Cybersecurity

RESEARCH

Open Access

Reversible data hiding based on histogram and prediction error for sharing secret data

Chaidir Chalaf Islamy, Tohari Ahmad* and Royyana Muslim Ijtihadie

Abstract

With the advancement of communication technology, a large number of data are constantly transmitted through the internet for various purposes, which are prone to be illegally accessed by third parties. Therefore, securing such data is crucial to protect the transmitted information from falling into the wrong hands. Among data protection schemes, Secret Image Sharing is one of the most popular methods. It protects critical messages or data by embedding them in an image and sharing it with some users. Furthermore, it combines the security concepts in that private data are embedded into a cover image and then secured using the secret-sharing method. Despite its advantages, this method may produce noise, making the resulting stego file much different from its cover. Moreover, the size of private data that can be embedded is limited. This research works on these problems by utilizing prediction-error expansion and histogram-based approaches to embed the data. To recover the cover image, the SS method based on the Chinese remainder theorem is used. The experimental results indicate that this proposed method performs better than similar methods in several cover images and scenarios.

Keywords Data hiding, Secret image sharing, Prediction error expansion, Histogram-based embedding, Network infrastructure

Introduction

The vast integration of the Internet of Things (IoT) in recent years has resulted in many aspects of people's activities being recorded and transmitted on the internet (Shambour and Gutub 2022). This technology is useful for people's daily lives, business, and health and helps create opportunities to solve problems that were previously impossible to overcome (Namasudra et al. 2020). Despite its positive impact, this technology is also accompanied by one weakness; it can invite potential disruption to the transmitted data and communications. That is why proper information security must be implemented to prevent any possibility of the data being accessed, stolen, or edited by illegal parties. Generally, there are two approaches to information security: cryptography and steganography. Both serve the same purpose but have different manners of achieving it. In cryptography, the main idea is to change the data into an incomprehensible and unreadable form (Kumar et al. 2021; Pavithran et al. 2022). Protecting data using this method typically indicates the importance of the encrypted data, creating a risk of disruption. However, this risk is minimalized in the latter method. In steganography, also known as data hiding, the confidential data are embedded into cover media (Kadhim et al. 2019); it does not change the data's format but keeps the data's presence secret (Ardiansyah et al. 2017). The nature of this approach can reduce the risk of attempts to disrupt the data because only the sender and the receiver know the significance of the transmitted data. A suitable data hiding method must prevent undesirable parties from realizing the data's presence. To that end, there are several essential aspects of suitable data hiding: imperceptibility, security, data

*Correspondence:
Tohari Ahmad
tohari@if.its.ac.id
Present Address: Department of Informatics, Institut Teknologi Sepuluh Nopember (ITS), Kampus ITS Keputih Sukolilo, Surabaya 60111, Indonesia

capacity, and robustness, which must be kept at an optimum level.

In data hiding, the protected data can be any binary file, while the cover is either a digital image, audio, video, or text file. Digital images are a popular medium for covering confidential data (Kamal and Islam 2019; Yao et al. 2020; Hassan and Gutub 2022) because of their relatively small size. For this reason, however, the maximum amount of embedded data is quite limited compared to audio and video. The payload size stored in the cover image affects the number of changes in the pixels of this cover. It reduces the quality of the produced stego image. While some degradation types are inevitable, they should be kept to a minimum and not be easily identified, especially by the human eye (Suresh and Sam 2022). Research may focus on different aspects of data hiding, like improving the payload capacity of the stego images and maintaining their imperceptibility (Kumar and Agrawal 2016; Chang et al. 2015) or increasing the quality of the stego images while still having a decent payload size (Islamy and Ahmad 2019). In some circumstances, the embedding method only focuses on improving the capacity of the embedded data (Yu et al. 2022a). This approach is gaining popularity because of the widespread use of cloud storage (Yu et al. 2022b). Generally, these methods are applied alongside cryptography, where the payload is embedded in the encrypted image.

The embedded data must be fully extractable from the cover image, which can be disposed of without returning it to its original state. However, in some conditions, we may need to restore the cover image after reconstructing the embedded data; this scheme is called Reversible Data Hiding (RDH) (Cheddad et al. 2010; Kar et al. 2018). The RDH method is established around the expansion of pixel values. It can be divided into three major types: Differential Extension (DE), Histogram Shifting (HS), and Prediction-Error (PE) (Rad et al. 2016).

The DE method (Tian 2003) employs the difference and the integer average in a pixel block of an image to embed the data. This scheme is further improved by Dragoi and Coltuc (2014) by adding a local prediction-based DE. In that scheme, PE values are generated by calculating the least-squares predicted value of the pixel block, and then DE extends the PE value and embeds the data. The applications of the DE method can be observed further in (Al Huti et al. 2016; Niu et al. 2017; Prabowo and Ahmad 2018). On the other hand, the PE focuses on finding the predicted error value of the pixels. It is then utilized as the space for the payload (Thodi and Rodríguez 2007). This method is paired with the HS-based method to improve the quality of the stego images (Hong et al. 2009). In recent years, much research has used the prediction function to calculate the prediction error values, from which a histogram can be generated to embed the secret data (Hong et al. 2009; Rad et al. 2014; Luo et al. 2015; Kumar and Agrawal 2016; Yao et al. 2017; Kamal and Islam 2019). PE can also be implemented on the encrypted image (Tang et al. 2021), where the secret data are embedded using PE after the image has been encrypted.

Despite all signs of progress in information security methods, cryptography and steganography have a potential flaw in which only one party can access the secured data. This disadvantage can lead to misuse of the information or loss of the key in the case of encrypted data (Al-Shaarani and Gutub 2021). In order to minimize those problems, the Shamir's Secret Sharing method (1979) can be implemented to share secured data into parts and allocate them to different participants. In the case of image-based data hiding, it produces several shadows or shared images, known as Secret Image Sharing (SIS), which the corresponding participants retrieve. It is applicable in numerous cases and is responsible for securing the distribution and storage of digital images in a cloud environment. However, previous research shows (Islamy and Ahmad 2022) that those generated stego images have dropped in quality, affecting their imperceptibility.

Based on their robustness, data-hiding approaches can be categorized into two groups. The first is robust, which can withstand modifications, such as compression. The second one is non-robust that the stego image is damaged (un-recoverable) if there is a change. Both methods have advantages and disadvantages, all of which can be applied depending on the purpose. The non-robust is typically used in the spatial approach. This is intended to maintain the integrity of the stego image (Kadhim et al. 2019). That is, if the receiver can extract the payload and cover back to its origin, then the stego image is certainly not to experience an active attack. Meanwhile, to deal with passive attacks, like other research, is done by making the stego as similar as possible to the cover. This is also one of the objectives to be achieved in this research.

Considering those issues, this research aims to tackle the imperceptibility problem affecting the stego image by investigating both PE and HS methods, and utilizing the SIS technique. The remaining sections of this study are described as follows. "Related works" section discusses related research around data hiding and secret sharing. "Proposed method" section explains the proposed method, whose experimental results are analyzed in "Results and discussion" section. Finally, "Conclusion" section is presented to conclude the proposed method.

Related works

Secret sharing

The secret sharing technique divides data into n shares and circulates them among participants (Shamir 1979). In order to recover those original data, the dealer must at least retrieve k of them, where $k \leq n$. With that in mind, the original data can be restored if k or more shares are collected. However, it is not feasible to retrieve the original data if the collected shares are less than k since that collected information is not enough to recover the original data. This process can be calculated using the polynomial function in Eq. (1). In this function, h is the original data, while c is the random coefficient. When implemented on an image, h can be substituted for a pixel of the image or I.

$$F(x) = h + c_1 x + c_2 x^2 + \ldots + c_{k-1} x^{k-1} \tag{1}$$

The Lagrange function is utilized to restore the original data (h) and c_1, …, c_{k-1} of $F(x)$, after k or more shares are collected.

Histogram-based method

As the name suggests, this method is developed based on the utilization of image histograms (Ni et al. 2006). This histogram contains information that can help embed private data. Overall, there are three steps required to embed those data. The first step is searching for the most and least frequent pixels on the cover image, data that are easily obtainable from the histogram. The histogram's most frequent pixel can be recognized as the peak point, while the least frequent pixel is the lowest or the zero point. Then, all pixels positioned between the lowest and the peak points are 'shifted' to a new position leaving one pixel empty. It means that the shifted pixel's value is changed according to the location of the peak and lowest point pixels. Next, the empty pixel is utilized where the embedding process takes place. To embed the data, the empty pixel is gradually filled by the neighboring pixels, which indicates the total amount of private data in the number of bits. To fully understand these processes, let us define them in Eqs. (2) and (3), where the former is the pixel-shifting process, and the latter is the embedding process. In both equations, P and L are the peak and the lowest pixel points, respectively; I and I' are the pixel of the cover image before and after being shifted. The i and j notations indicate the pixel's position in a block; and lastly, $b(n)$ denotes the secret bits with n as the index.

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

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

From those equations, notice that the embedding process can only occur as much as the number of peak pixels. It shows that the capacity of the data is tied to peak pixel frequencies. This is a weak aspect of this method compared to others like the LSB and DE. For that reason, cover images with a high peak pixel frequency, such as medical images, are preferable when using this method.

Still related to this method, an improvement is proposed by Islamy and Ahmad (2021) to increase the quality of the stego image and also enhance the payload capacity. They use PE to expand the embedding capacity of HS, and the histogram is generated after the image pixels are transformed into an error value. The error value is categorized according to the corresponding histogram partitions, each with the peak and lowest error values. They also implement the payload distribution to increase the embedding capacity, increasing the embedded bits in an error value. Their experimental results show better image quality and capacity performance than previous research.

The combination of data hiding and secret image sharing

Wu et al. (2018) presented a combination of data hiding and SIS to protect data in the cloud computing environment. First, they use SS to encode the cover image and HS and DE to embed it. This method can significantly increase the embedded data size but decrease the stego images' quality. The SIS method is also utilized by Ahmad et al. (2014) to protect medical data inside medical images. In that algorithm, the cover image is separated using SS; then, the medical data are embedded into the share images using 1-bit LSB and 2-bit LSBs. Based on the experimental results, implementing 1-bit LSB yields better image quality, but the drawback is that it has lower data capacity. It needs a more extensive cover image to match the capacity of 2-bit LSBs, but a more extensive cover image size requires more bandwidth and storage.

In (2016), Yuan et al. proposed adjusting the threshold (k), which is beneficial if the security policy is changed or it is impossible to retrieve the required k. For instance, the remaining shares are useless if some participants are lost. To alleviate this problem, the proposed scheme has N probability of the potential thresholds t_1, t_2,…, t_N. Then they use the two-variable one-way function to create the identification value. The experimental results indicate

that the quality of the stego images is reasonable, and the threshold can be safely changed.

Another SIS-based method has been proposed by Yan et al. (2020). Instead of hiding information by applying Visual Secret Sharing (VSS) to polynomial-based SIS using screening operations, they implement an SIS scheme with different shadow authentication capabilities. That proposed scheme is less complex in generation and recovery (authentication) and does not have pixel extensions with different shadow authentication capabilities. In addition, lossless recovery is achieved without additional encryption.

Later, Meng et al. (2021) introduced a reversible extended secret image sharing (RESIS) scheme to secure data. That scheme is designed based on the implementation of the secret-sharing method by employing the Chinese Remainder Theorem (CRT) for a polynomial ring to turn confidential data into pieces of information. First, they define $m_0(x)$, which can be described in Eq. (4). The dealer picks four pixels in a block of 4×4 pixels and then utilizes 2-bits LSBs in those pixels to construct a polynomial $C(x)$ in Eq. (5). A pixel value of I is used in Eq. (6) to construct $D(x)$. A sharing function $F(x)$ is calculated in Eq. (7) to obtain the share values. The quality of the generated shared image, measured by the Peak Signal-to-Noise Ratio (PSNR), is over 40 dB.

$$m_0(x) = x^8 \tag{4}$$

$$C(x) = a_{i,1}x^0 + a_{i,2}x^1 + \ldots + a_{i,2}x^7 \tag{5}$$

Here, $a_{i,1}$ and $a_{i,2}$ are the least and the second least LSB of one of the pixels in a block.

$$D(x) = b_j x^0 + b_{j-1}x^1 + \cdots + b_{j-8}x^7 \tag{6}$$

In this case, b_j is the j-th LSB of I started from 8.

$$F(x) = C(x) + D(x)m_0(x) \tag{7}$$

Proposed method

The proposed embedding phase is generally shown in Fig. 1, consisting of three phases: initialization, embedding, and extraction. It also describes the complete flow of the proposed scheme to obtain the stego data from the initialization of the SS implementation.

Initialization

This initialization phase aims to prepare the cover image for embedding and set the parameter for the Secret Sharing method, which can be described in the following steps:

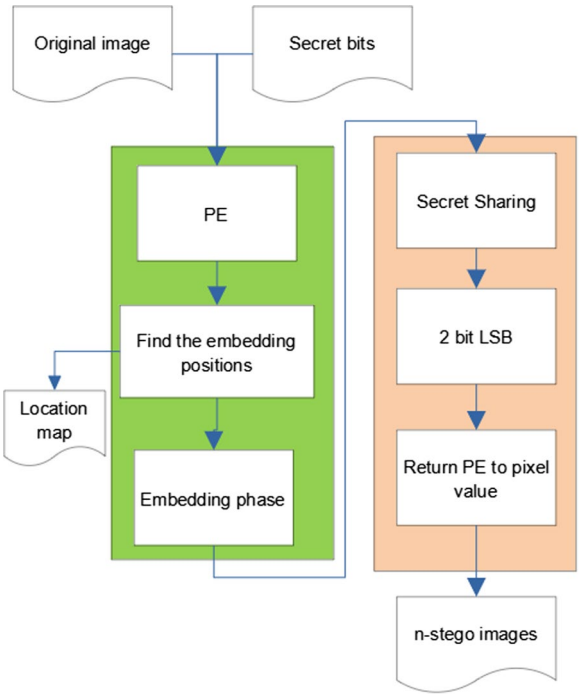

Fig. 1 The flow of the proposed method

1. First, transform the pixel values of the cover image into PE values by using a predictor. Prediction error refers to the difference between a specific pixel and the value that was estimated based on its surroundings. For this purpose, the median edge detector (MED) is utilized as the predictor to calculate the prediction value specified in Eq. (8). In that formula, $\hat{I}_{i,j}$ represents the prediction value of a pixel.

$$\hat{I}_{i,j} = \begin{cases} \min\ (I_{i,j-1}, I_{i-1,j}) \, if \, I_{i-1,j-1} \geq \max\ (I_{i,j-1}, I_{i-1,j}) \\ \max\ (I_{i,j-1}, I_{i-1,j}) \, if \, I_{i-1,j-1} \leq \min\ (I_{i,j-1}, I_{i-1,j}) \\ I_{i,j-1} + I_{i-1,j} - I_{i-1,j-1} \ otherwise \end{cases} \tag{8}$$

2. Calculate the difference between the original pixel and the generated prediction value using Eq. (9) to obtain the PE value ($E_{i,j}$).

$$E_{i,j} = I_{i,j} - \hat{I}_{i,j} \tag{9}$$

3. The dealer must set the total number of participants (n) and the minimum number required to restore the image (k).
4. The n predicted images are generated based on the total number of participants, which is set in step 3.

Furthermore, these images contain the SS pixels from the embedding phase.

Embedding phase

In the embedding phase, the secret bits are categorized into groups containing several bits, and each group has a different embedding position. In general, this phase scans the four leftmost secret bits and compares them with other groups, looks for a group having the same bit values, and then embeds the data by changing the value of the previously determined PE value. The embedding phase can be depicted in Fig. 2.

In detail, the steps proposed in the embedding phase are as follows:

1. First, search for the peak (P) of the PE or the most frequent PE value.
2. The secret bits are categorized into 16 groups, each consisting of four bits. The groups are formed based on all the possible combinations of those four bits. Each group has its embedding position,

Table 1 Secret bits group and its embedding position

Secret bits (b_1, b_2, b_3 and b_4)	Embedding position (ep)
1, 1, 1, 1	$P+1$
1, 1, 1, 0	$P+3$
1, 1, 0, 0	$P+5$
1, 0, 0, 0	$P+7$
0, 0, 0, 0	$P+9$
0, 0, 0, 1	$P+11$
0, 0, 1, 1	$P+13$
0, 1, 1, 1	$P+15$
1, 0, 1, 0	$P-1$
1, 0, 0, 1	$P-3$
1, 0, 1, 1	$P-5$
1, 1, 0, 1	$P-7$
0, 0, 1, 0	$P-9$
0, 1, 0, 0	$P-11$
0, 1, 1, 0	$P-13$
0, 1, 0, 1	$P-15$

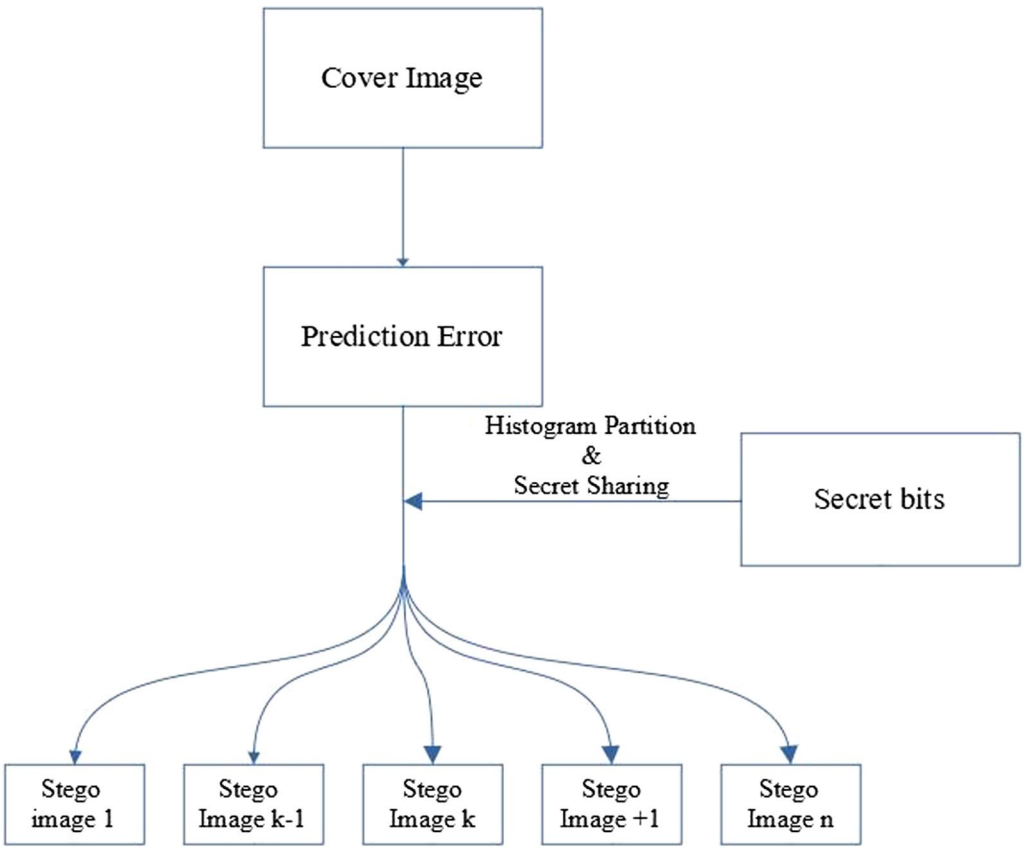

Fig. 2 The embedding phase illustration

explained in step 5. The list of the group and its corresponding position can be seen in Table 1.

3. Scan the secret bits (b_n) and pick the four leftmost: b_1, b_2, b_3, and b_4.
4. The number of embedding positions P_{ep} can be calculated using Eq. (10), where d is the number of bits in each secret bit group, as already described in step 2; so $d = 4$.

$$P_{ep}=2^d \tag{10}$$

5. Check the scan results in step 3 and compare them to the conditions presented in Eq. (11), then pick the embedding position or *ep*. The *ep* is the neighbouring PE value of P, and it corresponds to the secret bit groups. For example, if the scan results are $b_1 = 1$, $b_2 = 1$, $b_3 = 1$, $b_4 = 1$, then search the PE value of $P + 1$.

$$ep = \begin{cases} P+1 \; if \; b_1=1 \; and \; b_2=1 \; and \; b_3=1 \; and \; b_4=1 \\ P+3 \; if \; b_1=1 \; and \; b_2=1 \; and \; b_3=1 \; and \; b_4=0 \\ P+5 \; if \; b_1=1 \; and \; b_2=1 \; and \; b_3=0 \; and \; b_4=0 \\ P+7 \; if \; b_1=1 \; and \; b_2=0 \; and \; b_3=0 \; and \; b_4=0 \\ P+9 \; if \; b_1=0 \; and \; b_2=0 \; and \; b_3=0 \; and \; b_4=0 \\ P+11 \; if \; b_1=0 \; and \; b_2=0 \; and \; b_3=0 \; and \; b_4=1 \\ P+13 \; if \; b_1=0 \; and \; b_2=0 \; and \; b_3=1 \; and \; b_4=1 \\ P+15 \; if \; b_1=0 \; and \; b_2=1 \; and \; b_3=1 \; and \; b_4=1 \\ P-1 \; if \; b_1=1 \; and \; b_2=0 \; and \; b_3=1 \; and \; b_4=0 \\ P-3 \; if \; b_1=1 \; and \; b_2=0 \; and \; b_3=0 \; and \; b_4=1 \\ P-5 \; if \; b_1=1 \; and \; b_2=0 \; and \; b_3=1 \; and \; b_4=1 \\ P-7 \; if \; b_1=1 \; and \; b_2=1 \; and \; b_3=0 \; and \; b_4=1 \\ P-9 \; if \; b_1=0 \; and \; b_2=0 \; and \; b_3=1 \; and \; b_4=0 \\ P-11 \; if \; b_1=0 \; and \; b_2=1 \; and \; b_3=0 \; and \; b_4=0 \\ P-13 \; if \; b_1=0 \; and \; b_2=1 \; and \; b_3=1 \; and \; b_4=0 \\ P-15 \; if \; b_1=0 \; and \; b_2=1 \; and \; b_3=0 \; and \; b_4=1 \end{cases} \tag{11}$$

6. After the ep has been found, the secret bit can be embedded. Compare ep with P, if it is higher than P, increase it by 1; if it is lower than P, then reduce it by 1. Here, we take the same instance as the previous step and use $P + 1$, so add 1, and it becomes $P + 1 + 1$. Another example is, if the embedding position is lower than P, for instance $P-3$. To embed the secret bits, decrease it by 1, having $P - 3 - 1$. These steps can also be described in Eq. (12).

$$ep' = \begin{cases} ep+1 if \; (ep=P+1) or (ep=P+3) or (ep=P+5) or (ep=P+7) or \\ \quad (ep=P+9) or (ep=P+11) or (ep=P+13) or (ep=P+15) \\ \\ ep-1 if \; (ep=P-1) or (ep=P-3) or (ep=P-5) or (ep=P-7) or \\ \quad (ep=P-9) or (ep=P-11) or (ep=P-13) or (ep=P-15) \end{cases} \tag{12}$$

7. Scan the next four leftmost bits, and repeat steps 5 and 6 until all bits have been embedded.
8. The location map is used to save the location of ep' and it can be presented as LM_i, where i is the index of the LM_i. Each *ep* location is saved and used in the data retrieval process later.
9. The SS is implemented on the embedding position on ep' by using polynomials in Eqs. (4), (5), (6), and (7). Polynomial $D(x)$ stores the 8 bits of the ep', while 2 bits of LSB of the surrounding PE value of ep' are stored in $C(x)$. Finally, sharing polynomial $F(x)$ in Eq. (7) generates n share PE values.
10. Let the output of Eq. (12) be ep_i'', where i is the PE value of the i-th participant. The difference between ep_i'' and ep' is often quite large, and it can cause major distortion to the stego image if we substitute the value of *ep* with ep_i''. To mitigate this problem, ep_i'' is embedded by utilizing 2 bits of LSB and changing the PE values to binary bits. Then, split those binaries into four groups, each consisting of 2 bits. For instance, if the binaries are 11,101,011; the groups are (1, 1), (1, 0), (1, 0), and (1, 1).
11. Those binaries are embedded into the neighbour of the ep' of each predicted image and are located on the top, left, bottom and right of the p'. The position is formulated as $(i-1,j)$, $(i,j-1)$, $(i+1,j)$,

and$(i, j+1)$. The four pixels are calculated using Eq. (13), with b_i as the i-th bit of theep'.

$$\left.\begin{aligned} E'_{i-1,j} &= E_{i-1,j} - \left(E_{i-1,j} \bmod 2^t\right) + b_0 + b_1 \times 2 \\ E'_{i,j-1} &= E_{i,j-1} - \left(E_{i,j-1} \bmod 2^t\right) + b_2 + b_3 \times 2 \\ E'_{i+1,j} &= E_{i+1,j} - \left(E_{i+1,j} \bmod 2^t\right) + b_4 + b_5 \times 2 \\ E'_{i,j+1} &= E_{i,j+1} - \left(E_{i,j+1} \bmod 2^t\right) + b_6 + b_7 \times 2 \end{aligned}\right\} \tag{13}$$

12. Repeat steps 8–9 until all of the ep' are embedded into $E_{i-1,j}$, $E_{i,j-1}$, $E_{i+1,j}$,$E_{i,j+1}$
13. Next, return the PE values of each predicted image to pixel form by using Eq. (14), where $I'_{i,j}$ is the pixel value of the stego image, and $E'_{i,j}$ is the PE value after the embedding and sharing process.

$$I'_{i,j} = \hat{I}_{i,j} - E'_{i,j} \tag{14}$$

Extraction phase

The extraction phase restores the embedded secret data from the share images. To extract the secret data and restore the original cover image, at least k shared images are needed. In general, this process is the reverse step of the embedding process. This process is described in detail in the following step:

1. First, transform the image to PE values using Eq. (15) and identify P.

$$E'_{i,j} = \hat{I}_{i,j} - I'_{i,j} \tag{15}$$

2. With the help of LM_i obtained earlier, scan the PE value and compare it to LM_i. If the location of the scanned PE values matches LM_i, then identify the neighbour PE values.
3. To obtain ep''_i extract the share PE values of the stego image by employing the surrounding PE values using Eq. (16).

$$\begin{aligned} ep''_i = &\left(E_{i-1,j} \bmod 4\right) \times 2^0 + \left(E_{i,j-1} \bmod 4\right) \times 2^2 \\ &+ \left(E_{i+1,j} \bmod 4\right) \times 2^4 + \left(E_{i,j+1} \bmod 4\right) \times 2^6 \end{aligned} \tag{16}$$

4. Determine the value of $F(x_1)$, $F(x_2)$, $F(x_3)$, …, $F(k)$ by collecting at least k share images.
5. Next, Eq. (7) is implemented to retrieve ep' and its surrounding 2 bits of the LSB of the PE value.
6. To obtain the embedded bits, check their position related to P. For this purpose, use Eq. (11) to help understand the extracted bits.
7. Steps 2–5 are repeated until all secret bits are taken completely.

Table 2 The average PSNR (dB) of each k. on the general images

Image	$k = 3$	$k = 4$	$k = 5$	$k = 6$
Aerial	48.97	49.01	49.12	48.86
Airplane	51.90	49.02	49.06	48.95
Pepper	49.05	49.04	49.02	49.01
Male	49.07	49.03	49.05	49.06
Truck	51.28	50.99	51.19	51.04
Couple	50.45	50.16	50.08	50.14
Airport	49.20	49.19	49.15	49.21
Tank	47.67	47.56	47.48	
APC	48.16	48.15	48.13	
Fishing boat	49.06	48.99	49.01	48.89

Table 3 The average PSNR (dB) of each k on the medical images

Image	$k = 3$.	$k = 4$	$k = 5$	$k = 6$
Hand	53.36	53.56	53.26	53.24
Chest	53.55	53.63	53.53	53.64
Head	51.54	51.35	51.56	51.52
Leg	52.65	52.70	52.56	52.23
Abdominal	54.21	51.92	51.76	51.89
Left Lower Leg	53.25	53.19	53.16	53,.05
Lateral Neck	51.28	51.18	51.23	51.17
Right Knee	52.77	52.56	52.18	52.66
Left Wrist	53.15	53.18	53.09	53.05
Pelvis	54.32	54.16	54.17	54.11

8. After the data extraction and the PE value recovery processes have finished, the cover image is obtained using Eq. (17).

$$I_{i,j} = \hat{I}_{i,j} + E_{i,j} \tag{17}$$

Results and discussion

Experimental environment

In the experiment, ten general images and ten medical images are used as the test images. They are acquired from (USC-SIPI 2021) and (National Library of Medicine 2022), respectively, and have a resolution of 512×512 pixels. The experiments are applied using MATLAB 2017a on AMD Ryzen 5 3600 CPU with 16 GB memory.

In analyzing the quality of the stego images, the Peak Signal-to-Noise Ratio (PSNR) is used as a measurement. It works by calculating the noise level of an image; in this case, the noise is the difference between the original image and the stego image. The calculation of PSNR is carried out using Eqs. (18) and (19), where I_{MAX} is the image's highest pixel value, MSE is the mean square error,

and W and H are the width and height of the image in pixels, respectively.

$$\mathrm{MSE} = \left(\frac{1}{WH}\right)\sum_{i=1}^{W}\sum_{j=1}^{H}\left(I_{i,j} - I'_{i,j}\right)^2 \tag{18}$$

$$\mathrm{PSNR} = 10\log_{10}\frac{(I_{\mathrm{MAX}})^2}{\mathrm{MSE}} \tag{19}$$

Result analysis

The first experiment scenario tests the impact of the different k on the stego images, in which there are four tested k: 3, 4, 5, and 6, while the number of participants is 6. It is essential to notice that in all scenarios, we divide the results based on the type of cover images, general and medical; either one has different characteristics and can impact the results. For the secret data, we generate 131,072 bits, which is the maximum number of payload size can be held by (Yuan et al. 2016; Meng et al. 2021). It matches the number of bits of 128×128 pixels of a greyscale image (Islamy 2022). Table 2 shows the average PSNR value of stego images of each k tested in general cover images, while Table 3 provides it for the medical images. Data presented in these tables reflect that the average PSNR values of the stego images higher than 30 dB, render the images not visually distinguishable as they could be if the values are below 30 dB (Kyriakopoulos and Parish 2007). It shows that the threshold (k) does not significantly impact the quality of the resulting stego images. Then, a one-way analysis of variance (ANOVA) is performed to prove whether or not k affects the quality of the resulting stego image. We pick the probability value or p-value and compare it to the significance level (α). The primary interpretation of the p-value is whether or not there is enough evidence to reject the null hypothesis, which, in this case, is that k has no significant impact.

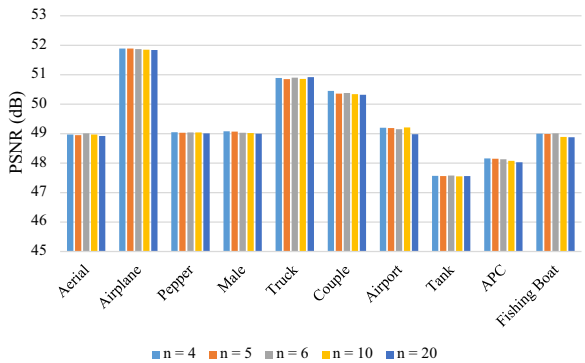

Fig. 3 The comparison of PSNR (dB) of general images with different n

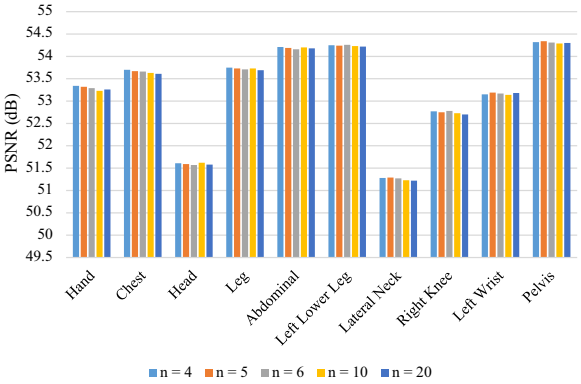

Fig. 4 The comparison of PSNR (dB) of medical images with different n

This test's significance level is 0.05 because it is considered conventional and the most commonly used. From the statistical test, the p-value of results in Tables 1 and 2 is 0.9999 and 0.9994, respectively. Both have more p-value than the α; this means the null hypothesis is proven to be correct, and statistically, there is no significant difference between different groups of k. There is no significant impact on the results because of the utilization of 2-bit LSB. So, the level of change in the PE value caused by the sharing process can be reduced. It can also be observed that the general image has a lower PSNR value than the medical images. It is found that medical images have more black pixels and a smaller overall variety of pixel colours; all these traits have helped them become more tolerant of change.

For the second scenario, the experiment was performed on a different number of participants (n), and then the average PSNR of each n was measured. In this scenario, the utilized k is 4, tested on n of 7, 8, 9, and 10 using the same secret bits as the previous scenario. It is performed in order to understand the effect of utilizing various n values. The result is presented in Figs. 3 and 4, where the former represents the general images while the latter is for medical images. It is found that the use of different n has minimal impact on the quality of the stego images. Again, to prove this statement, those results are calculated using one-way ANOVA. The p-value of Figs. 3 and 4 are 0.9999; both are more than the α. These results are identical to the previous scenario and show that there are not enough differences. Similar to the previous scenario, 2-bit LSBs help reduce the sharing process's impact.

Given the results from those two scenarios, one thing that should be noticed is how to decide the optimal combination of k and n. From the image quality standpoint, the dealer can use as many participants as possible and choose higher thresholds, as there is no noticeable impact on quality as provided in the previous analysis.

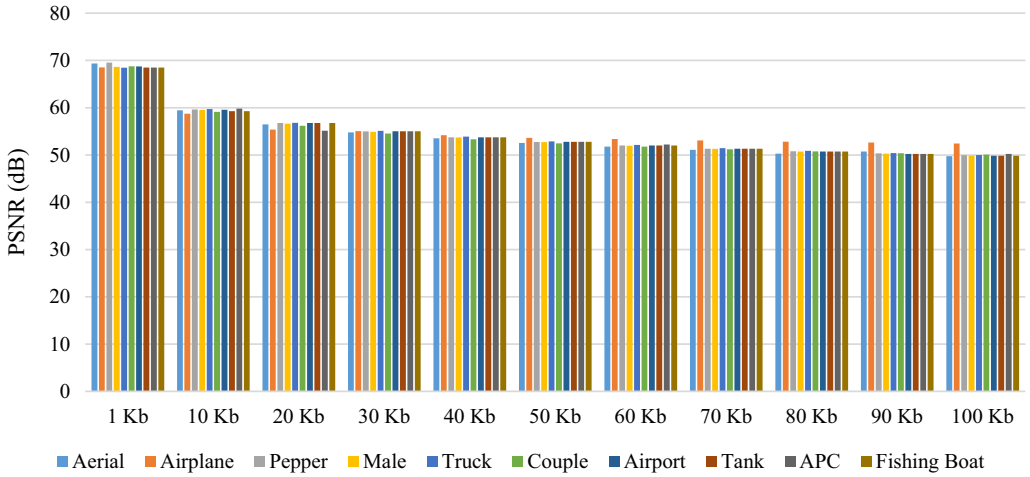

Fig. 5 The quality of the stego image when embedded with various data sizes on general image

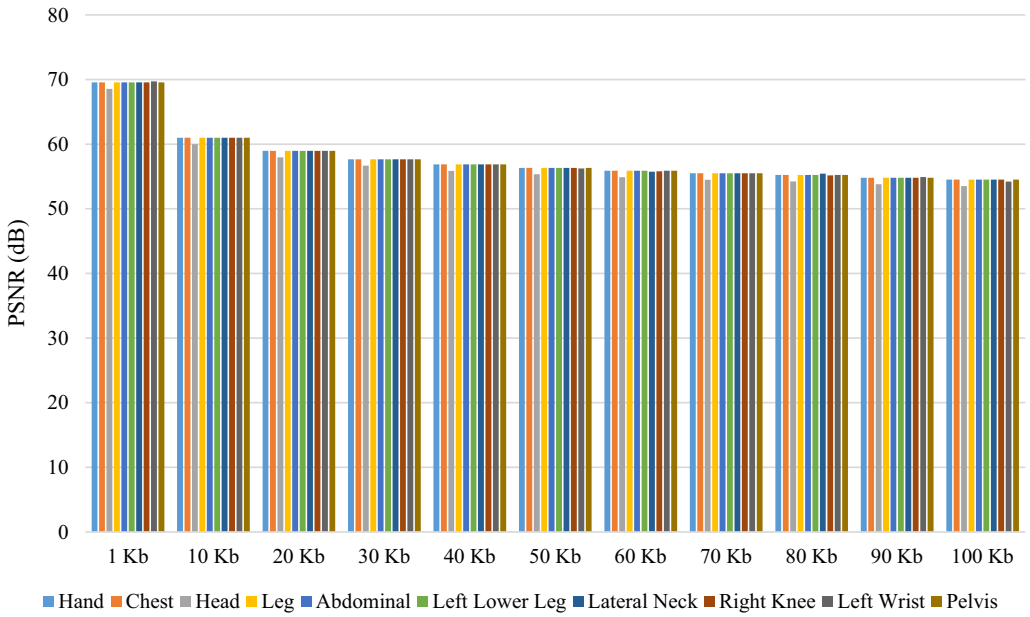

Fig. 6 The quality of the stego image when embedded with various data sizes on medical image

Furthermore, the more k and n means that it is harder for third parties to obtain the original data. Nevertheless, both values affect the complexity of the algorithm. A higher participant number involved in the sharing process increases the computation, representing linear growth complexity ($O(n)$). Therefore, theoretically, despite the PSNR results of $n = 4$ and $n = 20$ being similar, the lower number of n can produce a faster execution time.

In the third scenario, the proposed method is tested with various secret data sizes. There are eleven sizes of the secret data: 1 Kb, 10 Kb, 20 Kb, 30 Kb, 40 Kb, 50 Kb, 60 Kb, 70 Kb, 80 Kb, 90 Kb, and 100 Kb, obtained from (Islamy 2022). This scenario aims to understand the relationship between the embedding capacity and the quality of the stego images. In this scenario, n is 10 and k is 4. The average PSNR is measured for each data size, whose results can be found in Figs. 5 and 6 for general and medical images, respectively. Based on the results, it is found that the more data embedded in the cover image, the more the quality of the stego image decreases. Nevertheless, the quality reduction is getting smaller along with the rising payload size. For example, the PSNR of the general and medical images started to degrade less when embedded with more than 60 Kb of data. This means that the proposed method is suitable for embedding large amounts of data.

Table 4 The comparison of PSNR (dB) of the general images between the proposed method and previous works

Image	$k = 4$			$k = 5$			$k = 6$		
	Proposed scheme	Meng et al. (2021)	Yuan et al. (2016)	Proposed scheme	Meng et al. (2021)	Yuan et al. (2016)	Proposed scheme	Meng et al. (2021)	Yuan et al. (2016)
Aerial	49.01	44.17	40.12	49.12	44.14	40.10	48.86	44.13	40.02
Airplane	49.02	44.18	40.20	49.06	44.13	40.16	48.95	44.14	40.09
Pepper	49.04	44.15	41.01	49.02	44.16	40.90	49.01	44.15	40.87
Male	49.03	44.16	40.13	49.05	44.15	40.08	49.06	44.16	40.05
Truck	49.05	44.17	40.12	49.07	44.13	40.16	49.01	44.15	40.87
Couple	49.02	44.18	40.20	49.06	44.13	40.16	48.95	44.14	40.09
Airport	49.04	44.15	41.01	49.02	44.16	40.90	49.01	44.15	40.87
Tank	49.03	44.16	40.13	49.01	44.15	40.87	49.06	44.16	40.05
APC	49.02	44.18	40.20	49.02	44.16	40.90	49.01	44.15	40.87
Fishing Boat	49.06	44.15	40.01	49.05	44.17	40.08	48.86	44.13	40.02

Table 5 The comparison of PSNR (dB) of the medical images between the proposed method and previous works

Image	$k = 4$			$k = 5$			$k = 6$		
	Proposed scheme	Meng et al. (2021)	Yuan et al. (2016)	Proposed scheme	Meng et al. (2021)	Yuan et al. (2016)	Proposed scheme	Meng et al. (2021)	Yuan et al. (2016)
Hand	53.56	47.12	43.10	53.26	46.13	42.63	53.24	45.65	42.11
Chest	53.63	47.16	44.21	53.53	47.14	43.07	53.64	46.48	42.91
Head	51.35	49.02	44.52	51.56	46.15	43.89	51.52	47.17	42.73
Leg	52.70	48.38	43.05	52.56	47.16	44.05	52.23	47.13	42.67
Abdominal	53.63	47.16	44.21	51.56	46.15	43.89	53.63	47.16	44.21
Left Lower Leg	51.23	49.02	44.52	51.35	49.02	44.52	51.35	49.02	44.52
Lateral Neck	52.50	48.38	43.05	53.64	46.48	42.91	53.53	47.14	43.07
Right Knee	51.55	46.14	43.89	51.52	46.17	42.73	51.56	46.15	43.89
Left Wrist	52.56	49.06	44.05	51.35	49.02	44.52	51.35	49.05	44.52
Pelvis	52.64	46.48	42.91	52.70	46.38	43.01	52.70	46.44	43.05

Table 6 Comparison of functionality between the proposed method and previous works

Functionality	The proposed method	Meng et al. (2021)	Yuan et al. (2016)
Lossless secret data	Yes	Yes	Yes
Lossless cover image	Yes	Yes	No
Meaningful stego image	Yes	Yes	Yes
Sharing method	CRT-SS	CRT-SS	SS with adjustable Threshold
Embedding	Payload distribution using PE Histogram and 2-bit LSB	2-bit LSB	2-bit LSB

The stego image quality of the proposed method is compared with earlier work (Yuan et al. 2016; Meng et al. 2021) and is shown in Tables 4 and 5. The secret data used in this fourth scenario is the same as in the first and second scenarios. The results indicate that the proposed method has a better PSNR value than existing methods with the same amount of payload. It is worth noting that in the proposed method, we calculate the PE value first and then embed the data. The sharing process is implemented within the embedded PE value. It has been found that instead of the actual image pixels, the sharing process occurs within the PE value of the cover image. Afterwards, the value generated from the sharing process is embedded into its neighbour through 2-bit LSBs. Because of that, the embedding space of the proposed method does not depend on the cover image size.

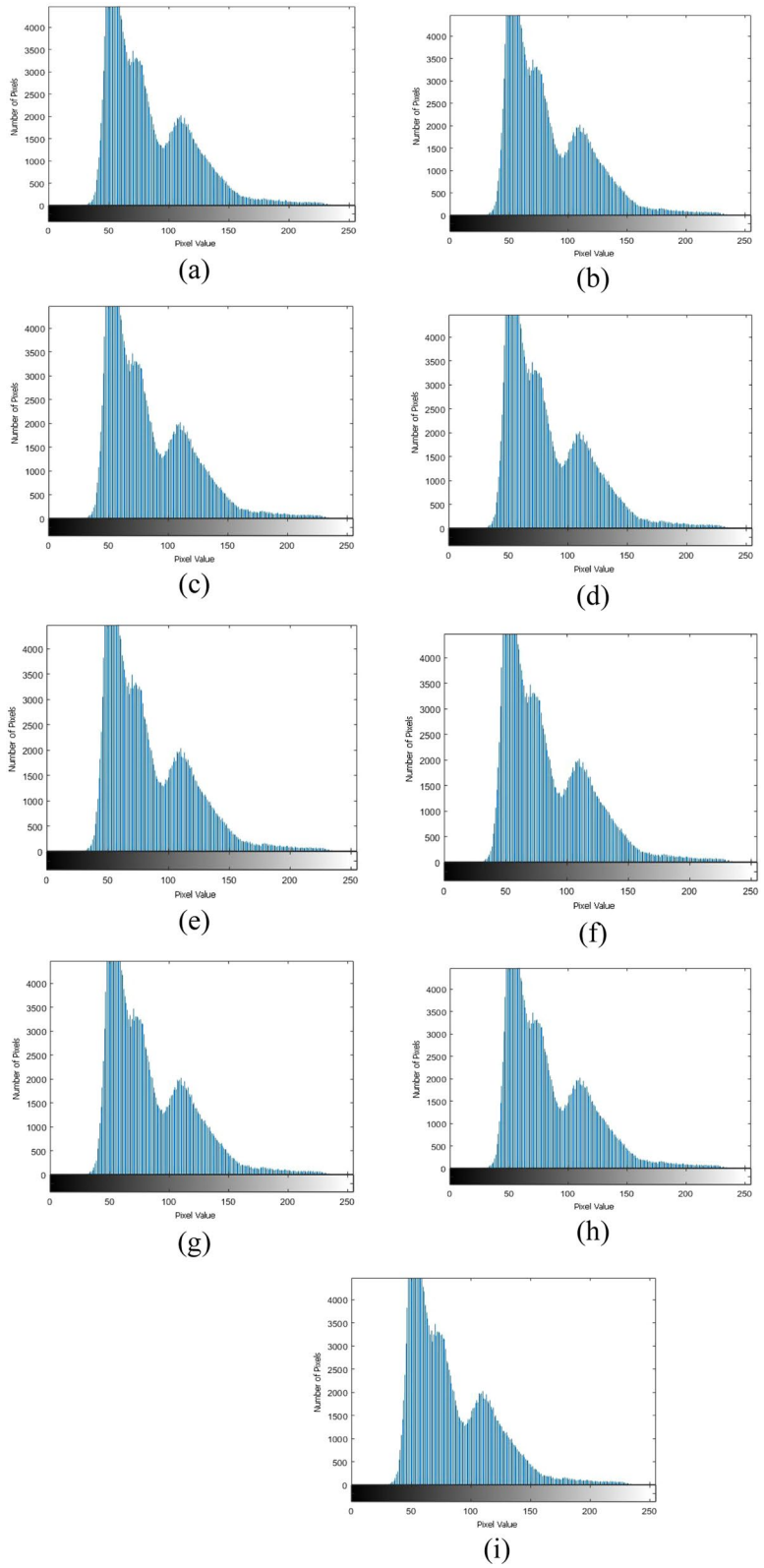

Fig. 7 The histograms of the original Airport image and the stego images: **a** original, **b** stego 1, **c** stego 2 **d** stego 3, **e** stego 4, **f** stego 5, **g** stego 6 h stego 7, **i** stego 8

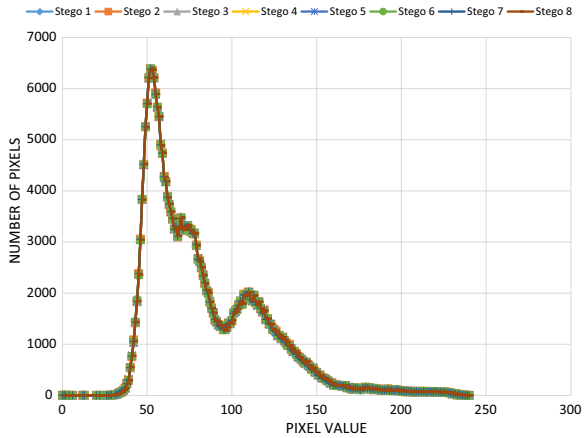

Fig. 8 The histogram comparison between the stego images of Airport

In contrast, the cover image size plays a significant role in dictating the embedding space of the related methods (Yuan et al. 2016; Meng et al. 2021). The larger the size, the more embedding space is provided, which can cause a bandwidth issue if the cover image has a high resolution.

Table 6 compares the proposed scheme with (Yuan et al. 2016; Meng et al. 2021) from the functionality perspectives. It indicates that this proposed scheme maintains essential functionality, such as secret data and original cover images that can be recovered losslessly. Also, in the embedding phase of the proposed scheme, the payloads are divided into different categories, so each PE value used for embedding can contain more than one bit. It means that the number of secret bits that can be embedded increases. This scheme reduces the number of PE value that needs to be changed. For this reason, the stego image quality is improving than only embedding one bit per PE value. The proposed method utilizes LSB, and it is generally difficult to recover the original pixel of the cover image. Implementing CRT-based SIS helps to eliminate side information needed to recover the original cover image. The method includes the original cover PE value in the design's sharing polynomial (x) calculations. Thus, when (x) is recovered by k stego images—the minimum number—both the secret image and the cover image can be losslessly restored.

Validity and security analysis

To validate the proposed method, we implement the threshold $k = 1$ without 2-bits LSBs, checking whether the scheme is valid. This threshold value has to be the same as the normal process without dividing (sharing) the stego image. The generated stego image is precisely the same as the stego image generated without sharing process; it is shown by its PSNR value, which is ∞.

An apparent concern in the proposed method is the access to confidential information by a third party or the possibility of destroying the stego images because of the weak LSB substitution. The issue is addressed while implementing SS after the embedding phase, leaving the only way the third party accessing or modifying the protected data by collecting at least k images. The unwanted party has to destroy or modify at least $k + 1$ share images to remove the possibility of recovering the secret data completely, where $k + 1 > n/2$. To put it simply, the higher the number of participants and the thresholds, the harder the unwanted parties to obtain the protected data. Therefore, both of them directly influence the method's security.

The histogram is the distribution of pixels of an image and can be used as the indication of a visually secure stego image (Al-Shaarani and Gutub 2021). In an image histogram, the x-axis is the pixel value of the image while the y-axis is the number of the respective pixels. Generally, the stego image histogram has to be similar to the original cover image. Figure 7 compares the six share stego images of 'Airport' with the original image. The embedded data are 50 Kb, and the n and k are 8 and 4, respectively. The result shows that all the histogram is quite similar to each other; this characteristic is also presented in other test images. So the proposed method can produce a secure stego image in terms of the histogram. This is also emphasized in Fig. 8, where the histogram of the stego images are presented in a chart and compared to each other. Based on that figure, it is found that the difference of each stego image histogram is very minimal and appears identical.

Another metric to measure security is by comparing the PSNR of the stego images with the original (Kadhim et al. 2019), which is discussed in the previous section because the PSNR value of the stego image represents its similarity with the original image. The higher the PSNR value, the harder to distinguish the stego image and the original image. Therefore, lowering the chance of an attack.

Conclusion

This research is motivated by hiding private data into a cover medium to secure them. We consider SS based on CRT and use it alongside the HS-based scheme. Before dividing the image using CRT-SS, the embedding process is done on the PE value. We implement 2-bit LSBs to minimize the distortion of the stego image. Several thresholds and participants are evaluated in the experiment, showing minimum changes to the stego images. The implementation of LSB causes the cover image to be lost after the extraction process, but using CRT-SS helps

prevent this. The experimental results depict that the proposed method provides better results than the previous ones.

In the future, this research can be extended to include some possibilities, for instance, how the dealer selects the cover image and ensures that it is safe and free from malicious software. Although it is out of the data hiding research scope, that selection can improve the security of the whole system.

Acknowledgements
The authors would like to thanks all lab and research group members who have supported this research, and all institutions, which have funded this research.

Authors' information
Chaidir Chalaf Islamy is a Ph.D student in Department of Informatics, Institut Teknologi Sepuluh Nopember (ITS), Indonesia, focussing on shared-secret data hiding. His related research is available at https://www.scopus.com/authid/detail.uri?authorId=57210750661 . Tohari Ahmad received the Bachelor degree in computer science from Institut Teknologi Sepuluh Nopember (ITS), Indonesia, the master degree in information technology from Monash University, Australia, and the Ph.D degree in computer science from RMIT University, Australia. He was a consultant for some international companies. In 2003, he moved to ITS, where he is now a professor. His research interests include network security, information security, data hiding and computer network. He is a reviewer of a number of journals. Prof. Ahmad's awards and honors include the Hitachi Research Fellowship, and JICA Research Program to conduct research in Japan. His research is available at https://www.scopus.com/authid/detail.uri?authorId=35241970700. Royyana Muslim Ijtihadie received bachelor and master degrees from Institut Teknologi Sepuluh Nopember (ITS), Indonesia; and Ph.D from Kumamoto University, Japan. His research interests include computer network and computer security. He is now a senior lecturer in ITS and is responsible for managing the network computer infrastructure and computer security in his university. His research can be found at: https://www.scopus.com/authid/detail.uri?authorId=36975529900

Author contributions
CCI: Conceptualization, methodology, software, formal analysis, investigation, writing original draft, visualization. TA: Conceptualization, methodology, writing review and editing, supervision, project administration, funding acquisition. RMI: Conceptualization, methodology, supervision. All authors read and approved the final manuscript.

Funding
This research was supported by the Ministry of Education, Culture, Research and Technology, The Republic of Indonesia, Institut Teknologi Sepuluh Nopember, and Universitas 17 Agustus 1945 Surabaya.

Availability of data and materials
https://github.com/chaidirchalaf/payload.

Declarations

Competing interests
All authors have no competing interests.

Received: 21 November 2022 Accepted: 22 February 2023
Published online: 02 June 2023

References

Ahmad T, Studiawan H, Ahmad HS, Ijtihadie RM, Wibisono W. Shared secret-based steganography for protecting medical data. In: International Conference on Computer, Control, Informatics and Its Applications. pp 87–92; 2014.

Al Huti MHA, Ahmad T, Djanali S. Increasing the capacity of the secret data using DE pixels blocks and adjusted RDE-based on grayscale images. In: International Conference on Information and Communication Technology and Systems. pp 225–230; 2016.

Al-Shaarani F, Gutub A (2021) Securing matrix counting-based secret-sharing involving crypto steganography. J King Saud Univ Comput Inf Sci 34(9):6909–6924. https://doi.org/10.1016/j.jksuci.2021.09.009

Ardiansyah G, Sari CA, Setiadi DRIM, Rachmawanto EH. Hybrid method using 3-DES, DWT and LSB for secure image steganography algorithm. In: 2nd International conferences on Information Technology, Information Systems and Electrical Engineering. pp 249–254; 2017.

Chang IC, Hu YC, Chen WL, Lo CC (2015) High capacity reversible data hiding scheme based on residual histogram shifting for block truncation coding. Signal Process 108:376–388. https://doi.org/10.1016/j.sigpro.2014.09.036

Cheddad A, Condell J, Curran K, Mc Kevitt P (2010) Digital image steganography: Survey and analysis of current methods. Signal Process 90(3):727–752. https://doi.org/10.1016/j.sigpro.2009.08.010

Dragoi I-C, Coltuc D (2014) Local-prediction-based difference expansion reversible watermarking. IEEE Trans Image Process 23(4):1779–1790. https://doi.org/10.1109/TIP.2014.2307482

Hassan FS, Gutub A (2022) Novel embedding secrecy within images utilizing an improved interpolation-based reversible data hiding scheme. J King Saud Univ Comput Inf Sci 34(5):2017–2030. https://doi.org/10.1016/j.jksuci.2020.07.008

Hong W, Chen T, Shiu C (2009) The journal of systems and Software Reversible data hiding for high quality images using modification of prediction errors. J Syst Softw 82(11):1833–1842. https://doi.org/10.1016/j.jss.2009.05.051

Islamy CC, Ahmad T (2019) Improving the quality of stego image using prediction error and histogram modification. Int J Intell Eng Syst 12(5):95–103. https://doi.org/10.22266/ijies2019.1031.10

Islamy CC, Ahmad T (2021) Enhancing quality of the stego image by using histogram partition and prediction error. Int J Intell Eng Syst 14(2):511–520. https://doi.org/10.22266/ijies2021.0430.46

Islamy CC, Ahmad T (2022) ANALYZING THE IMPACT OF THE SECRET SHARING ON STEGO IMAGES. ICIC Exp Lett 16(3):307–315. https://doi.org/10.24507/icicel.16.03.307

Islamy CC. Payload. https://github.com/chaidirchalaf/payload. Accessed 20 Apr 2022; 2022.

Kadhim IJ, Premaratne P, Vial PJ, Halloran B (2019) Comprehensive survey of image steganography: techniques, evaluations, and trends in future research. Neurocomputing 335:299–326. https://doi.org/10.1016/j.neucom.2018.06.075

Kamal AHM, Islam MM (2019) A prediction error based histogram association and mapping technique for data embedment. J Inf Secur Appl 48:102368. https://doi.org/10.1016/j.jisa.2019.102368

Kar N, Mandal K, Bhattacharya B (2018) Improved chaos-based video steganography using DNA alphabets. ICT Express 4(1):6–13. https://doi.org/10.1016/j.icte.2018.01.003

Kumar M, Agrawal S (2016) Reversible data hiding based on prediction error expansion using adjacent pixels. Secur Commun Netw 9(16):3703–3712. https://doi.org/10.1002/sec.1575

Kumar A, Abhishek K, Shah K, Namasudra S, Kadry S (2021) A novel elliptic curve cryptography-based system for smart grid communication. Int J Web Grid Serv 17(4):321–342. https://doi.org/10.1504/IJWGS.2021.118398

Kyriakopoulos K, Parish DJ. A live system for wavelet compression of high speed computer network measurements. In: International Conference on Passive and Active Network Measurement. Berlin, Heidelberg, pp 241–244; 2007.

Luo T, Jiang G, Yu M, Gao W (2015) Novel prediction error based reversible data hiding method using histogram shifting. Int J Comput Theory Eng 7(5):332–336. https://doi.org/10.7763/IJCTE.2015.V7.981

Meng K, Miao F, Xiong Y, Chang C-C (2021) A reversible extended secret image sharing scheme based on Chinese remainder theorem. Signal Process Image Commun 95:116221. https://doi.org/10.1016/j.image.2021.116221

Namasudra S, Devi D, Kadry S, Sundarasekar R, Shanthini A (2020) Towards DNA based data security in the cloud computing environment. Comput Commun 151:539–547. https://doi.org/10.1016/j.comcom.2019.12.041

National Library of Medicine eMicrobes Digital Library (2022) http://www.idimages.org/images/browse/ImageTechnique/. Accessed 1 Jun 2022
Ni Z, Shi Y-Q, Ansari N, Su W (2006) Reversible data hiding. IEEE Trans Circuits Syst Video Technol 16(3):354–362. https://doi.org/10.1109/TCSVT.2006.869964
Niu X, Yin Z, Zhang X, Tang J, Luo B. Reversible data hiding in encrypted AMBTC compressed images. In: Digital Forensics and Watermarking. Cham, pp 436–445; 2017.
Pavithran P, Mathew S, Namasudra S, Srivastava G (2022) A novel cryptosystem based on DNA cryptography, hyperchaotic systems and a randomly generated Moore machine for cyber physical systems. Comput Commun 188:1–12. https://doi.org/10.1016/j.comcom.2022.02.008
Prabowo HE, Ahmad T (2018) Adaptive pixel value grouping for protecting secret data in public computer networks. J Commun 13(6):325–332. https://doi.org/10.12720/jcm.13.6.325-332
Rad RM, Wong K, Guo JM (2014) A unified data embedding and scrambling method. IEEE Trans Image Process 23(4):1463–1475. https://doi.org/10.1109/TIP.2014.2302681
Rad RM, Wong KS, Guo JM (2016) Reversible data hiding by adaptive group modification on histogram of prediction errors. Signal Process 125:315–328. https://doi.org/10.1016/j.sigpro.2016.02.001
Shambour MK, Gutub A (2022) Progress of IoT research technologies and applications Serving Hajj and Umrah. Arab J Sci Eng 47(2):1253–1273. https://doi.org/10.1007/s13369-021-05838-7
Shamir A (1979) How to share a secret. Commun ACM 22(11):612–613. https://doi.org/10.1145/359168.359176
Suresh M, Shatheesh Sam I (2022) 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 34(6, Part B):3489–3496. https://doi.org/10.1016/j.jksuci.2020.08.007
Tang Z, Pang M, Yu C, Fan G, Zhang X (2021) Reversible data hiding for encrypted image based on adaptive prediction error coding. IET Image Process 15(11):2643–2655. https://doi.org/10.1049/ipr2.12252
Thodi DM, Rodríguez JJ (2007) Expansion embedding techniques for reversible watermarking. IEEE Trans Image Process 16(3):721–730. https://doi.org/10.1109/TIP.2006.891046
Tian J (2003) Reversible data embedding using a difference expansion. IEEE Trans Circuits Syst Video Technol 13(8):890–896. https://doi.org/10.1109/TCSVT.2003.815962
USC-SIPI SIPI image database (2021) http://sipi.usc.edu/database/database.php?volume=misc. Accessed 1 Mar 2021
Wu X, Weng J, Yan WQ (2018) Adopting secret sharing for reversible data hiding in encrypted images. Signal Process 143:269–281. https://doi.org/10.1016/j.sigpro.2017.09.017
Yan X, Gong Q, Li L, Yang G, Lu Y, Liu J (2020) Secret image sharing with separate shadow authentication ability. Signal Process Image Commun 82:115721. https://doi.org/10.1016/j.image.2019.115721
Yao H, Qin C, Tang Z, