IMPROVING SECURITY OF VISUAL CRYPTOGRAPHY BY CONTRAST SENSITIVITY FUNCTION

R. Hemalatha and S. Selvi
Department of Computer Science, PSG College of Arts & Science, Coimbatore, TamilNadu, India

ABSTRACT

Without using complicated conventional cryptographic techniques, Visual Cryptography (VC) has been created to encode images into multiple shares and decode them by stacking the shares. This method aims to securely transmission of real-time images without compromising their visual quality. From this perspective, a Signific VC (SVC) method has been suggested to generate meaningful shares from the Secret Image (SI) and embed them into the Least Significant Bits (LSB) of the Cover Image (CI). By extracting the LSB, the SI was restored on the receiver side. But, this LSB embedding was not vulnerable to attacks since the LSBs of the image were easily decoded by invaders. Hence, in this article, a Secure SVC (SSVC) method is proposed which applies the Contrast Sensitivity Function (CSF) rather than using the LSB embedding and extraction tasks. It comprises 2 different stages: share generation and reconstruction. In the share generation stage, the SI is transformed into the Signific SI (SSI) and the shares are created. Then, the CSF is determined to choose the blocks of the CI and the created hidden shares are implanted at random with the selected blocks of the CI. So, semantic and meaningful shares are produced. Such embedded CI blocks are known as shares. After that, the created shares are forwarded to the user over the transmission medium. Similarly, a key share is created from the received shares in the reconstruction step to recreate the SI. Based on this SSVC method, the robustness of retrieving SIs from the CI is increased. Further, the testing outcomes prove that the SSVC achieves high efficiency in secure image transfer/access in cloud systems compared to conventional VC methods.

Keywords: *Cryptography, cloud computing, Confidentiality, Watermarking*

I. Introduction

Cloud computing is an innovation that makes it simple for numerous businesses, banks, health practitioners, and government agencies to collect, analyze, and adopt database-driven services. But, cloud data privacy is challenging as there are still different challenges and errors. The most frequent privacy problems include information security during storage and transfer, system functionality protection and user data access management. Information safety and integrity are bothered by data owners. Information security during storage and transport is ensured using cryptographic methods [1-2]. They can encode plain text into a cipher and decode cipher text into plain text. However, these systems demand high levels of calculation and essential techniques of administration. They also demand a great deal of knowledge about cryptography.

VC is special cryptography for the concealing of visual data to be decoded by the customer using the corresponding key picture. The system uses two sorts of images: one consists of randomized pixels and the other contains sensitive data. The secret picture is turned into two or more small, unequal portions, excluding encryption keys [3-4]. Only if the shares are combined will the hidden secret key be identified. This makes VC easier if you do not know cryptography and complicated computations in detail. VC is a shared secret in cryptography. It enables users to hide secrets in multiple shares that never define confidentiality until they are stored together. For high-sensitivity technologies such as biomedical verification, access control, steganography and internet banking, VC is mostly appropriate. The advantages of VC use are key-free cryptography, easy processing, no decoding involved, lower cost of estimations and sharing through FAX or email. Many scientists have created numerous VC methods for various purposes in recent days [5].

Among many VC methods, Mary & Kumar [6] designed a new Error Abatement Technique (EAT) to obtain significant shares. It uses value discretization and reduced error filtration strategies. The value discretization filtration splits the pixel coefficients from the grayscale SI and determines the nearby pixel loss that might be regularized to provide meaningful shares. Also, the reduced error filtration was applied to minimize the induced errors and obtain the nearby meaningful shares. Also, the

SVC method was developed, which has share generation and reconstruction steps. In this method, LSB embedding was utilized in the share generation step to generate the shares and the LSB extraction was applied in the reconstruction step to restore the secret photo. On the other hand, this LSB embedding and extraction was vulnerable to steganalysis and was not secure at all. Also, its robustness was less since it can be simply decoded by taking the LSBs of the photo and obtaining the data in binary format. If the embedding data was more than a single LSB, the photo quality may degrade based on how many pixels were modified.

Therefore, in this paper, the CSF is introduced instead of the LSB embedding and extraction processes in the SVC method. In the share generation step, the SI is transformed into the SSI and the shares are created. Then, the CSF is determined to choose the blocks of the CI and the created secret share values are embedded randomly with the selected blocks of CIs. So, semantic and meaningful shares are produced. Such embedded CI blocks are known as shares. After that, the created shares are forwarded to the user over the transmission medium. Similarly, a key share is created from the received shares in the reconstruction step to recreate the SI. Thus, it is more robust than the LSB embedding strategy and cannot be able to decode the blocks easily to retrieve the secret data.

