Fast Comprehensive Secret Sharing using Naive Image Compression

Heri Prasetyo[1], Kukuh Caezaocta Prayuda[2]
Department of Informatics, Universitas Sebelas Maret (UNS), Surakarta, Indonesia

***Abstract*—This paper presents a simple method for performing *(k,n)*-Secret Sharing (SS) with fast computation. It aims to reduce the computational time of the former scheme in the shadow generation process. The former scheme performs SS with the polynomial function computation by involving the color palette. The color palette transforms noisy-like shadow image into more meaningfull appearance. However, this scheme requires a high computational burden on this transformation process. The proposed method exploits naive image compression to decrease the required bit for representing a secret and cover image. It effectively avoids the color palette usage previously used by the former scheme. The proposed method produces a set of shadow images with a cover image-like appearance. In addition, the secret and cover image can be reconstructed by gathering at least *k* shadow images. As documented in the Experimental Results section, the proposed method yields a promising result in the *(k,n)*-SS with reduced computational time compared to that of the former scheme.**

***Keywords*—Comprehensive; image compression; naïve; polynomial; secret sharing**

I. Introduction

Several methods have been proposed for secure secret image communication. The SS is the most popular approach to securely send one or multiple images from the sender to other parties, i.e. called as receiver or participant. The first work in the SS can be traced back to the classical paper [1]. It introduces a SS concept under (k,n)-SS thresholded setting. In this method, a secret method is converted into n shadows images and then transferred to the n participants. The recovery process aims to reconstruct a secret image by collecting k or more shadow images to achieve a correct or lossless result. If the number of collected shadow images is less than k, the recovered secret image is lossy, or nothing is obtained. An improvement of SS method is Visual Cryptography (VC) [2] which performs SS into a grayscale image. This improvement leads the direction for further development of SS methods. On the other hand, the Chinese Remainder Theorem (CRT)-based SS [3] also gain popularity because of its wider application ability. However, the CRT-based SS has a slight limitation in the secret image recovery process. The recovered image is lossy compared to that the original image. While the other methods use a binary set basis [4-5], modular arithmetics [6], general access structure [7], bitwise Boolean operation [8-9], adaptive weight priority [10], etc., to generate a set of shadow images.

In another ways, several techniques have also been developed for the multiple secret sharing [11-14]. Most methods exploit the exclusive-OR operation and CRT computation to generate a set of shadow images. The method in [11] involves a simple image encryption, while scheme in [12] utilizes the generalized chaotic image scrambling. The methods in [13] and [14] use the hyperchaotic image scrambling and improved beta chaotic image encryption, respectively, to yield a set of shadow images. However, all technique produces the noise-like shadow.

The SS and its variants effectively secure secret image communication. But, a set of shadow images generated by these methods are in a noise-like appearance. A malicious attacker can easily recognize these shadow images as a secure image containing some confidential information. This attacker may collect several shadow images to obtain a fake or counterfeit secret image. This situation is unacceptable in secret image communication. Thus, the friendly SS tries to solve this problem by converting each shadow image into a more friendly appearance or cover image-like. An attacker now cannot perceive the noise-like shadow image. The method in [15] is an example of a friendly SS approach. It utilizes the CRT and bitwise Boolean operation to generate a set of shadow images. The methods in [16] and [17]perform thresholded SS and progressive SS, respectively, with the meaningfull shadow images. Meanwhile, the method [18] generates a set of meaningfull shadow images under the multiple secret sharing framework.

Several method have been reported in literature in order to convert the noise-like shadow image into more friendly or meaningfull appearance such as in [15-19]. The method in [19] performs the comprehensive visual SS. A secret image is converted into a set of shadow images with a friendly or cover image-like appearance. This scheme employs the polynomial function computation and color palette in the shadow image generation stage. It can be categorized as (k,n)-SS. This method effectively produces a set of shadow images in the cover-like appearance. The secret and cover images can be recovered from at least k collected shadow images. However, this method requires a very high computational burden in the shadow image generation since it needs to compare the similarity over four bits as mentioned in [19]. It becomes inferior for the practical implementation of SS required fast computation. The method offers a solution to transform the noise-like shadow to be more meaningfull.

Thus, this paper offers a solution to reduce the computational time of [19] using naive image compression. This naive compression or image companding scheme effectively overcomes the former scheme limitation. The proposed work give a significant contribution on reducing the computational time of [19] in the comprehensive secret sharing task. It replaces the color pallete usage with a simple image compression technique. It introduces a new concept for converting the noise-like shadow image into more friendly appearance with noise compression (companding) which can be further utilized for future works, i.e. friendly secret sharing, comprehensive secret sharing, image watermarking [20], etc.

II. Former Scheme of Comprehensive Secret Sharing

This section introduces the former scheme [19] for performing secret sharing. It can be regarded as (k,n)-SS, with $k<n$, since it converts a secret image into n shadow images, while it requires at least k shadow images to obtain a recovered secret image. The method in [19] generates a set of shadow images in which their appearance is maintained as similar as possible to the targeted cover images. It employs a set of cover images in shadow image generation. The secret image can be recovered by using at least k shadow images. In addition, the cover image can also be reconstructed using after obtaining the recovered secret image. This aforementioned method employs the color palette to generate a set of shadow images and to recover secret and cover images.

