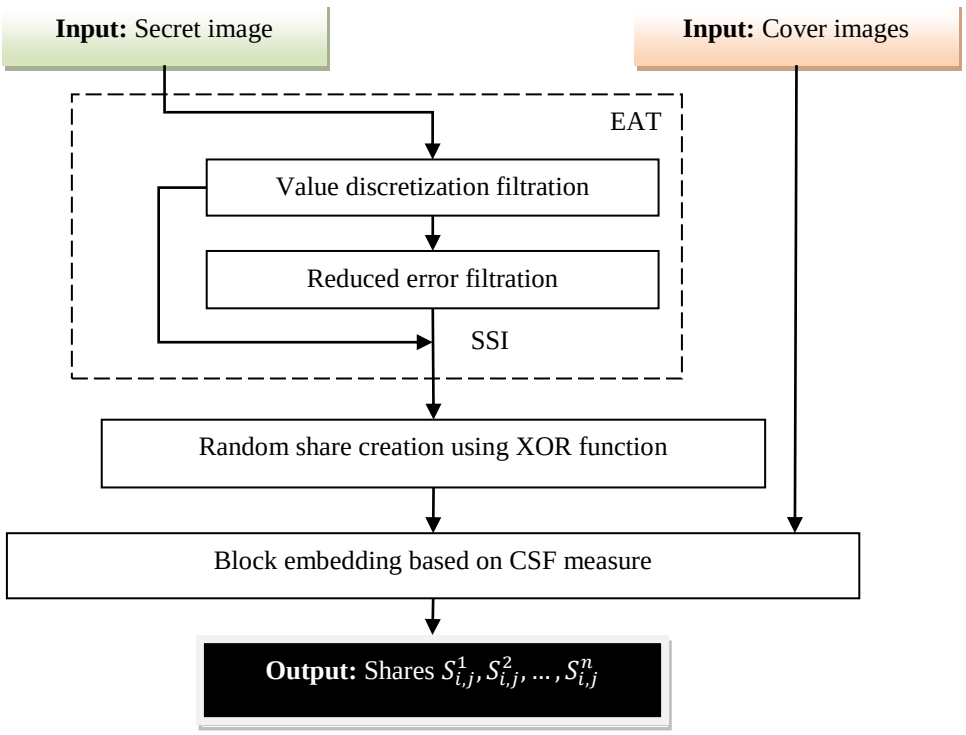

Figure. 2 Share creation

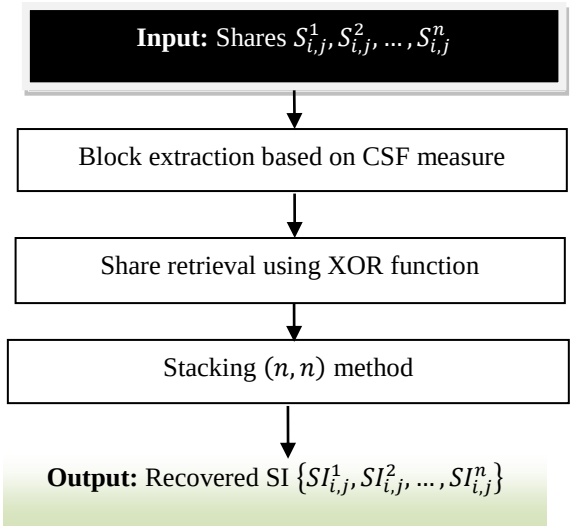

Figure. 3 Secret image recovery phase

3. After, the shift bits algorithm on z (as described in Algorithm 3) is employed to replace the initial half of the bits with another of all pixels in the image.
4. The XOR of $S_{i,j}^l$ and outcome of the earlier step is considered and accumulated in $SI_{i,j}^l$. This is the l^{th} SI.

In this process, each other real images are restored and $SI_{i,j}^n, SI_{i,j}^{n-1}, \dots, SI_{i,j}^1$ are created. It observes that $SI_{i,j}^1$ is created only if $SI_{i,j}^2$ has been created. Likewise, each image excluding the final is dependent on the earlier restored images and so entirely minimizing the chance of collusion.

Algorithm 2: Restoration Phase (Decoding)
Input: Shares, $S_{i,j} = \{S_{i,j}^1, S_{i,j}^2, \dots, S_{i,j}^n\}$
$\boldsymbol{for}(l \in \{n, n-1, \dots, 1\})$
  $z \leftarrow 0$;
  $\boldsymbol{for}(m \in \{1, 2, \dots, l-1\})$
    $z \leftarrow z \oplus S_{i,j}^m$;
    $\boldsymbol{for}(m \in \{l+1, l+2, \dots, n\})$
      $z \leftarrow z \oplus SI_{i,j}^m$;
      $SI_{i,j}^l \leftarrow S_{i,j}^l \oplus Shift\ bit(z)$;
    $\boldsymbol{end\ for}$
  $\boldsymbol{end\ for}$
$\boldsymbol{end\ for}$
Return $SI_{i,j}$
Output: $SI_{i,j} = \{SI_{i,j}^1, SI_{i,j}^2, \dots, SI_{i,j}^n\}$

Algorithm 3: Shift-Bits Algorithm
Input: Grayscale image (G)
$\boldsymbol{for}(i \in \{0, 1, \dots, image\_width\})$
  $\boldsymbol{for}(j \in \{0, 1, \dots, image\_height\})$
    $p \leftarrow z[i][j] \ll 4$; //Bit-shift operator
    $q \leftarrow z[i][j] \gg 4$; //Bit-shift operator
    $z[i][j] = p \| q$; //Bit-wise OR operator
  $\boldsymbol{end\ for}$
$z' = z$;
$\boldsymbol{end\ for}$
Return z'
Output: Replaced bits image (G')

Thus, this RCA-SSVC scheme can prevent the probability of collusion absolutely and increase the robustness against collusion attacks.

4. Experimental results

The efficiency of (n,n) RCA-SSVC scheme is evaluated by executing it in MATLAB 2017b. Also, the efficiency is evaluated with the PVC [20], MLDA-PVC [21], CT-EVC [22], (x,n) and (n,n) SVC [13], (x,n) and (n,n) SSVC methods [14]. The comparative study is carried out based on the MAE, PSNR, UIQI, MSE, SSIM, time complexity and computation cost. In this scrutiny, 4 grayscale SI of different varieties and 4 CIs of size 512×512 are decided at random. The SI is forwarded to the receiver by dividing them into 4 shares, which are concealed in 4 CIs. Fig. 4 portrays considered actual SIs, the conversion of such SIs into SSI and the shares created by CIs.

- **MSE:** It is the mean error of the recovered SI to the real SI. The lower the MSE value, the smaller the degradation in the recovered SI.

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

In Eq. (1), M,N are the overall rows and columns in the SI, $SI_{m,n}$ is the real SI at m^{th} row and n^{th} column and $RSI_{m,n}$ is the recovered SI at m^{th} row and n^{th} column.

- **PSNR:** It is the proportion of the real SI to the deciphered SI. The larger the PSNR, the more precise the recovered SI.

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

In Eq. (2), SI_{max} is the maximum number of pixels in the SI.

- **MAE:** It is a mean variance of pixel range from the restored to the actual SI.

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

- **UIQI:** It is determined by 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 Eq. (4), μ_a,μ_b are the mean ranges of real (a) and recovered (b) images, σ_a,σ_b are the standard deviation of real and recovered images and σ_{ab} is the covariance of both images.

- **SSIM:** It is determined by 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 Eq. (5), c_1 and c_2 are the constants. The value of UIQI and SSIM are $[-1,1]$ where 1 indicates the real and recovered SI is impossible to differentiate for each pixel.

- Time complexity: It is the time taken to execute the VC schemes to recover the SIs.
- Computation cost: It is the computation complexity of encoding (share creation) and decoding (recovery) processes. The computation cost of the (n,n) RCA-SSVC scheme is $O(n\log_2 n)$, where n is the number of shares.

Fig. 5 illustrates the MSE values attained by various VC schemes using 5 distinct test images. This scrutiny addresses that the (n,n) RCA-SSVC achieves a zero MSE compared to the other VC schemes, which defines that the recovered SI and the real SI are comparable without any pixel losses.

Fig. 6 shows the PSNR values attained by various VC schemes using 5 distinct test images. It analyze s that the (n,n) RCA-SSVC scheme results in a mean PSNR about 56.46dB, which is greater than the other VC schemes due to the minimization of pixel errors in the recovered SI significantly.

Fig. 7 shows the MAE of proposed and existing VC schemes using 5 distinct test images. It observes that the (n,n) RCA-SSVC scheme minimizes the mean MAE by approximately 69% compared to the other VC schemes, which defines that this scheme can diminish the pixel losses in the recovered SI to obtain the real SI.

Fig. 8 portrays the UIQI of the proposed and existing VC schemes using 5 distinct test images. This analysis signifies that the (n,n) RCA-SSVC scheme accomplishes 0.9478 mean UIQI, which is 8.64% greater than all other traditional VC schemes and defines that the real and recovered SI are indistinguishable.

Fig. 9 portrays the SSIM of the proposed and existing VC schemes using 5 distinct test images. This analysis signifies that the (n,n) RCA-SSVC scheme accomplishes 0.9122 mean SSIM, which is 8.99% greater than all other classical VC schemes and defines that the actual and restored SI are identical.

Fig. 10 shows the time complexity (execution time in seconds) of the proposed and existing VC

schemes applied to the five distinct test images. This analysis signifies that the (n, n) RCA-SSVC scheme accomplishes 0.9 sec execution time which is 72% less than all other classical VC schemes. It addresses that the (n, n) RCA-SSVC scheme can reconstruct the SI timely and accurately.

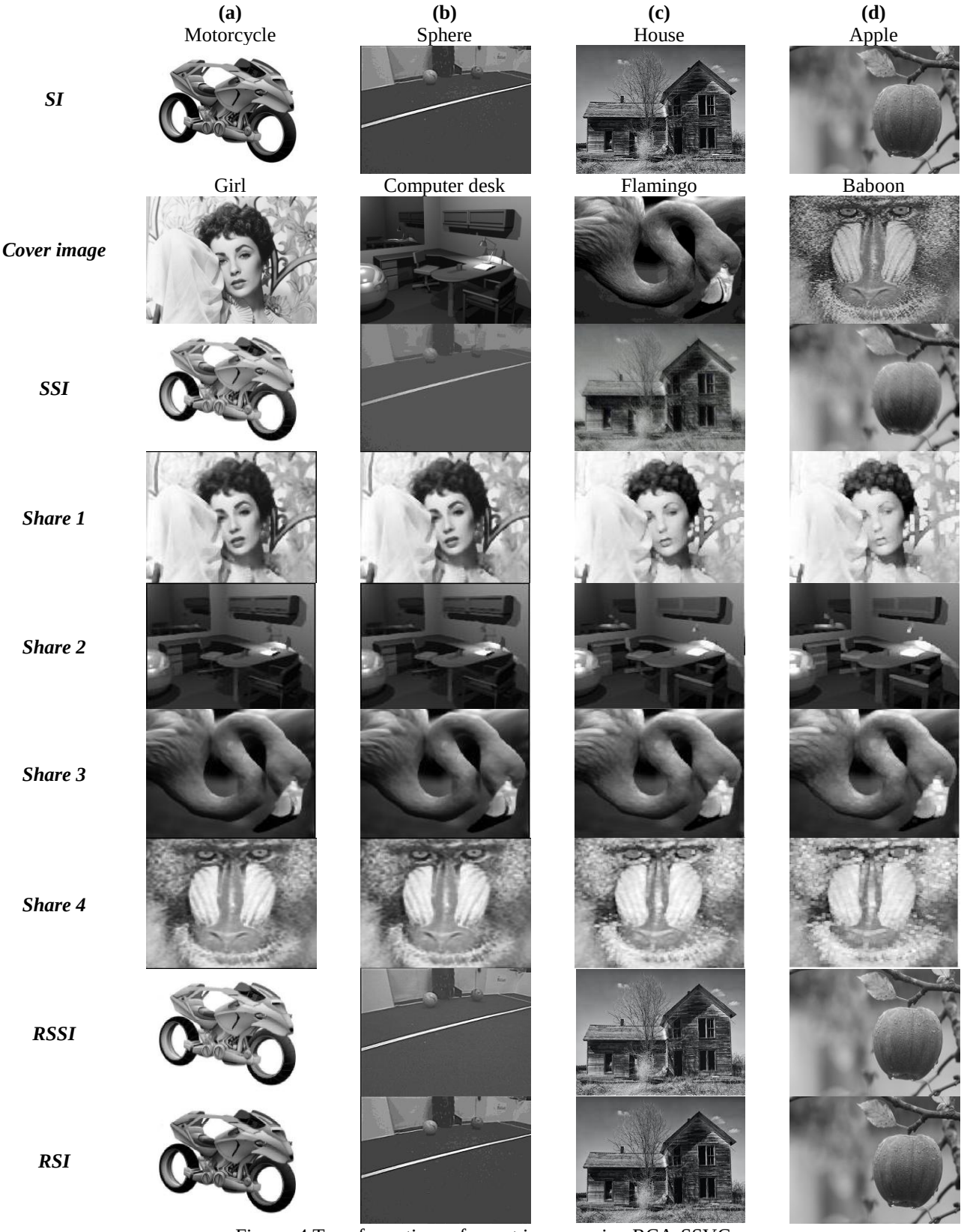

Figure. 4 Transformations of secret images using RCA-SSVC

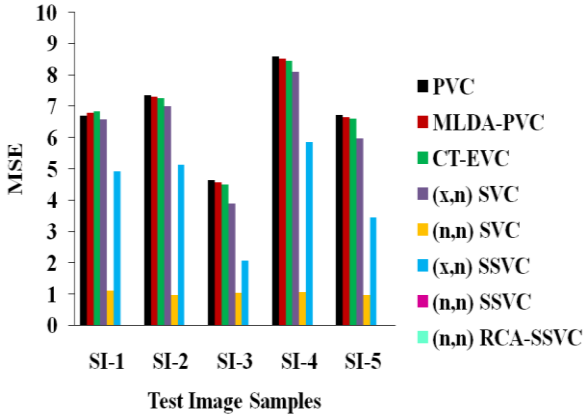

Figure. 5 Evaluation of MSE for proposed and existing VC schemes

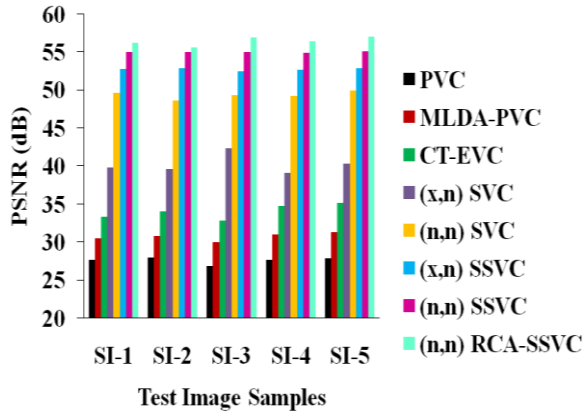

Figure. 6 Evaluation of PSNR for proposed and existing VC schemes

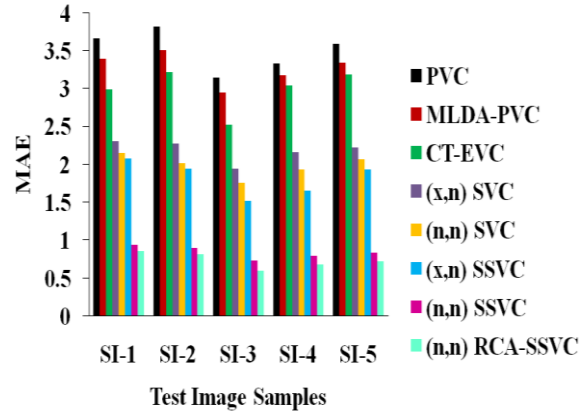

Figure. 7 Evaluation of MAE for proposed and existing VC schemes

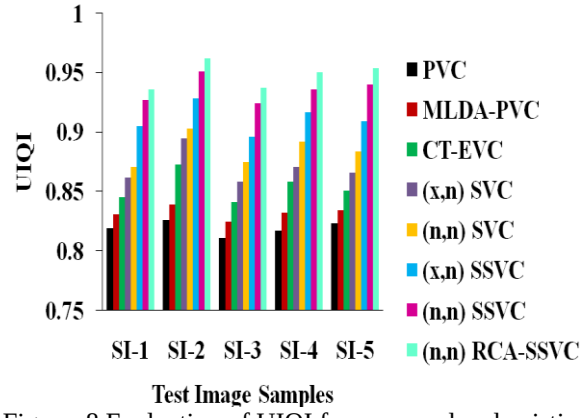

Figure. 8 Evaluation of UIQI for proposed and existing VC schemes

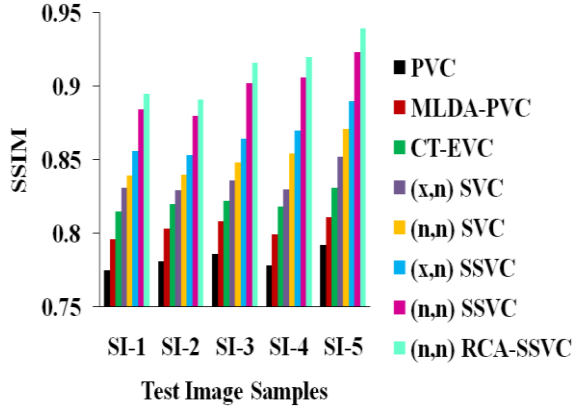

Figure. 9 Evaluation of SSIM for proposed and existing VC schemes

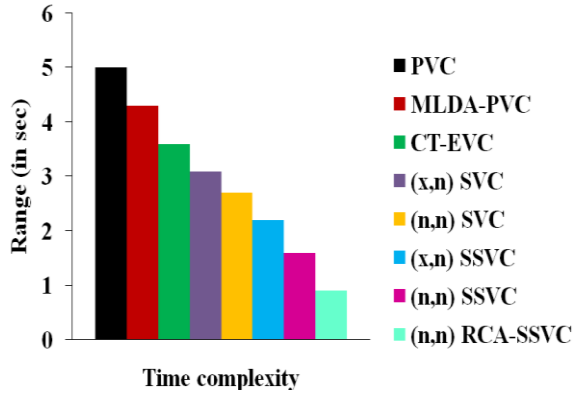

Figure. 10 Evaluation of time complexity for proposed and existing VC schemes

4.1 Security analysis

From the image quality assessment in Fig. 6, the (n,n) RCA-SSVC scheme achieves a high PSNR, MSE, MAE, UIQI and SSIM compared to the other VC schemes. It defines when one of the shares is substituted with a random image or noisy image, one of the SIs remains unchanged. That is, it can be reconstructed without using one share at all, which is represented as greater risk for security breach in the form of collision. The PSNR values with respect to the (n,n) RCA-SSVC scheme are nearly the same in real life. It reveals that the noise is disturbing each share, which must be the scenario when the actual case is of (n,n) RCA-SSVC scheme. But, values of this presented scheme are greater, portraying higher reconstruction quality under the presence of noise in any one of the shares than other schemes. This inference is also verified by the UIQI and SSIM values shown in Fig. 8 and 9, respectively. It is addressed that the when PSNR

values are identical for the presented scheme; but in SSIM and UIQI values, the image quality variance is high. Presence of noise severely affects the image reconstruction quality in existing schemes. So, the presence of noise in the share images, the presented scheme provides better outcomes compared to the other schemes with respect to the security constraints for RCA-SSVC schemes.

5. Conclusion

In this paper, a new RCA-SSVC scheme was presented to produce the collusion-resistant SI shares which were dependent on all other images. It was clear that the image data was distributed homogeneously across clients and the collusion risks were prevented. During the share creation phase, a Boolean XOR function and a shift-bit algorithm were applied to produce many shares from SIs. It produced the shares as long as the prior shares had been formerly generated. Once all the shares were embedded with the CI blocks decided by CSF and transmitted to the clients with the help of transfer channel. Moreover, the real SI was recovered from the received shares during the recovery phase. At last, the testing findings proved that the RCA-SSVC scheme has zero mean MSE, 56.46dB mean PSNR, 0.736 mean MAE, 0.9478 mean UIQI and 0.9122 mean SSIM compared to the traditional VC schemes. In future, the secure recovery of the images will be considered by preventing the fake or illegitimate shares stored in the cloud storage.

Conflicts of interest

All authors declare that they have no conflict of interest.

Author Contributions

Conceptualization, Selvi Sellappan; Methodology, Hemlatha Rangaswamy; Software, Simulation, Hemlatha Rangaswamy; Writing-Original draft preparation, Hemlatha Rangaswamy; Visualization, Investigation, Supervision, Selvi Sellappan; Reviewing and Editing, Selvi Sellappan.

References

[1] R. Wang, "Research on data security technology based on cloud storage", *Procedia Engineering*, Vol. 174, pp. 1340-1355, 2017.

[2] P. R. Kumar, P. H. Raj, and P. Jelciana, "Exploring data security issues and solutions in cloud computing", *Procedia Computer Science*, Vol. 125, pp. 691-697, 2018.

[3] S. Fatima and S. Ahmad, "Secure and effective key management using secret sharing schemes in cloud computing", *International Journal of e-Collaboration*, Vol. 16, pp. 1-15, 2020.

[4] M. S. Taha, M. S. Rahi, S. A. Lafta, M. M. Hashim, and H. M. Alzuabidi, "Combination of steganography and cryptography: a short survey", In: *Proc. of IOP Conf. Series: Materials Science and Engineering*, Vol. 518, pp. 1-13, 2019.

[5] K. Brindha and N. Jeyanthi, "Secured document sharing using visual cryptography in cloud data storage", *Cybernetics and Information Technologies*, Vol. 15, pp. 111-123, 2015.

[6] P. V. Lahande and P. R. Kaveri, "Increasing data secrecy in cloud by implementing image cryptography", *International Journal of Scientific and Technology Research*, Vol. 9, pp. 26-31, 2020.

[7] F. Liu and W. Yan, "Various applications of visual cryptography", *Visual Cryptography for Image Processing and Security*, pp. 149-164, 2015.

[8] A. Pandey and S. Som, "Applications and usage of visual cryptography: a review", In: *Proc. of IEEE 5th International Conf. on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)*, pp. 375-381, 2016.

[9] R. I. A. Khalid, R. A. A. Dallah, A. M. A. Anani, R. M. Barham, and S. I. Hajir, "A secure visual cryptography scheme using private key with invariant share sizes", *Journal of Software Engineering and Applications*, Vol. 10, pp. 1-10, 2017.

[10] B. Shrivas and S. Yadav, "A survey on visual cryptography techniques and their applications", *International Journal of Computer Science and Information Technologies*, Vol. 6, pp. 1076-1079, 2015.

[11] R. Bhatnaga and M. Kuma, "Visual cryptography: a literature survey", In: *Proc. of IEEE Second International Conf. on Electronics, Communication and Aerospace Technology*, pp. 78-83, 2018.

[12] P. Li, L. Yin, and J. Ma, "Visual cryptography scheme with essential participants", *Mathematics*, Vol. 8, pp. 1-19, 2020.

[13] G. S. Mary and S. M. Kumar, "Secure grayscale image communication using significant visual cryptography scheme in real time applications", *Multimedia Tools and Applications*, Vol. 79, pp. 10363-10382, 2020.

[14] R. Hemalatha and S. Selvi, "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*, pp. 1322-1330, 2021.

[15] A. A. S. Begum and S. Nirmala, "Secure visual cryptography for medical image using modified cuckoo search", *Multimedia Tools and Applications*, Vol. 77, pp. 27041-27060, 2018.

[16] L. Liu, Y. Lu, and X. Yan, "Polynomial-based extended secret image sharing scheme with reversible and unexpanded covers", *Multimedia Tools and Applications*, Vol. 78, pp. 1265-1287, 2019.

[17] A. Fatahbeygi and F. A. Tab, "A highly robust and secure image watermarking based on classification and visual cryptography", *Journal of Information Security and Applications*, Vol. 45, pp. 71-78, 2019.

[18] R. Sun, Z. Fu, and B. Yu, "Size-invariant visual cryptography with improved perceptual quality for grayscale image", *IEEE Access*, Vol. 8, pp. 163394-163404, 2020.

[19] D. H. Zhang, H. B. Zhu, S. L. Liu, and W. Xu, "HP-VCS: a high-quality and printer-friendly visual cryptography scheme", *Journal of Visual Communication and Image Representation*, pp. 1-10, 2021.

[20] G. Ju and U. Ko, "Research on a novel construction of probabilistic visual cryptography scheme $(k, n, 0, 1, 1)-$PVCS for threshold access structures", *Theoretical Computer Science*, Vol. 863, pp. 19-39, 2021.

[21] S. Vijitha and S. N. Unnithan, "Secure medical image transmission using modified leading diagonal sorting with probabilistic visual cryptography", *Materials Today: Proc.*, pp. 1-9, 2021.

[22] S. Kukreja, G. Kasana, and S. S. Kasana, "Copyright protection scheme for color images using extended visual cryptography", *Computers and Electrical Engineering*, Vol. 91, pp. 1-19, 2021.