ICIC Express Letters
Volume **16**, Number **3**, March **2022**
 ISSN 1881-803X
pp. **307–315**

ANALYZING THE IMPACT OF THE SECRET SHARING ON STEGO IMAGES

Chaidir Chalaf Islamy[1,2] and Tohari Ahmad[1,*]

[1]Department of Informatics
Institut Teknologi Sepuluh Nopember
Kampus ITS, Surabaya, Jawa Timur 60111, Indonesia
7025201003@mhs.its.ac.id; *Corresponding author: tohari@if.its.ac.id

[2]Department of Informatics
Universitas 17 Agustus 1945 Surabaya
Semolowaru No. 45, Surabaya, Jawa Timur 60118, Indonesia

Received April 2021; accepted July 2021

Abstract. *The improvement of information transmission technology not only benefits our day-to-day life but also causes a risk in privacy and data security. There are two commonly used methods to protect the transmitted data, cryptography and data hiding. In this paper, we analyze the combination of these two methods to secure data. For the data hiding method, we utilize the histogram of the prediction error (PE) to embed data. We use Shamir's secret sharing to secure the produced stego image further. After that, we measure the quality of the share images. The result of the experiment shows that the quality of the generated shares relies on the number of generated images and the number required to reconstruct the stego image.*
Keywords: Data hiding, Secret sharing, Security, Data protection

1. **Introduction.** In the era where multimedia data were constantly transmitted through the Internet, it is essential to protect the transmitted data with a secure method. Without a reliable and robust security system, important and confidential data can be stolen, attacked, or changed at will. The information security system is broadly divided into two main categories: cryptography and data hiding [1,2]. Both methods are intended to protect the information, but their mechanism is different.

In cryptography, the way how the information is secured is by transforming it to have a randomized encrypted form. This scheme is appropriate for transmitting confidential data in a secure channel as it is inconceivable by the public. It is beneficial for communication in a public network. Since the transformed data are produced using methods involving variations and exchanges, illegitimate users may not gain access to the plain message.

Unlike cryptography, the data hiding method does not change the secret message format but embeds it into distortion-sensitive multimedia cover. It must be extracted from the embedded media cover or the stego cover to access the protected data. There are two ways to recover the embedded data: reversible or irreversible. The original cover can be entirely recovered in a reversible method; while in a non-reversible, they cannot be extracted to the original condition [1]. The application of the reversible techniques is suitable when the details of the cover are essential. In comparison, the irreversible method is convenient for systems where essential information in the cover media does not need to be retrieved. The cover medium used in this method includes audio [3], image [4] and video.

Besides using those two methods, the data can be altered to conceal the original secret message to secure the data further. It is done by partitioning the data into some segments, which can be restored later to acquire the original data. We employ a method provided

DOI: 10.24507/icicel.16.03.307

by Shamir [5], which is known as Shamir secret sharing scheme. Combining this scheme and data hiding is intended to obtain a mechanism capable of protecting data security.

In this paper, we implement secret sharing for reversible data hiding in images. Secret data are embedded in the cover image using histogram utilization and error value difference. The rest of this paper is presented as follows. Section 2 briefly describes the related methods. The proposed model, which implements histogram utilization and prediction error combined with secret sharing, is given in Section 3. Experimental results and analysis on the difference between the stego images generated by secret sharing and their corresponding image are presented in Section 4. Lastly, we draw the conclusions in Section 5.

2. **Literature Review.** Shamir secret sharing's main idea is to separate data into some fragments to access the original data; the separated data are then rejoined. To elaborate, the original data are put into n shares, which are distributed to different users. To access or reconstruct the original data successfully, there must be at least k of them, where $n \geq k$. The original data can be reconstructed with k or more shares, but if the collected shares $k-1$ or less give no clue of the original data. This process can be described in (1), where H is the secret message and d is the random coefficients.

$$F(x) = H + d_1 x + d_2 x^2 + \cdots + d_{(k-1)} x^{(k-1)} \tag{1}$$

Once k or more shares are obtained, a polynomial interpolation algorithm such as Lagrange can reconstruct coefficients H and $d_1, \ldots, d_{k-1}$ of $F(x)$; therefore, the secret message H can be discovered. It is worth noting that if only less than k shares can be obtained, the k unknown coefficients cannot be found; so, the H cannot be generated. Because the secret data is an image, H can also resemble a pixel of the secret image. It can be described as $H = I$, where I is the pixel of the secret image.

Data hiding or steganography is another layer of protection of the secret message. Few things must be noted when implementing a data hiding method on an image, imperceptibility or quality of the stego image, capacity of the private data, robustness, and security [1]. Steganography can be performed on several media covers, such as audio [3], image [4] and video [6]. Numerous methods have been developed to improve the quality of the stego image and the capacity of secret data. On spatial domains, the steganography method can be classified into three groups: compress-and-append, histogram shifting (HS)-based and expansion-based (EB) [7]. The compress-and-append technique is generally used in the earlier incarnation of reversible data hiding system. The EB-based scheme, known as difference expansion (DE), is initially established by Tian [8]. It takes advantage of the differences of nearby pixels of an image. Another steganography method based on EB is prediction error expansion (PEE), established by Thodi and Rodríguez [9]. It uses differences between the original pixel and the error value of the original pixel.

The HS-based scheme was first researched by Ni et al. [10]. This method's main idea is to select the most frequent pixel of the image as a reference to embed data. The process of embedding data is divided into three phases. First, searching for the most frequent pixel and least frequent pixel in the cover image, it can be done quickly by creating a cover image histogram. In this histogram, the most frequent pixel is that with the highest peak or peak pixel, and the least frequent pixel is the minimum or sometimes zero pixels because that particular pixel number does not exist in the cover image. Then, shift all pixels between the peak and minimum pixels. In doing so, there is one pixel left empty. The next step is filling it with pixels from the neighbors. The phase of shifting pixels is explained in (2), and the embedding data phase can be described in (3). Here, the peak pixel is P, and the minimum pixel is L; I is the pixel before being shifted; I' is the pixel that has been shifted; i and j are the pixel location. Then $b(n)$ is secret bits, where n is an index of secret bits.

$$I'_{i,j} = \begin{cases} I_{i,j} + 1 & \text{if } P + 1 \leq I_{i,j} \leq L - 1 \text{ and } P < L \\ I_{i,j} - 1 & \text{if } L + 1 \leq I_{i,j} \leq P - 1 \text{ and } P > L \end{cases} \tag{2}$$

$$I''_{i,j} = \begin{cases} I'_{i,j} + 1 & \text{if } I'_{i,j} = P \text{ and } b(n) = 1,\ P < L \\ I'_{i,j} - 1 & \text{if } I'_{i,j} = P \text{ and } b(n) = 1,\ P > L \\ I'_{i,j} & \text{if } I'_{i,j} = P \text{ and } b(n) = 0 \end{cases} \tag{3}$$

We can see in (2) that embedding operation can only occur as many as the number of the peak pixels. It has become the drawback of this scheme because the peak pixel (P) frequencies limit the total capacity. If the cover image has an even distribution of pixel color, it will impact the hiding capacity.

Another scheme developed by Hong et al. [11] also employed an HS and combines them with EB. However, before the embedding process occurs, they change the cover image into a prediction error (PE). They insert it with the help of the histogram produced by PE. This resulting stego image has better quality than that of EB and HS schemes, and the major drawback of HS can be mitigated. A histogram is used as a reference for the embedding phase, or the PE histogram can provide a higher number of pixel frequencies. This method is also used and further refined in [12-14].

Islamy and Ahmad [15] also developed a method based on the utilization of histogram and PE. This method provides better stego image imperceptibility than some previous works. Like [11], before the embedding phase, the original cover image is transformed into PE. The next step is to generate the histogram of the PE value and divide it into partitions. After that, the peak value of each partition is selected as a reference to embed data. Subsequently, more peaks can be used as a reference to embed data, which leads to an increase in data capacity. The overall process of this method can be described in Figure 1.

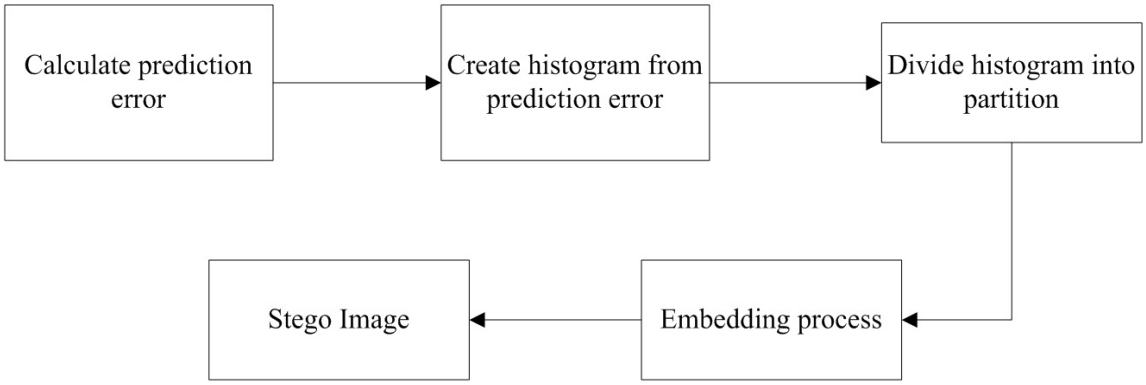


FIGURE 1. The embedding process of [15]

Wu et al. [16] proposed a Shamir secret share-based steganography scheme. This method focuses on the application of data privacy in cloud computing. In this scheme, the original image is encrypted using Shamir secret sharing. The produced shares are then embedded using both DE and HS schemes. Because the embedding phase occurred after the original image divided into encrypted n shares, the embedding capacity is greatly improved.

3. **Proposed Method.** In the previous section, we have concentrated on several methods that utilize HS and DE with their extensions and improvements. Along with those methods, we also discussed the use of the Shamir secret sharing method and how it works when combined with the steganography method. The Shamir secret sharing method can provide better security of the secret message, but there is also a drawback regarding imperceptibility since the produced shares are in encrypted form.

The proposed method is established based on that earlier research explained in Section 2. The proposed method is related to that in [15] and consists of several phases. Those are the initialization phase, where the calculation of PE takes place, and the histogram partition process and the embedding phase, where data are embedded into PE according to the reference value. In this paper, however, the secret-sharing phase is added after the initialization and embedding phases. The flow of this process can be seen in Figure 2.

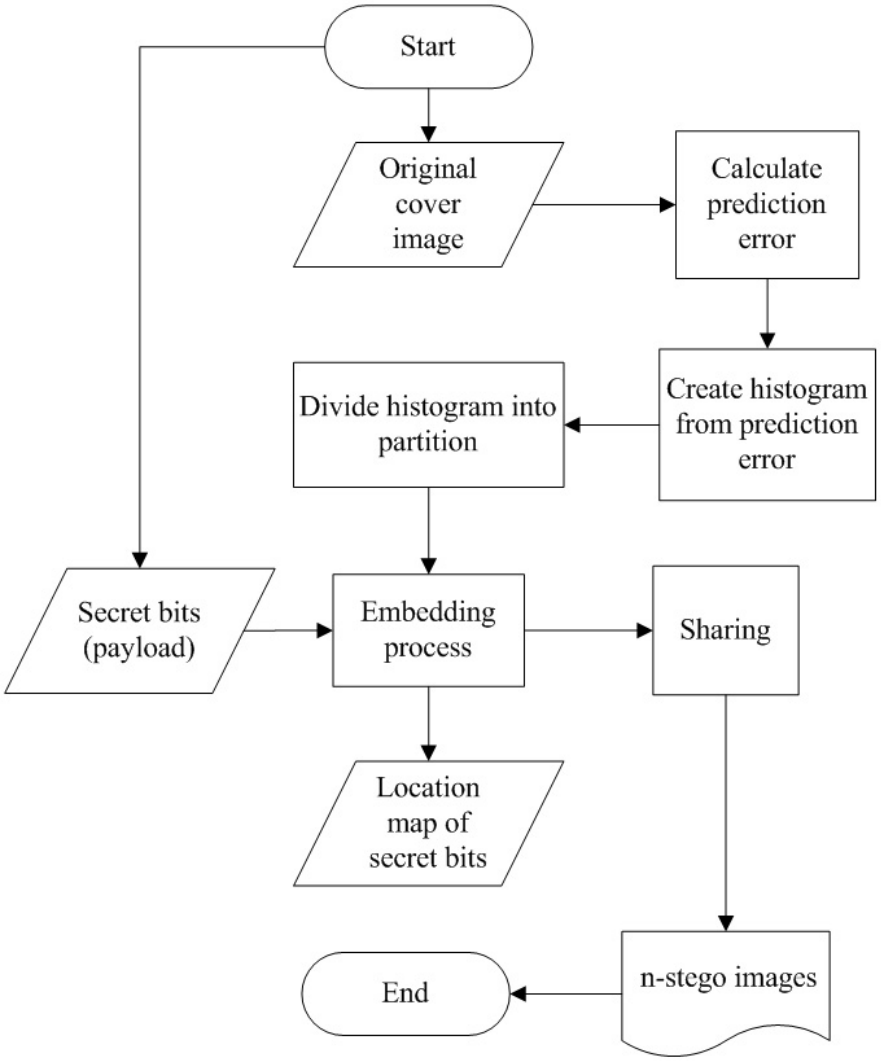


FIGURE 2. Process of data embedding and stego image sharing

3.1. **Initialization.** In this phase, the original cover image is converted into PE by using a predictor. We use a median edge detector (MED) to calculate the error value of each pixel of the image. This process can be presented in (4), where I is the original pixel value and $\hat{I}$ is the calculated error value. PE value E is obtained after implementing (5). Generate the histogram of PE value, and then allocate the histogram into partitions by using (6), (7) and (8), where Y is the PE value range, F is the number of the partitions, p^n is the allocated partition. Figure 3 depicts the process of data embedding using the partitioned histogram.

$$\hat{I}_{i,j} = \begin{cases} \min\left(I_{i,j-1}, I_{i-1,j}\right) & \text{if } I_{i-1,j-1} \geq \max\left(I_{i,j-1}, I_{i-1,j}\right) \\ \max\left(I_{i,j-1}, I_{i-1,j}\right) & \text{if } I_{i-1,j-1} \leq \min\left(I_{i,j-1}, I_{i-1,j}\right) \\ I_{i,j-1} + I_{i-1,j} - I_{i-1,j-1} & \text{otherwise} \end{cases} \tag{4}$$

$$E_{i,j} = I_{i,j} - \hat{I}_{i,j} \tag{5}$$

$$Y = P - L + 1 \tag{6}$$

$$F = 256/2^{\lceil \log_2 X \rceil} \tag{7}$$

$$p = \left\{p^1, p^2, p^3, \ldots, p^F\right\} \tag{8}$$

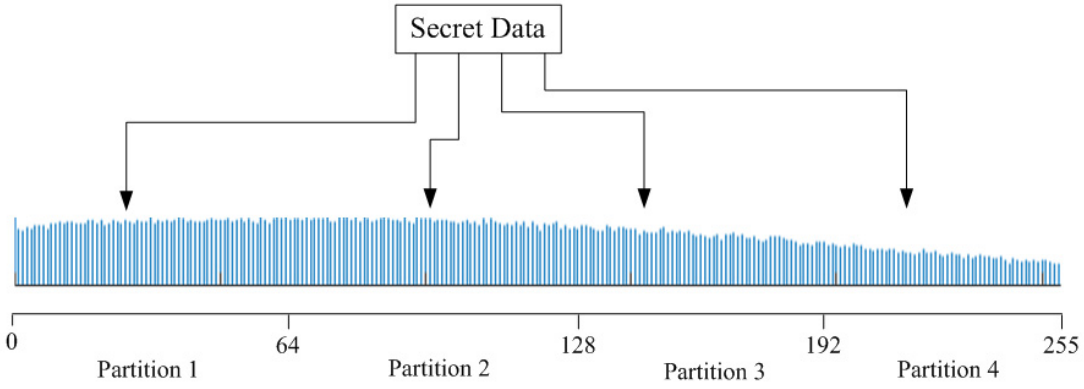


FIGURE 3. The illustration of the embedding process using the partitioned histogram

3.2. **Embedding.** The steps that occurred during the embedding phase are similar to those in [15]. This process is applied in each partition and is presented as follows.

- Scan the secret bits, and check the two neighboring bits to find a pair. There are four pairs of secret bits, which are $(0,0)$, $(0,1)$, $(1,0)$ and $(1,1)$.
- Check the peak value of the current partition P_C^n , the lowest value of the partition $C_{\min}^n$ and the highest value of the partition $C_{\max}^n$.
- As explained in [15], the position to embed the secret bits depends on P_C^n, $C_{\max}^n$, $C_{\min}^n$ and their pair.
- After the position has been found, then change the value by decreasing or increasing it by 1.
- Add the location of the PE value to the location map. The location map here provides another layer to secure the secret bits and we will need it in the extraction process.
- After all the secret bits have been embedded, change the PE value to pixel value by using (9).

$$I'_{i,j} = \hat{I}_{i,j} - E'_{i,j} \tag{9}$$

3.3. **Secret sharing.** After the embedding process has been done, Shamir secret sharing is used to split the stego image into parts. Pixel values of the stego image are converted into base 255 by performing modulus 255 to each pixel value. The modulus process is implemented in (1), which becomes (10), where $I'_{i,j}$ is the pixel of the stego image.

$$F(x) = \left(I'_{i,j} + d_1 x + d_2 x^2 + \cdots + d_{k-1} x^{k-1}\right) \bmod 255 \tag{10}$$

The resulted value from (3) is used as a new pixel value in the n shared images. Those pixel values are combined to form an image. At the end of this operation, there will be n images generated.

3.4. **Extraction.** This process is intended to retrieve the secret data which have been hidden previously. The overall extraction process is the inverse of the embedding procedure. First, we must reconstruct the stego image that can be done after at least k images have been obtained. Next, we calculate the value of $F(x_1), F(x_2), F(x_3), \ldots, F(k)$. From these values, we have pairs of $(x_1, F(x_1)), (x_2, F(x_2)), (x_3, F(x_3)), \ldots, (x_k, F(x_k))$. The formula in (1) is taken to obtain the stego image pixel values.

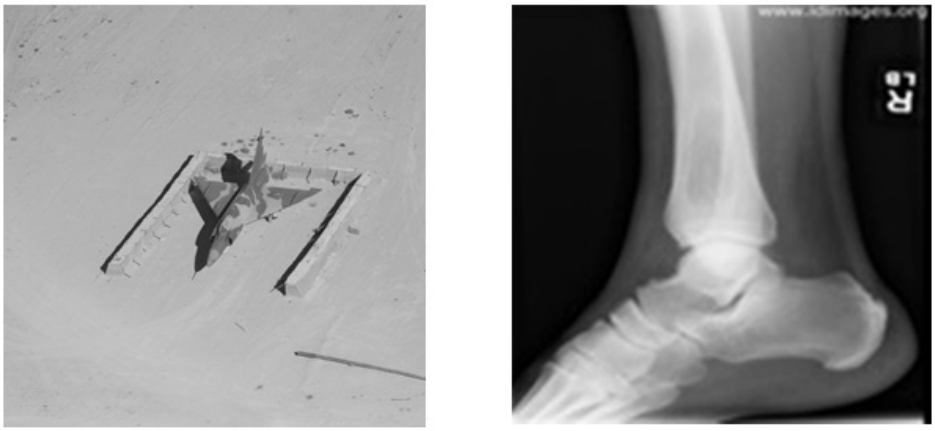
Once the stego image has been retrieved, we begin to extract the embedded data inside it. Here, the location map we obtain earlier is required to obtain the secret data and restore the original image completely. The extraction process follows similar steps as in [15].

4. **Experiment Results.** The experiment is conducted to evaluate the proposed method previously presented in Section 3. To evaluate the proposed method, we measure the share images' imperceptibility using the peak signal to noise ratio (PSNR). The mean square error (MSE) is first obtained using (11), where H and W are the image's height and width, respectively. This MSE value is taken by calculating the difference of total pixel value between the original cover image and the stego image. The lower MSE value indicates that the quality of the stego images is also lower. Then we use (12) to calculate PSNR, where I_{MAX} is the maximum value of the pixel in an image. PSNR measures the distortion level caused by the embedding and sharing process and detects any distinction between the original cover and stego images.

$$MSE = \left(\frac{1}{WH}\right) \sum_{i=1}^{W} \sum_{j=1}^{H} \left(I_{i,j} - I'_{i,j}\right)^2 \tag{11}$$

$$PSNR = 10 \log_{10} \frac{\left(I_{MAX}\right)^2}{MSE} \tag{12}$$

This experiment uses four standard test images and four medical images acquired from [17] and [18], each of which is an 8-bit grayscale image in 512×512 pixels. Test images are embedded with 20 Kb of secret bits, and then each of the images is processed with secret sharing under different scenarios. In the first scenario, all images are tested with $n = 2$, $k = 2$. For the second scenario, we set $n = 3$, $k = 2$, and lastly, we implement $n = 3$, $k = 3$. This measurement aims to analyze the effect of the difference between n and k in the PSNR value. Examples of test images are depicted in Figure 4, and the result of the experiment is given in Tables 1-6. From these tables, we find that the PSNR value of the generated share images is less than 30 dB, which is the standard for stego images [1]. It is because the secret-sharing heavily modifies the stego images, which themselves are the modified original cover images. The comparison between the original image and one of the shared images can be observed in Figure 4.



(a) (b)

FIGURE 4. Examples of test images: (a) Airplane image obtained from [17]; (b) leg medical image obtained from [18]

TABLE 1. PSNR of scenario 1 with $k = 2$ and $n = 2$ on general images

Image	**PSNR (dB)**	
	Share 1	**Share 2**
Aerial	13.69	9.00
Airplane	13.27	8.78
Pepper	13.34	8.78
Boat	13.21	8.68

TABLE 2. PSNR of scenario 1 with $k = 2$ and $n = 2$ on medical images

Image	**PSNR (dB)**	
	Share 1	**Share 2**
Hand	14.13	9.19
Chest	14.37	9.27
Head	14.46	9.28
Leg	14.19	9.21

TABLE 3. PSNR of scenario 2 with $k = 2$ and $n = 3$ on general images

Image	**PSNR (dB)**		
	Share 1	**Share 2**	**Share 3**
Aerial	13.67	8.98	7.22
Airplane	13.28	8.80	7.32
Pepper	13.34	8.78	7.30
Boat	13.23	8.69	7.32

TABLE 4. PSNR of scenario 2 with $k = 2$ and $n = 3$ on medical images

Image	**PSNR (dB)**		
	Share 1	**Share 2**	**Share 3**
Hand	14.13	9.19	7.14
Chest	14.35	9.26	6.99
Head	14.46	9.29	6.97
Leg	14.19	9.21	7.08

TABLE 5. PSNR of scenario 2 with $k = 3$ and $n = 3$ on general images

Image	**PSNR (dB)**		
	Share 1	**Share 2**	**Share 3**
Aerial	11.46	6.54	5.61
Airplane	11.20	6.72	5.89
Pepper	11.13	6.71	5.87
Boat	10.98	6.80	6.02

The average PSNR of share images are presented in Figures 5 and 6. From those results, we can see that for $n = 2$, $k = 2$, the PSNR values are a little bit higher than $n = 3$, $k = 2$, and $n = 3$, $k = 3$. This also indicates that for the same k, the overall PSNR values are better if the number of shares or n is higher. For the same n, the quality of the produced share images is, in general, higher for lower k. We can see in those figures, even though the difference is relatively small, the overall PSNR value with $k = 2$ is higher than that with $k = 3$.

TABLE 6. PSNR of scenario 2 with $k = 3$ and $n = 3$ on medical images

Image	PSNR (dB)		
	Share 1	Share 2	Share 3
Hand	11.74	6.36	5.32
Chest	11.86	6.07	4.87
Head	11.88	6.00	4.80
Leg	11.77	6.22	5.11

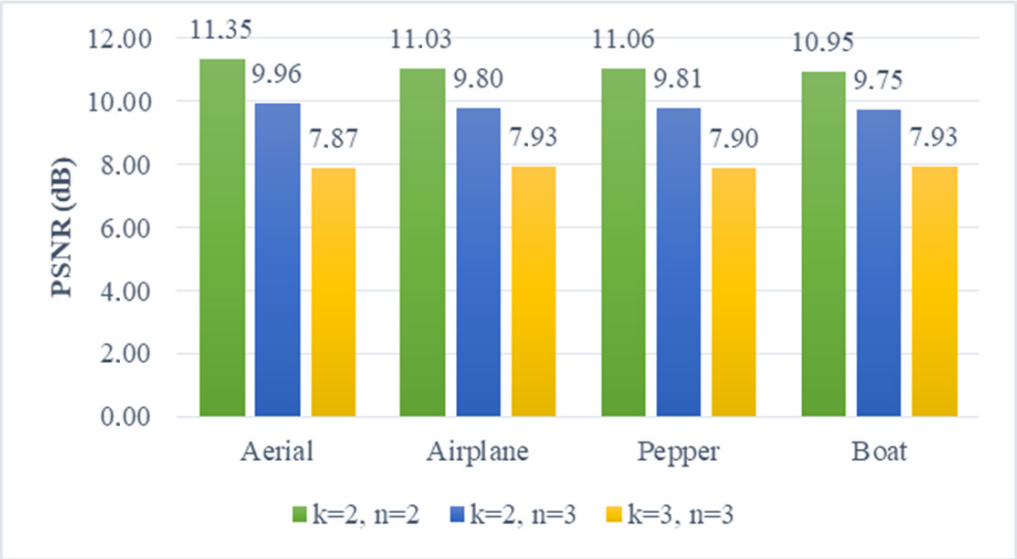


FIGURE 5. Average PSNR of share images using general images

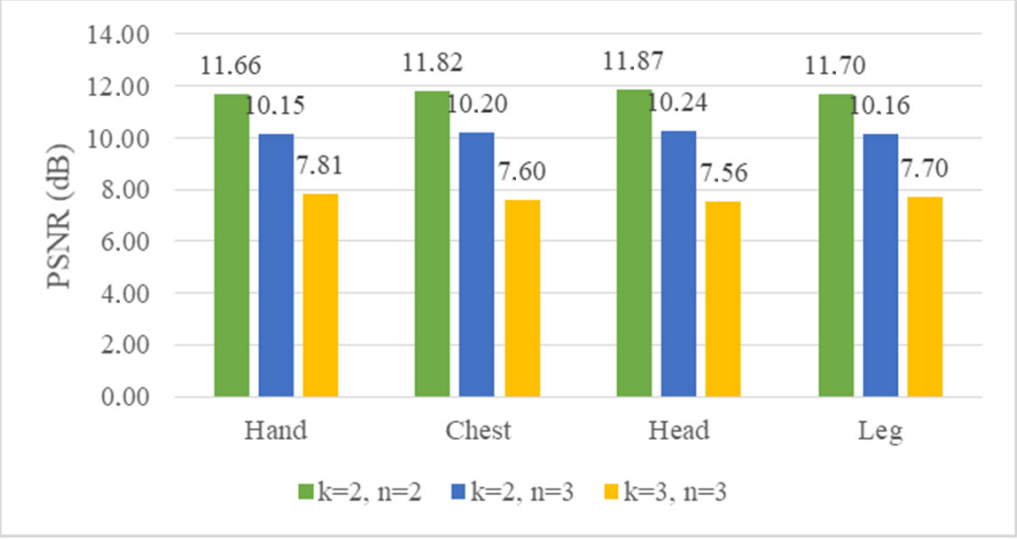


FIGURE 6. Average PSNR of share images using medical images

5. **Conclusions.** In this research, the concept of secret sharing is implemented for reversible image-based data hiding. Firstly, reversible data hiding using the PE and histogram modification is applied. Secondly, a method of Shamir secret sharing is implemented. To retrieve the embedded data, the stego image must be reconstructed by some participants by joining the share images together.

From the experimental results, we find that the more share produced, the more severe the distortion of the images. The more participants involved in reconstructing the stego

images, the higher the stego image quality. For the next research, we aim to increase the share images' quality, making them as close as possible to the cover image.

Acknowledgment. This work is funded and supported by Universitas 17 Agustus 1945 Surabaya.

REFERENCES

[1] I. J. Kadhim, P. Premaratne, P. J. Vial and B. Halloran, Comprehensive survey of image steganography: Techniques, evaluations, and trends in future research, *Neurocomputing*, vol.335, pp.299-326, 2019.

[2] M. Hussain, A. W. A. Wahab, Y. I. B. Idris, A. T. S. Ho and K.-H. Jung, Image steganography in spatial domain: A survey, *Signal Process. Image Commun.*, vol.65, pp.46-66, 2018.

[3] T. Ahmad and T. P. Fiqar, Enhancing the performance of audio data hiding method by smoothing interpolated samples, *International Journal of Innovative Computing, Information and Control*, vol.14, no.3, pp.767-779, 2018.

[4] P. Maniriho and T. Ahmad, High quality PVM based reversible data hiding method for digital images, *International Journal of Innovative Computing, Information and Control*, vol.15, no.2, pp.667-680, 2019.

[5] A. Shamir, How to share a secret, *Commun. ACM*, 1979.

[6] M. Suresh and I. S. Sam, Optimized interesting region identification for video steganography using fractional grey wolf optimization along with multi-objective cost function, *J. King Saud Univ. – Comput. Inf. Sci.*, 2020.

[7] R. M. Rad, K. S. Wong and J. M. Guo, Reversible data hiding by adaptive group modification on histogram of prediction errors, *Signal Processing*, vol.125, pp.315-328, 2016.

[8] J. Tian, Reversible data embedding using a difference expansion, *IEEE Trans. Circuits Syst. Video Technol.*, vol.13, no.8, pp.890-896, 2003.

[9] D. M. Thodi and J. J. Rodríguez, Expansion embedding techniques for reversible watermarking, *IEEE Trans. Image Process.*, vol.16, no.3, pp.721-730, 2007.

[10] Z. Ni, Y.-Q. Shi, N. Ansari and W. Su, Reversible data hiding, *IEEE Trans. Circuits Syst. Video Technol.*, vol.16, no.3, pp.354-362, 2006.

[11] W. Honga, T.-S. Chen and C.-W. Shiu, Reversible data hiding for high quality images using modification of prediction errors, *Journal of Systems and Software*, vol.82, no.11, pp.1833-1842, 2009.

[12] H. E. Prabowo and T. Ahmad, Adaptive pixel value grouping for protecting secret data in public computer networks, *J. Commun.*, vol.13, no.6, pp.325-332, 2018.

[13] H. Chen, J. Ni, W. Hong and T. Chen, High-fidelity reversible data hiding using directionally enclosed prediction, *IEEE Signal Process. Lett.*, vol.24, no.5, pp.574-578, 2017.

[14] J. Qin and F. Huang, Reversible data hiding based on multiple two-dimensional histograms modification, *IEEE Signal Process. Lett.*, vol.26, no.6, pp.843-847, 2019.

[15] C. C. Islamy and T. Ahmad, Enhancing quality of the stego image by using histogram partition and prediction error, *Int. J. Intell. Eng. Syst.*, vol.14, no.2, pp.511-520, 2021.

[16] X. Wu, J. Weng and W. Q. Yan, Adopting secret sharing for reversible data hiding in encrypted images, *Signal Processing*, vol.143, pp.269-281, 2018.

[17] *SIPI Image Database*, http://sipi.usc.edu/database/database.phpvolume=misc, Accessed on 01-Mar-2021.

[18] *eMicrobes Digital Library*, http://www.idimages.org/images/browse/ImageTechnique/, Accessed on 01-Jun-2020.