The detail of the former method [19] can be explained as follow. Let I be a secret image, and $\{C_1, C_2, \dots, C_n\}$ be a set of cover images. This method forces to change I into a set of shadow images $\{S_1, S_2, \dots, S_n\}$. The appearance of shadow image should be as similar as possible to the cover image, i.e. $S_i \approx C_i$ for $i=1,2,\dots,n$. The method in [19] firstly extracts four bits of each cover image C_i as follow:

$$C_i = \langle c_1, c_2, \dots, c_4 \rangle \quad (1)$$

where $c_1, c_2, \dots, c_4$ denotes four extracted bits of C_i, with c_1 is the most significant bit. These four bits are acquired by using a color palette [19]. Yet, The secret image is regarded as a_0, i.e. $a_0 = I$. Subsequently, the polynomial function computation is applied to perform (k,n)-SS as follows:

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1} (\mathrm{mod}\, P) \quad (2)$$

where $f(x)$ is the polynomial function order k, for $x = 1,2,\dots,n$. The value of P is a prime number. It is typically set as $P=257$ in the 8-bits image representation. While the value of a_i is a random number generated in the range $a_i \sim [0, P)$, for $i = 1,2,\dots,k-1$. The temporary shadow image T_i can be obtained by changing the value of x in (2) with the index of shadow image, i.e. $i=1,2,\dots,n$. The computation of T_i can be conducted as follow:

$$T_i = f(i) \quad (3)$$

for $i=1,2,\dots,n$. From this process, one obtains a set of temporary shadow images $\{T_1, T_2, \dots, T_n\}$.

Until this process, the appearance of each shadow image T_i is in noise-like form. The appearance of T_i should be exchanged to be more resemble as C_i. An additional step is needed to perform this process. The temporary shadow image T_i should be converted from decimal into 8-bits representation. This binary number extraction process is given as:

$$T_i = \langle t_1, t_2, \dots, t_8 \rangle \quad (4)$$

where t_i is the i-th bit, for $i = 1,2,\dots,8$, with t_1 is the most significant bit. The proposed method simply compares the four significant bits of T_i with the four significant bits of C_i. If there are all identical, T_i is then regarded as the shadow image S_i. Specifically, if $c_i = t_i$ for $i=1,2,\dots,4$, this process is performed:

$$S_i = T_i \quad (5)$$

where S_i denotes the i-th shadow image, for $i=1,2,\dots,n$. Otherwise, the proposed method needs to recompute (2), i.e. the computation of polynomial function is executed again until the four significant bits are identical to that of the four significant bits of cover image. This process produces a set of shadow images $\{S_1, S_2, \dots, S_n\}$. Now, each shadow image S_i is visually similar to the cover image C_i.

The Lagrange interpolation is utilized to extract a secret image. Herein, the receiver simply collects at least k shadow images in the recovery process to obtain a lossless secret image. One gets a recovered secret image $\tilde{I}$ after applying the Lagrange interpolation. To reconstruct the cover image, the receiver needs to extract four significant bits of each S_i. Then, the inverse process of color palette computation [19] is performed to yield C_i, for $i=1,2,\dots,n$, by considering four significant bits of S_i. This process produces a set of recovered cover images as $\{C_1, C_2, \dots, C_n\}$. The former scheme performs well in the (k,n) under the comprehensive SS setting.

Even though the former method effectively generates a set of shadow images with a cover-like appearance. However, the computation of similarity matching over four significant bits, i.e. $c_i = t_i$ for $i=1,2,\dots,4$, need a high computational burden. The method should recalculate $f(x)$ if the four bits are not identical. It will be inconvenient if a fast computation response is required to generate a set of shadow images from a secret image.

III. Proposed Method

The proposed method offers a simple solution for the limitation of former scheme [19]. It tries to reduce the computational burden of similarity matching for four significant bits. The proposed method avoids this similarity matching to further reduce the computational time. Herein, simple naive image compression is exploited in the shadow image generation and secret image recovery. Sender and receiver do not use the color palette in this SS process. The proposed method is further explained in this section as follows.

A. Shadow Image Generation

As mentioned before, the proposed method converts a secret image I into a set of shadow images. This method involves a set of cover images as $\{C_1, C_2, \dots, C_n\}$. Let r and q be the required bit for compressing the secret and cover images, respectively. The value should satisfy $r+q=8$, for an 8-bits representation of an image. These two values should be kept for both sender and receiver in the SS process. The proposed method performs naive image compression or image companding process utilizing two specific quantizer values. These two quantizer values can be computed as follows:

$$Q_s = 2^{8-r} \quad (6)$$

$$Q_c = 2^{8-q} \quad (7)$$

where Q_s is the quantizer value for the secret image, and Q_c is the quantizer for cover image. Subsequently, the compression processes for secret image I and cover image C_i are performed as follows:

$$\hat{I} = \left\lfloor \frac{I}{Q_s} \right\rfloor \quad (8)$$

$$\hat{C}_i = \left\lfloor \frac{C_i}{Q_c} \right\rfloor \quad (9)$$

where $\hat{I}$ is a compressed secret image, and $\hat{C}_i$ is the i-th compressed cover image. The symbol $\lfloor \cdot \rfloor$ represents the floor operator. From these computations, the lengths of $\hat{I}$ and $\hat{C}_i$ are now with r and q-bits, respectively. The compressed secret image $\hat{I}$ can be converted into binary form as follow:

$$\hat{I} = \langle \hat{\imath}_1, \hat{\imath}_2, \dots, \hat{\imath}_r \rangle \quad (10)$$

where $\hat{\imath}_i$ is the i-th bit of $\hat{I}$, for $i = 1,2,\dots,r$. While $\hat{\imath}_1$ is the most significant bit. The binary conversion of compressed cover image $\hat{C}_i$ is given as:

$$\hat{C}_i = \langle \hat{c}_{i1}, \hat{c}_{i2}, \dots, \hat{c}_{iq} \rangle \quad (11)$$

where $\hat{c}_{ij}$ is the j-th bit of $\hat{C}_i$, for $j = 1,2,\dots,q$. The most significant bit is represented with $\hat{c}_{i1}$. These binary numbers are used in shadow image generation.

Subsequently, the polynomial function is computed with $P = 2^r$. Herein, the value of P is a non-primary number. In our proposed method, the value of P depends on the required bit of secret image, i.e. r. Similar to the former scheme [19], the proposed method also considers $a_0 = I$. It also generates a set of random numbers in a specific range, i.e. $a_i \sim [0, P)$ for $i = 1,2,\dots,k-1$. The polynomial function for the SS can be calculated as follow:

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1} (\operatorname{mod} P) \quad (12)$$

This computation is for $x = 1,2,\dots,n$. It should be noted that $f(x)$ is in r-bits representations, i.e. the length of $f(x)$ is r under the binary form. The temporary shadow image is then obtained by replacing x with the index of shadow image, i.e. $x = i$. This process is formally defined as follows:

$$T_i = f(i) \quad (13)$$

for $i = 1,2,\dots,n$. Each temporary shadow image is also in r-bits representation, i.e. $T_i = \langle t_{i1}, t_{i2}, \dots, t_{ir} \rangle$. The proposed method performs bit concatenation between all bits in T_i with all bits in $\hat{C}_i$. Then, the final shadow image is obtained as follows:

$$S_i = [\hat{c}_{i1}, \hat{c}_{i2}, \dots, \hat{c}_{iq}, t_{i1}, t_{i2}, \dots, t_{ir}] \quad (14)$$

where S_i is the i-th shadow image, for $i = 1,2,\dots,n$. The symbol $[\cdot]$ denotes the bit concatenation operator. Herein, the length of S_i is 8-bits. After converting the binary number into the decimal representation of each S_i, one can gain a set of shadow images $\{S_1, S_2, \dots, S_n\}$. The sender sends these shadow images to the receiver via a communication channel.

B. Secret Image Recovery

In the secret image recovery process, the receiver tries to produce a set image and recovered cover image by collecting several shadow images $\{S_1, S_2, \dots, S_K\}$, while $k \le K \le n$ to obtain a perfect reconstruction process. The receiver firstly converts each shadow image into binary representation as follows:

$$S_i = [\hat{c}_{i1}, \hat{c}_{i2}, \dots, \hat{c}_{iq}, t_{i1}, t_{i2}, \dots, t_{ir}] \quad (15)$$

for $i = 1,2,\dots,K$. Where K denotes the number of collected shadow images. The r least significant bits are extracted from (15) to generate a temporary shadow image. This binary number is then converted into decimal number as follows:

$$T_i = \operatorname{Dec}\langle t_{i1}, t_{i2}, \dots, t_{ir} \rangle \quad (16)$$

for $i = 1,2,\dots,K$. While $\operatorname{Dec}\langle \cdot \rangle$ denotes the operator from binary to decimal number conversion. The Lagrange interpolation as used in [19] is then applied to all T_i to yield I^*, where I^* denotes a temporary secret image. This temporary secret image is still in low dynamic range, i.e. it is still in r-bits representation. The final secret image is then produced using the following process:

$$\tilde{I} = Q_r \times I^* \quad (17)$$

where $\tilde{I}$ represents a recovered secret image. In the proposed comprehensive (k, n)-SS, the cover image can be recovered from the shadow image. The receiver extracts q-bits from (15) to recover the cover image. The process of cover image recovery is given as follows:

$$\tilde{C}_i = Q_c \times \operatorname{Dec}\langle \hat{c}_{i1}, \hat{c}_{i2}, \dots, \hat{c}_{iq} \rangle \quad (18)$$

where $\tilde{C}_i$ denotes the i-th recovered cover image, for $i = 1,2,\dots,n$. Both sender and receiver need Q_s and Q_c in the secret image recovery and cover image reconstruction process. The receiver only keeps the values of r and q for computing Q_s and Q_c. Using this simple approach, the proposed method overcomes the limitation of the former scheme [19] in the high computational burden.

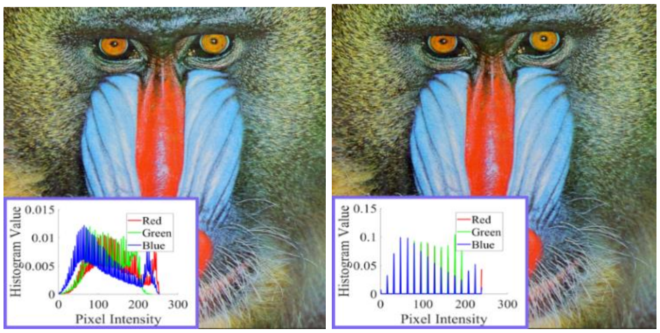
IV. Experimental Results

Several experiments have been conducted to investigate the proposed method performance. All experiments are then reported in this section. This section firstly shows the experimental results under the visual inspection, i.e. the correction of the proposed method is only observed under human investigation. Subsequently, it delivers the performance comparisons under the objective quality assessment. In our experiments, all images are of size 512×512. All images are in color format. The histogram is given at the bottom left of each image.

A. Visual Observation

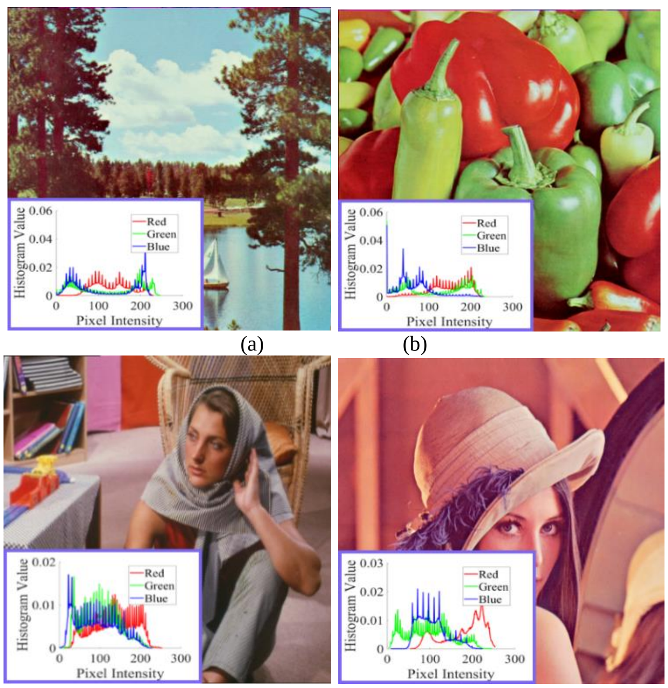
This subsection reports the proposed method performance for dealing with (3,4)-SS and (2,3)-SS. This experiment only overlooks the generated shadow images and recovered secret image with the visual investigation. Herein, one secret image is involved, and several cover images are used in the experiment. Fig. 1(a) depicts a secret image used in the experiment. This image is in original I, while Fig. 1(b) is the compressed version

$\hat{I}$ with $r = 4$. A set of original cover images is shown in Fig. 2, while the compressed version of all cover images are given in Fig. 3. Herein, the required bit for the cover image is set as $q = 4$.



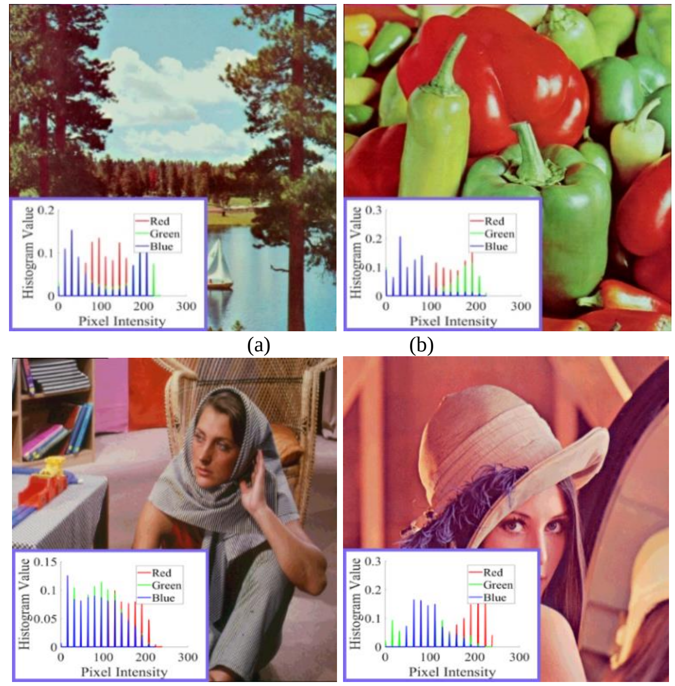
(a) (b)

Fig. 1. Secret image used as experiment: (a) original image I, and (b) compressed version $\hat{I}$



(a) (b) (c) (d)

Fig. 2. A set of cover images: (a) C_1, (b) C_2, (c) C_3, and (d) C_4



(a) (b) (c) (d)

Fig. 3. A set of compressed cover images: (a) $\hat{C}_1$, (b) $\hat{C}_2$, (c) $\hat{C}_3$, and (d) $\hat{C}_4$

This section firstly considers the proposed method performance under (3,4)-SS setting. Fig. 4 is a set of shadow images obtained from our scheme. As shown in this figure, the content of each shadow image is almost similar to that of the original cover image. Thus, the proposed method effectively performs the comprehensive secret sharing with (3,4)-SS approach. Recovered secret images are obtained by performing the secret image recovery process involving several shared images. Fig. 5 delivers the recovered secret image $\tilde{I}$ while two or more shared images are used in the recovery process. The proposed method yields correct results for (3,4)-SS. The secret image can be losslessly recovered while at least three shadow images are used in the recovery process. In addition, a set of cover images can be recovered after extracting the secret image. Fig. 6 reports the result of recovered secret image. Herein, all shadow images are employed for performing the cover image recovery. As demonstrated in this figure, the proposed method is able to recover the cover image with an identical result compared to the compressed version of cover image.

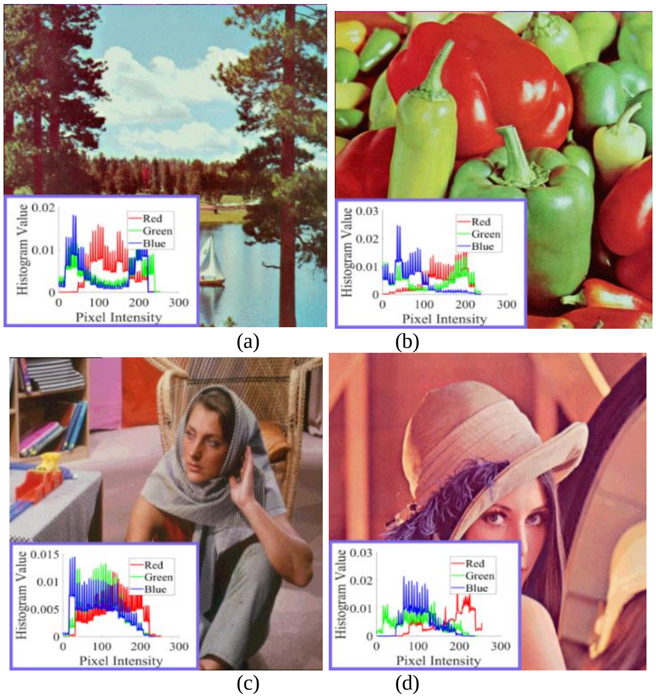


Fig. 4. A set of shadow images from (3,4)-SS: (a) S_1, (b) S_2, (c) S_3, and (d) S_4

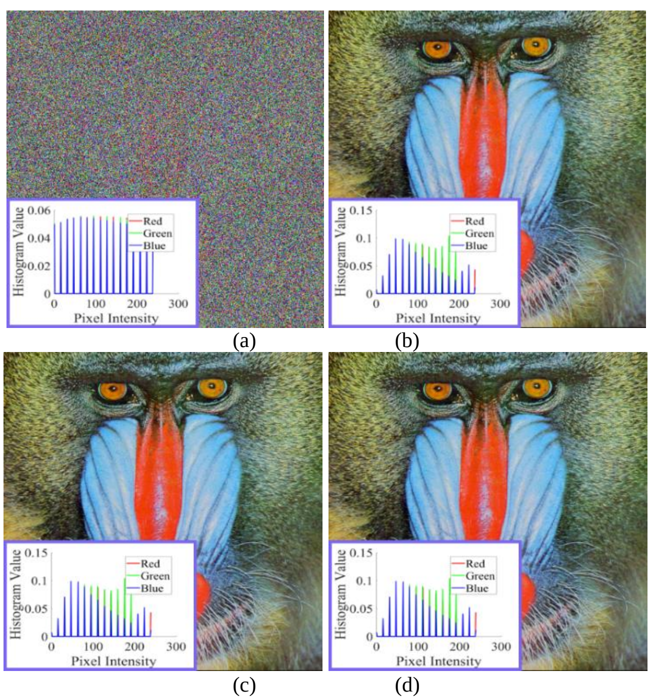


Fig. 5. Recovered secret image $\tilde{I}$ from (3,4)-SS by involving several shared images: (a) $\{S_1, S_2\}$, (b) $\{S_1, S_2, S_3\}$, (c) $\{S_2, S_3, S_4\}$, and (d) $\{S_1, S_2, S_3, S_4\}$.

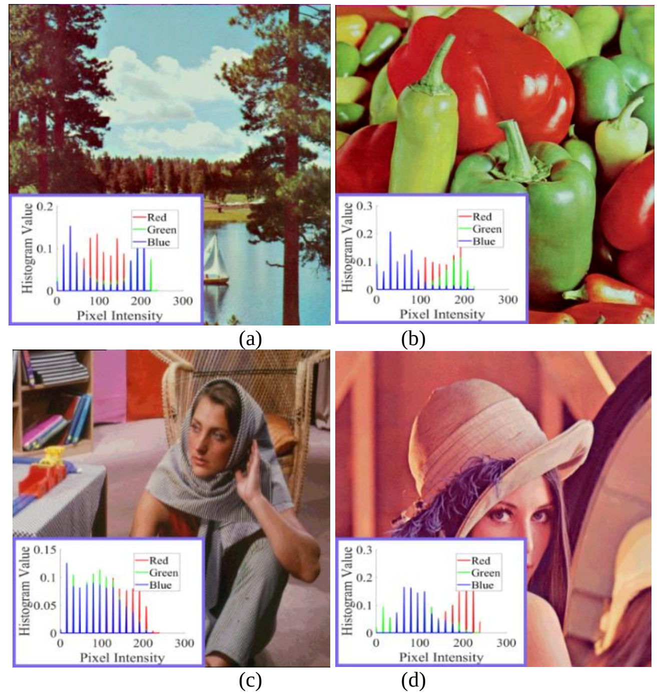


Fig. 6. Recovered cover images from (3,4)-SS: (a) $\tilde{C}_1$, (b) $\tilde{C}_2$, (c) $\tilde{C}_3$, and (d) $\tilde{C}_4$

An additional experiment is also executed further to examine the correctness of proposed method under visual investigation. This experiment inspects the proposed method under (2,3)-SS setting. A secret image and three cover images are from Fig. 1(a) and Fig. 3(a-c), respectively. It also utilizes $r = q = 4$. The proposed method yields a set of shadow images as delivered in Fig. 7. Again, the proposed method performs well in converting the secret image into a set of shadow images whose appearance is similar to that of the cover image. Fig. 8 exhibits the visual result of the recovered secret image $\tilde{I}$ while one or more shared images are involved during the recovery process. The recovered secret image is lossless, while at least two shadow images are used. Thus, the proposed method is correct for performing the (2,3)-SS. A set of recovered cover images can also be obtained using all shadow images during the recovery process. Fig. 9 shows a set of recovered cover images. All of these images are identical to that of the compressed cover image. It can be concluded that the proposed method gives promising results for (k, n)-SS with the comprehensive scenario. In addition, the proposed is a strong candidate while implementing the comprehensive secret sharing compared to the other scheme. It avoids the computation burden as used in [19]. It also requires a simple step for conducting the comprehensive secret sharing.

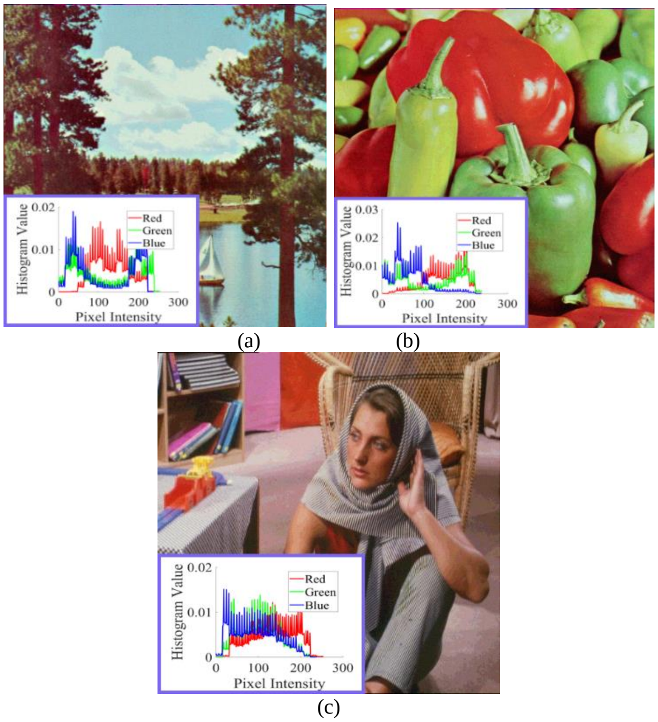


Fig. 7. A set of shadow images generated by (2,3)-SS: (a) S_1, (b) S_2, and (c) S_3

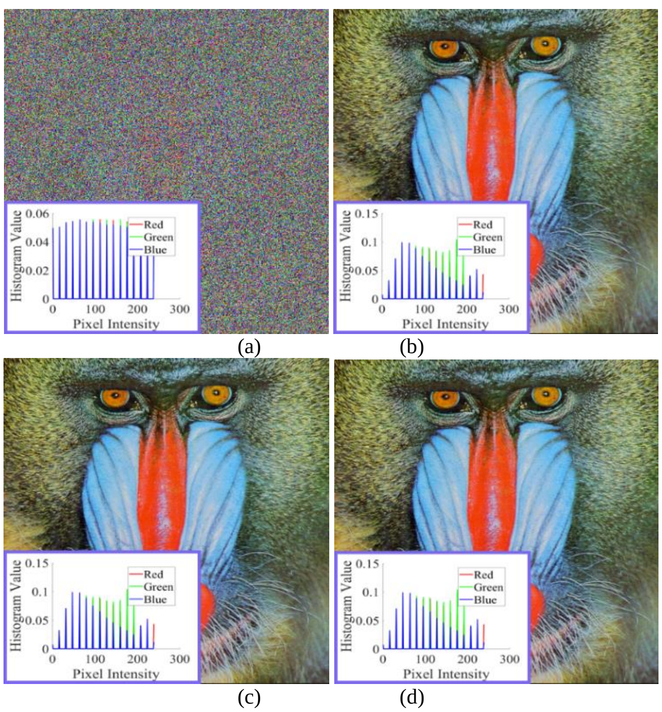


Fig. 8. The visual of $\tilde{I}$ from (2,3)-SS when shared images are used in the recovery process: (a) $\{S_2\}$, (b) $\{S_1, S_2\}$, (c) $\{S_2, S_3\}$, and (d) $\{S_2, S_3, S_1\}$

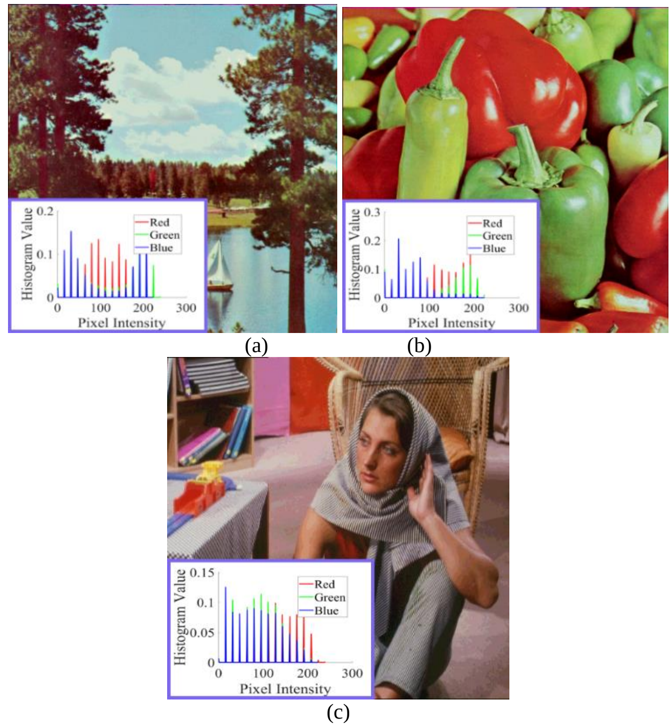


Fig. 9. A set of recovered cover images from (2,3)-SS: (a) $\tilde{C}_1$, (b) $\tilde{C}_2$, and (c) $\tilde{C}_3$

B. Objective Comparisons

This subsection summarizes the proposed method performance under the objective image quality assessment. This experiment only examines the proposed method under (3,4)-SS setting. It observes the performance by investigating the effect of required bit for secret image r. It means that the cover image is compressed with various q with $q = 8 - r$. All shadow images are involved during the secret image recovery process. The similarity between the shadow image and the original cover is measured with Peak-Signal-to-Noise Ratio (PSNR). It computes the average PSNR scores over all four shadow images. The similarity between the recovered cover image and the original version is also observed under the average PSNR score. This calculation is also for the recovered and original secret images. A higher value of average PSNR indicates better performance. Fig. 10 displays the performance comparisons with the average PSNR value over various $r = \{2,3, \ldots ,6\}$. The quality of shadow image and recovered cover image is decreased while applying higher r. But, the quality of a recovered secret image is increased by using a higher value r. The proposed method yields the best performance with $r = q = 4$, as confirmed in Fig. 10.

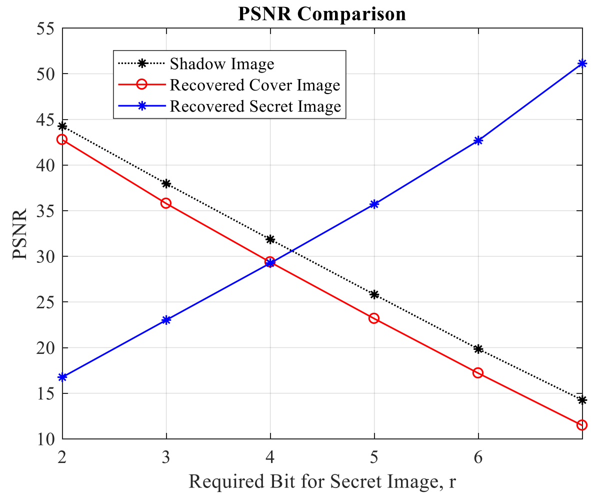


Fig. 10. Performance comparisons in terms of average PSNR value

The evaluations are also observed for the proposed method performance in terms of Structural Similarity Index Metric (SSIM). Herein, this experiment also considers the quality of shadow image, recovered cover image, and recovered secret image. A higher value of SSIM also implies better performance. Fig. 11 demonstrates the proposed method performance under the average SSIM score evaluation over various r, i.e. $r = \{2,3,\ldots,6\}$. The quality of shadow image and recovered cover image is reduced while applying a higher of r. However, the quality of recovered secret image is increased with higher r. The proposed method yields the best performance by setting $r = 4$ as demonstrated in Fig. 11. The proposed method effectively (k, n)-SS setting.

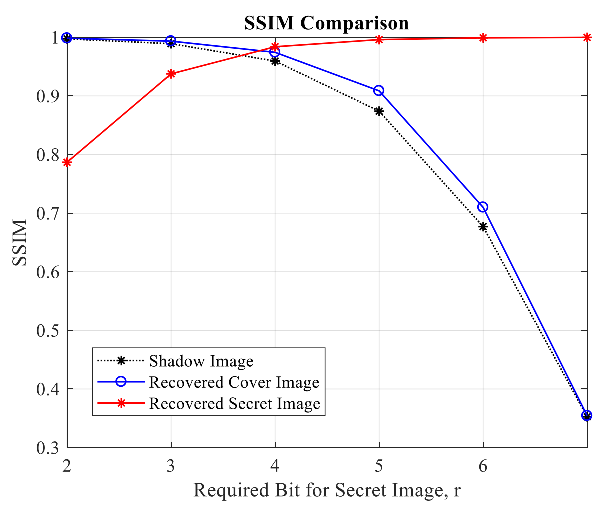


Fig. 11. Performance evaluations in terms of average SSIM score over various required bit for secret image

V. Conclusions

A simple solution for reducing the computational time for the former (k, n)-SS has been presented in this paper. The proposed method utilizes naive image compression to replace the color palette usage. This image compression is a straightforward approach to reduce the required bit of secret and cover image. The proposed method effectively produces a set of shadow images with a friendly appearance. In addition, it can recover the secret and cover images. For future works, the security level of the proposed method can be improved by involving image encryption or hashing functions. It can also be extended for secret video communication. The proposed method can also be applied to multiple secret sharing.

Acknowledgment

This work was fully funded by the Universitas Sebelas Maret (UNS), Indonesia, under the research grant "Hibah Penelitian Unggulan Terapan (PUT-UNS) Tahun Anggaran 2022" with the contract number 254/UN27.22/PT.01.03/2022.

References

[1] A. Shamir, "How to share a secret, " *ACM Communication*, vol. 22, no. 11, pp. 612-613, 1979.

[2] M. Naor M., and A. Shamir, "Visual cryptography," *Workshop on the theory and application of cryptographic techniques*, pp. 1-12, 1994.

[3] W. Yan, W. Ding, and Q. Dongxu, "Image sharing based on chinese remainder theorem," *Journal of North China University of Technology*, vol. 12, no. 1, pp. 6-9, (2000).

[4] H. Prasetyo, and C. H. Hsia, "Lossless progressive secret sharing for grayscale and color images," *Multimedia Tools and Applications*, vol. 78, pp. 24837–24862, 2019.

[5] A. Kanso, and M. Ghebleh, "An efficient lossless secret sharing scheme for medical images," *Journal of Visual Communication and Image Representation*, vol. 56, pp. 245-255, 2018.

[6] C. N. Yang, C. E. Zheng, M. C. Lu, and. X. Wu, "Secret image sharing by using multi-prime modular arithmetic," *Signal Processing*, vol. 205, 2023.

[7] X. Jia, Y. Guo, X. Luo, D. Wang, and C. Zhang, "A perfect secret sharing scheme for general access structures," *Information Sciences*, vol. 595, pp. 54-69, 2022.

[8] Y. Liu, C. N. Yang, S. Wu, and Y. Chou, "Progressive (k,n) secret image shading schemes based on Boolean operations and covering codes," *Signal Processing: Image Communication*, vol. 66, pp. 77-86, 2018.

[9] H. Prasetyo, D. Rosiyadi, and S. J. Horng, "Modified generalized random grids-based progressive secret sharing with lossless ability for binary image," *in Proc. International Conference on Computer, Control, Informatics and its Applications (IC3INA 2018)*, Tangerang, Indonesia, 2018.

[10] H. Prasetyo, C. H. Hsia, and A. W. H. Prayuda, "Progressive secret sharing with adaptive priority and perfect reconstruction," *Journal of Imaging*, vol. 7, no. 4, 2021.

[11] H. Prasetyo, C. H. Hsia, and J. Y. Deng, "Multiple secret sharing with simple image encryption," *Journal of Internet Technology*, vol. 21, no. 2, pp. 323-341, 2020.

[12] H. Prasetyo, C. H. Hsia, "Improved multiple secret sharing using generalized chaotic image scrambling," *Multimedia Tools and Applications*, vol. 78, no. 20, pp. 29089-29120, 2019.

[13] H. P., J. M. Guo, "A note on multiple secret sharing using Chinese remainder theorem and exclusive-OR," *IEEE Access*, vol. 7, pp. 37473-37497, 2019.

[14] J. M. Guo, D. Riyono, H. Prasetyo, "Improved beta chaotic image encryption for multiple secret sharing, " *IEEE Access*, vol. 6, pp. 46297-46321, 2018.

[15] H. Prasetyo, and D. Rosiyadi, "Converting (n, n)-multiple secret sharing into more friendly appearance using chinese remainder theorem and boolean operations," *in Proc. International Symposium on Electronics and Smart Devices (ISESD)*, pp. 1-6, 2021.

[16] C. N. Yang, P. Y. Tsai, and Y. Liu, "A (k,n) secret document sharing with meaningfull shares," *Journal of Information Security and Applications*, vol. 62, 2021.

[17] H. Prasetyo, and J. W. Simatupang, "XOR-ed Based Friendly-Progressive Secret Sharing," *in Proc. International Symposium on*

Intelligent Signal Processing and Communication Systems (ISPACS 2019), Taipei, Taiwan, 2019.

[18] H. Prasetyo, C. H. Hsia, C. Yu, and A. R. Wirawan, "Friendly Appearance of Multiple Secret Sharing," *in Proc. IEEE International Conference on Consumer Electronics-Taiwan (ICCE-Taiwan 2020)*, Taipei, Taiwan, 2020.

[19] J. Cheng, X. Yan, L. Liu, Y. Sun, and F. Xing, "Comprehensive reversible secret image sharing with palette cover images," *Journal of Information Security and Applications*, vol. 68, 2022.

[20] B. Harjito, and H. Prasetyo, "False-positive-free GSVD-based image watermarking for copyright protection," *in Proc. International Symposium on Electronics and Smart Devices (ISESD 2016)*, Bandung, Indonesia, 2016.