The rest of the article is prepared as follows: Section II studies the works related to the VC methods. Section III explains the proposed methodology and Section IV illustrates its experimental results. Section V concludes the entire work.

II. Literature Survey

An optimal protected VC scheme [7] has been developed, which partitions the brain MRI scans into different blocks using a discrete wavelet transform. Then, a Gaussian-based cuckoo search algorithm was employed to select the best position for all blocks. After that, the dual shares were created from the secret photo and the secret shares were embedded in the respective positions of the blocks. Moreover, the secret photo was extracted and the original photo was reconstructed on the receiver side. But, the number of scans taken was limited.

A double chaotic photo encryption scheme [8] has been developed using the fractional Fourier transform. First, the optimization scheme was acquired using Henon mapping and fractional Fourier transforms to provide the ciphered photo. Then, such photos were considered as input and the logistic chaos was synthesized based on the series of the optimum solution to get the resultant ciphered photo. But, its time complexity was high and it was only effective for non-stationary photos.

A visible clinical photo encryption method [9] has been designed to protect the presence of watermarked clinical photos. Initially, the electronic patient file details were embedded into the clinical photo depending on the watermarking to generate the watermarked clinical photo. Then, this watermarked photo was encrypted with a fingerprint scan based on the integer wavelet transform. Moreover, the fingerprint scan was decrypted using inverse integer wavelet coefficients during extraction. If the fingerprint was correlated, then the clinical photo was reconstructed to retrieve the patient's details. But, it has a high computational cost.

A new 2-step information protection method [10] has been suggested by using VC and QR codes. In the secret sharing scheme, public and secret information were concurrently encoded into subpixel blocks. Then, the visible data was mined from shares by the usual QR scanner. The secret information was restored by the non-determination with a relative difference of 14, lightweight determination with a relative difference of 12 and typical determination with a relative difference of 1. But, it needs to consider more information to detect a higher secret payload.

A protected photo inpainting method [11] has been presented based on a 2D-bicubic interpolation strategy to protect photo information from eavesdropping in the cloud. It has 4 major phases, such as preprocessing, obfuscated share generation, photo inpainting and inpainted photo reconstruction. The private photo to be inpainted was protected by generating many obfuscated photo shares based on the ramp secret sharing scheme. But, it does

not eliminate artifacts and large areas in high-textured photos.

An Extensive VC-based (EVC) copyright protection method [12] has been developed, which performs share generation and ownership validation processes. Initially, the master share was generated from the host photos based on SURF, LBP and K-means clustering. After that, the photos were provided to the owners as their ownership photos and validated by the typical access scheme. But, it has high time complexity to extract the features from photos.

A protected drug management method [13] has been presented by using the threshold sharing mechanism. First, the patient's photo and private information were encoded into the QR code transparencies. After that, the prescription and QR code transparencies were accumulated in the clinical drug management system. If the patient receives the pills, they can scan such QR code transparencies with their smartphone to ensure that they receive each pill prescribed by the doctor. But, the photo was distorted since it was not authenticated by the skilled person.

III. Proposed Methodology

In this section, the SSVC method is described briefly. It encompasses share generation stage and reconstruction stage. This SSVC supports (x, n) and (n, n) methods of VC, n denotes the number of shares created and x denotes the least amount of shares needed for recreating the secret. The value of x is selected to be $n-1$. The (x, n) SSVC method reconstructs the SI at the share creation stage and (n, n) SSVC method reconstructs the SI which is similar to the SI without loss. The structure of SSVC is illustrated in Figure 1.

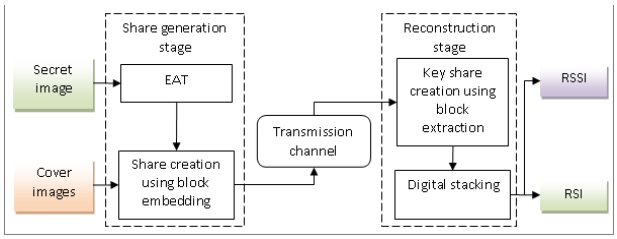


Figure 1. Structure of SSVC Method

3.1 Share Generation Stage

At this stage, the SI is transformed into SSI to create the shares. These secret shares are implanted at random with suitable CI blocks to create significant shares. Normally, CIs are few usual photos that hold coded hidden shares. The suitable CI blocks are chosen by determining the CSF of every block in the CIs. Such embedded CIs are termed as the shares which are transmitted to the users through the transmission medium. Consider, an input SI $(SI_{i,j})$, $0 \leq SI_{i,j} \leq 255$. Figure 2 portrays the functioning of the share creation stage. The steps involved in the creation of shares are the following:

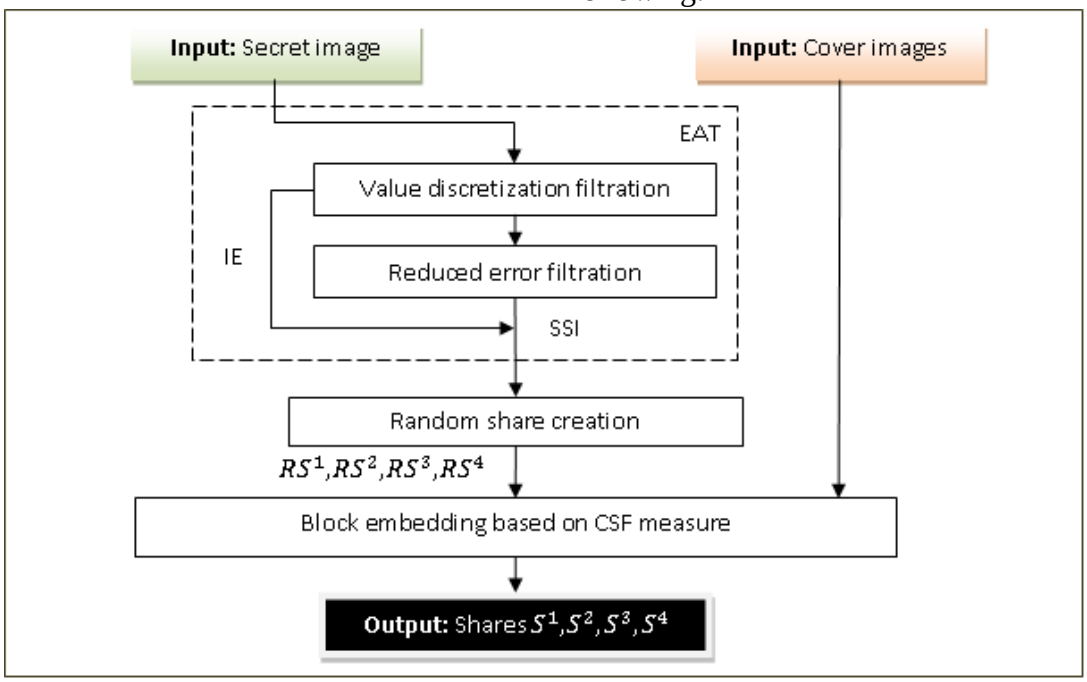


Figure 2. Share Creation Stage

- The input real-time SI is transformed into SSI and the accelerated loss (AL) is determined by the EAT [6] as:

$$AL_{i,j} = EAT(SI_{i,j}) \quad (1)$$

$$SSI_{i,j} = EAT(SI_{i,j}) \quad (2)$$

- The Random Shares (RS) are determined for creating the shares from SSI and AL randomly by

$$randmat = rand(0,1) \quad (3)$$

$$RS_{i,j}^{1} = V_{i,j} \quad \text{where } V_{i,j} \in \left\{\left(\frac{SI_{i,j}}{100}\right), \left(\frac{SI_{i,j}}{10}\right) \bmod 10, SI_{i,j}\ mod\ 10\right\} \quad (4)$$

$$RS_{i,j}^{2} = V_{i,j} \quad \text{where } V_{i,j} \in \left\{\left(\frac{SI_{i,j}}{100}\right), \left(\frac{SI_{i,j}}{10}\right) \bmod 10, SI_{i,j}\ mod\ 10\right\} - \{RS_{i,j}^{1}\} \quad (5)$$

$$RS_{i,j}^{3} = randmat_{i,j} \quad (6)$$

$$RS_{i,j}^{4} = AL_{i,j} \quad (7)$$

Here, $randmat$ indicates the random matrix of dimension as similar as SI created by the random function $rand(\cdot)$ for choosing the shares.

- Then, the RSs are embedded with the CI blocks chosen by the CSF randomly to generate the meaningful shares. The CSF is a measure of the ability to distinguish between luminance of different blocks in the CI. determined as:

$$CSF(u) = \alpha u e^{-\beta u}\sqrt{1 + \gamma e^{bu}} \quad (8)$$

$$\text{Where, } \alpha = \frac{540\left(1+0.7/L\right)^{-0.2}}{1+12/W\left(2+u/3\right)^{2}} \quad (9)$$

$$\beta = 0.3\left(1 + 100/L\right)^{0.15} \quad (10)$$

$$\gamma = 0.06 \quad (11)$$

Here, u is the frequency in cycle per degree, W is the contrast grid strip width and L is the luminance of the image. The blocks having high CSF value are decided for the embedding process which generates the meaningful shares as:

$$S_{i,j}^{n} = \left(C_{i,j}^{n} - mod\left(C_{i,j}^{n}, 10\right) + RS_{i,j}^{n}\right) \quad \text{where } n = 1,2,3,4 \quad (12)$$

In Eq. (12), n indicates the number of shares created and C is the CI. The shares created in this stage are transmitted to the users via a transmission medium.

3.2 Reconstruction Stage

At this stage, a key share is created from the received shares and merged with them to retrieve the SI. Figure 3 portrays the functioning of this phase.

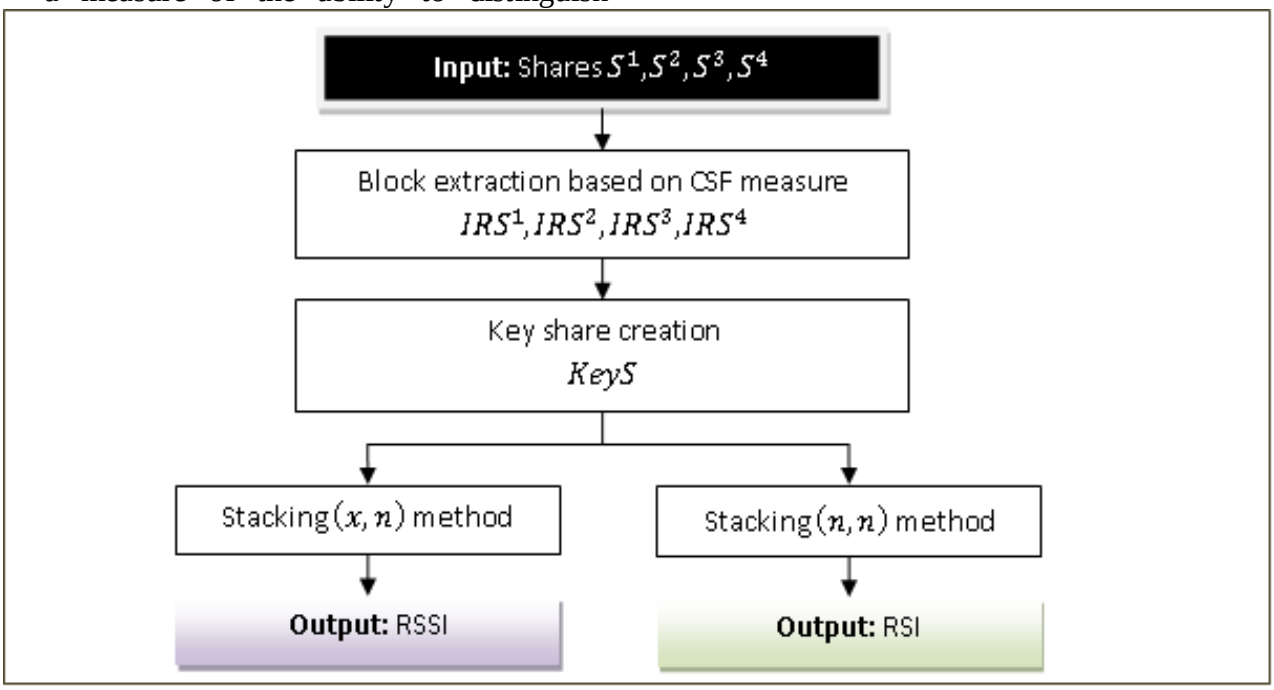


Figure 3. Reconstruction Stage

The steps involved in the reconstruction of the secret are the following:

- First, the CI blocks are extracted using the CSF from the received shares. The Extracted RSs (ERSs) contain the encoded SI.

$$ERS_{i,j}^{n} = \left(S_{i,j}^{n} \bmod 10\right) \text{ where } n = 1,2,3,4 \quad (13)$$

- Using the ERS, a novel key share $(KeyS)$ is created at the reconstruction stage by

$$KeyS_{i,j} = \begin{cases} \delta - \left(ERS_{i,j}^{1} + ERS_{i,j}^{2}\right), & if\ \left(ERS_{i,j}^{1} + ERS_{i,j}^{2}\right) \leq \delta \\ 2\delta - \left(ERS_{i,j}^{1} + ERS_{i,j}^{2}\right), & if\ \left(ERS_{i,j}^{1} + ERS_{i,j}^{2}\right) > \delta \\ 0, & if\ \left(ERS_{i,j}^{1} + ERS_{i,j}^{2}\right) = 0 \end{cases} \quad (14)$$

In Eq. (14), $\delta = 9$, is the highest threshold loss for all pixels.

- Then, the secret is reconstructed using (x, n) SVC method by digitally stacking the ERS and the $KeyS$ by

$$RSSI_{i,j} = \begin{cases} KeyS_{i,j} \times 100 + ERS_{i,j}^{2} \times 10 + ERS_{i,j}^{1}, & ERS_{i,j}^{3} = 1 \\ ERS_{i,j}^{2} \times 100 + KeyS_{i,j} \times 10 + ERS_{i,j}^{1}, & ERS_{i,j}^{3} = 0 \\ 0, & ERS_{i,j}^{3} > 1 \end{cases} \quad (15)$$

This Restored SSI (RSSI) will comprise the IEs from EAT.

- Also, the secret is reconstructed using (n, n) SVC method. An intermediary RSI (IRSI) is acquired through combining each accepted n shares and $KeyS$ as:

$$IRSI_{i,j} = \begin{cases} KeyS_{i,j} \times 100 + ERS_{i,j}^{2} \times 10 + ERS_{i,j}^{1} + ERS_{i,j}^{4}, & ERS_{i,j}^{3} = 1 \\ ERS_{i,j}^{2} \times 100 + KeyS_{i,j} \times 10 + ERS_{i,j}^{1} + ERS_{i,j}^{4}, & ERS_{i,j}^{3} = 0 \\ 0, & ERS_{i,j}^{3} > 1 \end{cases} \quad (16)$$

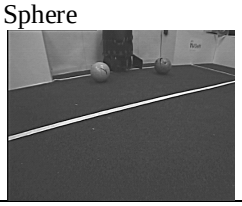
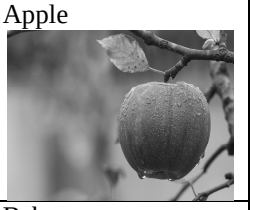
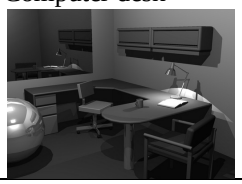
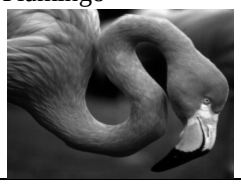
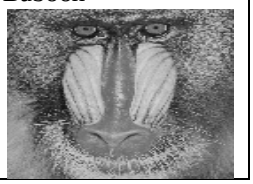
This IRSI is utilized to restore the actual SI by

$$RSI_{i,j} = \begin{cases} IRSI_{i,j} - \delta, & ERS_{i,j}^{4} > \varepsilon \\ IRSI_{i,j}, & Or\ else \end{cases} \quad (17)$$

In Eq. (17), $\varepsilon = 4$, is the average loss of a particular pixel. The SI is evaluated with RSSI and RSI by multiple criteria and the results are demonstrated.

IV. Experimental Results

In this section, the efficiency of (x, n) and (n, n) SSVC methods is analyzed by implementing them in MATLAB 2017b. Also, the efficiency is compared with the EVC [12], (x, n) and (n, n) SVC [6] methods. The comparative analysis is conducted regarding Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), Mean Absolute Error (MAE), Universal Image Quality Index (UIQI) and Structural Similarity Index (SSIM). In this study, 4 grayscale SI of various categories and 4 CIs of dimension 512×512 are selected randomly. The SI is transmitted to the recipient via splitting them into 4 shares, which are hidden in 4 CIs. Figure 4 portrays considered actual SIs, the conversion of such SIs into SSI and the shares created by CIs.

	(a)	(b)	(c)	(d)
SI	Motorcycle 	Sphere 	House 	Apple 
Cover image	Girl 	Computer desk 	Flamingo 	Baboon 

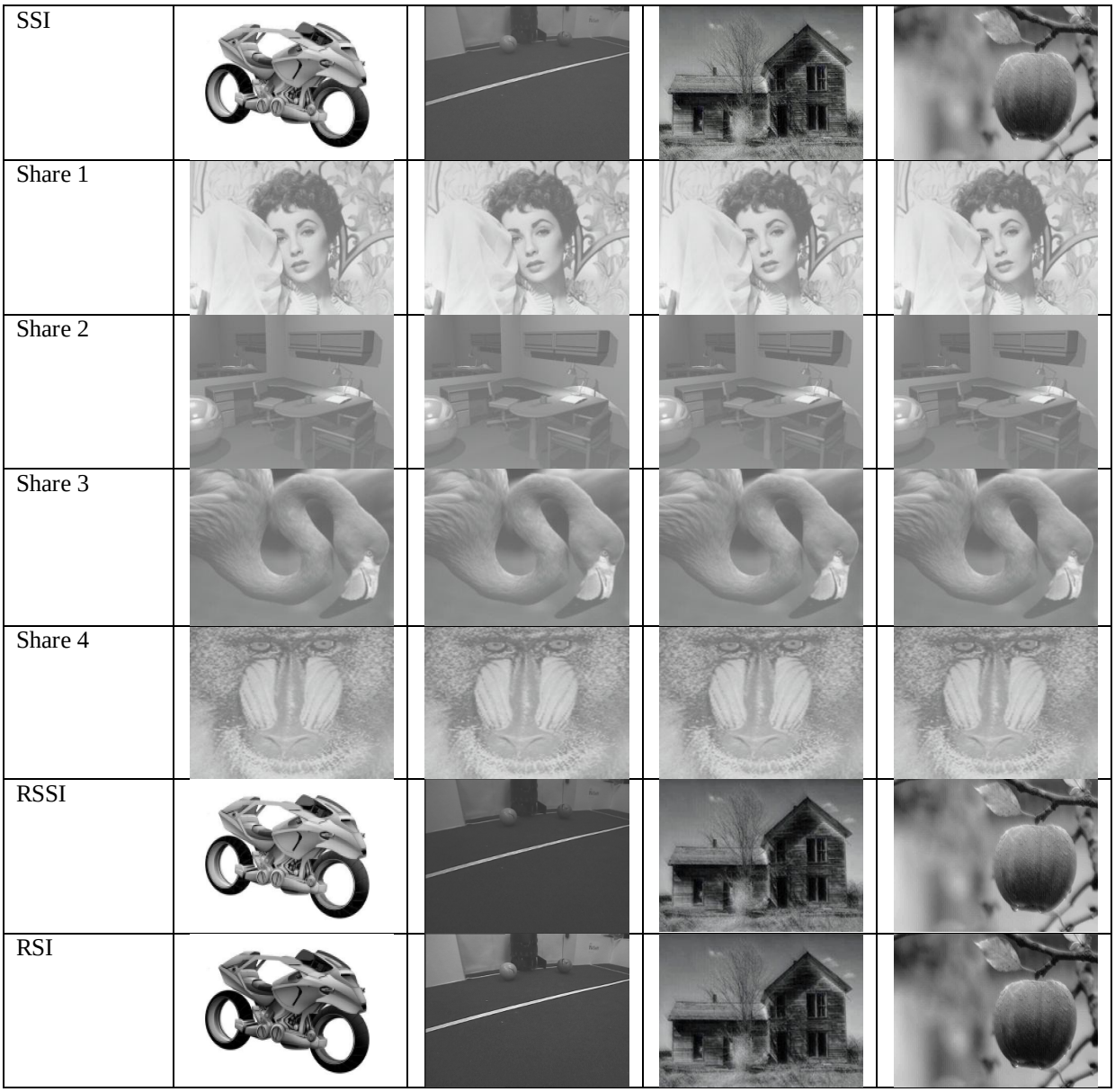


Figure 4. Transformations of Secret Images using SSVC

- **MSE:** It is the average loss of the restored SI to the actual SI. The smaller the loss in the restored SI, the less the MSE range.

$$MSE = \frac{\sum_{M,N}[SI_{m,n} - RSI_{m,n}]^2}{M \times N} \quad (18)$$

In Eq. (18), M, N are the total rows and columns in the SI, $SI_{m,n}$ is the actual SI at m^{th} row and n^{th} column and $RSI_{m,n}$ is the restored SI at m^{th} row and n^{th} column.

- **PSNR:** It is the fraction of the actual SI to the decoded SI. The greater the PSNR, the greater the accurateness of the restored image.

$$PSNR = 10 \log_{10} \left(\frac{SI_{max^2}}{MSE} \right) \quad (19)$$

In Eq. (19), SI_{max} is the highest pixel range of the SI.

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

$$MAE = \frac{\sum_{M,N}|RSI_{m,n} - SI_{m,n}|}{M \times N} \quad (20)$$

- **UIQI:** It depends on the luminosity, sharpness and texture. It is determined as:

$$UIQI(a, b) = \frac{4\mu_a \mu_b \sigma_{ab}}{(\mu_a^2 + \mu_b^2)(\sigma_a^2 + \sigma_b^2)} \quad (21)$$

In Eq. (21), μ_a, μ_b are the average values of actual (a) and restored (b) images, σ_a, σ_b are the standard variation of actual and restored images and σ_{ab} is the covariance of both images.

- **SSIM:** It depends on determination of the luminosity, sharpness and texture. It is determined as:

$$SSIM(a,b) = \frac{(2\mu_a\mu_b+c_1)(2\sigma_{ab}+c_2)}{(\mu_a^2+\mu_b^2+c_1)(\sigma_a^2+\sigma_b^2+c_2)} \quad (22)$$

In Eq. (22), c_1 and c_2 are the constants. The range of UIQI and SSIM are $[-1,1]$ where 1 refers to the actual and restored SIs are indistinguishable for each pixel.

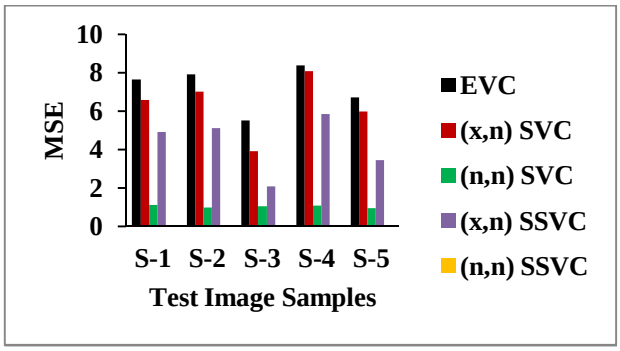


Figure 5. Evaluation of MSE for Proposed and Existing VC Methods

Figure 5 shows the MSE outcomes achieved by the different VC methods using six different test samples. This analysis indicates that the (x,n) SSVC decreases pixel losses by up to 11.9% compared to the other VC methods. Also, the (n,n) SSVC method has a zero MSE than the other VC methods, which means that the restored SI and the actual SI are alike without any pixel errors.

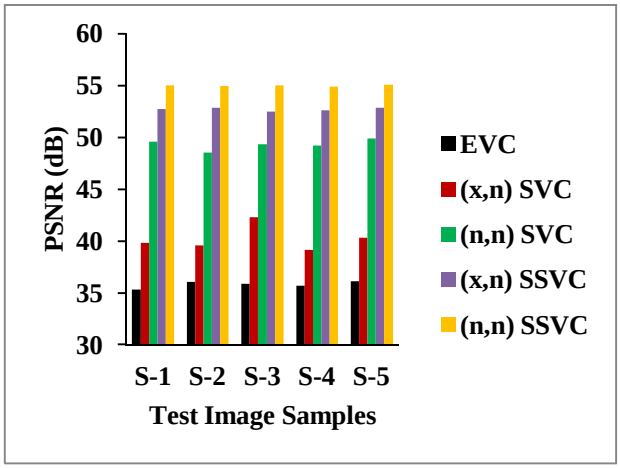


Figure 6. Evaluation of PSNR for Proposed and Existing VC Methods

Figure 6 depicts the PSNR outcomes achieved by the different VC methods using six different test samples. It observes that the (x,n) SSVC improves the PSNR value by up to 26.12% compared to the other VC methods. Also, the (n,n) SSVC method results in a PSNR about 55dB more than the existing VC methods. This is because of reducing the pixel losses in the restored SI efficiently.

Figure 7 shows the MAE values of proposed and existing VC methods using 6 different sample test images. It shows that the (n,n) SSVC method decreases the MAE by about 63.42% compared to the other existing VC methods, which indicates that this method can minimize the pixel errors in the restored SI to get the actual SI.

Similarly, Figure 8 and 9 portray the UIQI and SSIM values of the proposed and existing VC methods using 6 different sample test images. This analysis signifies that the (n,n) SSVC method achieves higher UIQI and SSIM, which means that the actual SI and restored SI are more identical.

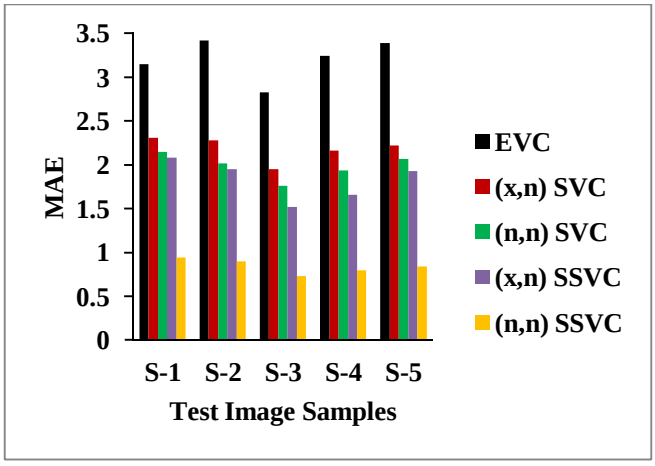


Figure 7. Evaluation of MAE for Proposed and Existing VC Methods

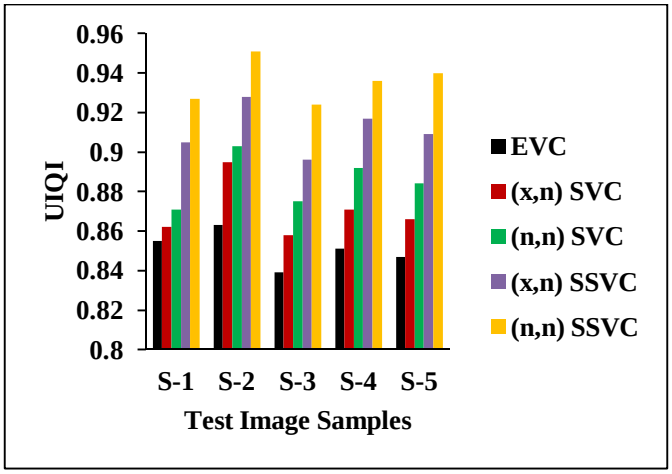


Figure 8. Evaluation of UIQI for Proposed and Existing VC Methods

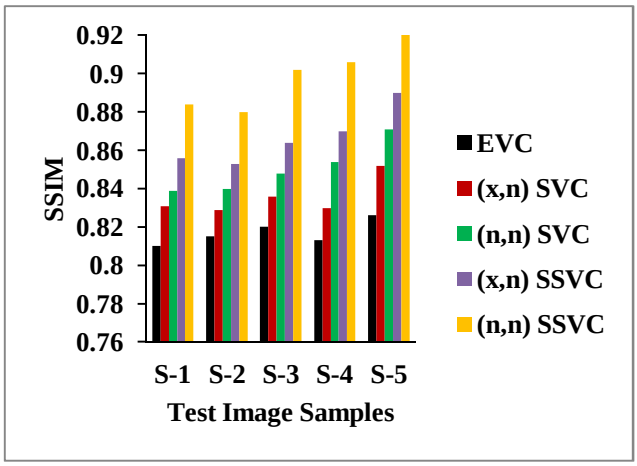


Figure 9. Evaluation of SSIM for Proposed and Existing VC Methods

V. Conclusion

In this paper, the SSVC method was presented to enhance SI sharing without losing its visual quality. This method has 2 stages, namely, share generation and reconstruction. First, the SI was converted into the SSI and the shares were generated. After that, the CSF was computed to decide the CI blocks for embedding secret shares into them randomly, which generated the meaningful shares. These generated shares were sent to the cloud users via a transmission channel. On the receiver side, a key share was generated by extracting the blocks which hold the received shares to restore the SI efficiently from the CI. Finally, the experimental outcomes show that the SSVC method has higher PSNR and less MSE compared to the classical VC methods.

References

1. Yan, Z., Deng, R. H., & Varadharajan, V. (2017). Cryptography and data security in cloud computing. Information Sciences, 387, 53-55.
2. Albalabi, A., & Hamza, N. (2020). A survey on cloud data security using image steganography. International Journal of Advanced Computer Science and Applications, 11(1), 645-649.
3. Punithavathi, P., & Subbiah, G. (2018). Visual cryptography for securing images in cloud. In Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications, IGI Global, pp. 360-380.
4. Almutairi, S., & Aborokbah, M. (2019). A new secure transmission scheme between senders and receivers using HVCHC without any loss. EURASIP Journal on Wireless Communications and Networking, 2019(1), 1-15.
5. Thomas, S. A., & Gharge, S. (2017). Review on various visual cryptography schemes. In IEEE International Conference on Current Trends in Computer, Electrical, Electronics and Communication, pp. 1164-1167.
6. Mary, G. S., & 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.
7. Begum, A. A. S., & Nirmala, S. (2018). Secure visual cryptography for medical image using modified cuckoo search. Multimedia Tools and Applications, 77(20), 27041-27060.
8. Li, G. D. (2019). Double chaotic image encryption algorithm based on optimal sequence solution and fractional transform. The Visual Computer, 35(9), 1267-1277.
9. Fu, Z., Cheng, Y., Liu, S., & Yu, B. (2019). A new two-level information protection scheme based on visual cryptography and QR code with multiple decryptions. Measurement, 141, 267-276.
10. Priya, S., & Santhi, B. (2019). A novel visual medical image encryption for secure transmission of authenticated watermarked medical images. Mobile Networks and Applications, 1-8.
11. Tanwar, V. K., Raman, B., Rajput, A. S., & Bhargava, R. (2020). 2DInpaint: a novel privacy-preserving scheme for image inpainting in an encrypted domain over the cloud. Signal Processing: Image Communication, 88, 1-57.
12. Kukreja, S., Kasana, G., & Kasana, S. S. (2020). Extended visual cryptography-based copyright protection scheme for multiple images and owners using LBP–SURF descriptors. The Visual Computer, 1-18.

13. Ti, Y. W., Chen, S. K., & Wu, W. C. (2020). A new visual cryptography-based QR code system for medication administration. Mobile Information Systems, 2020, 1-10.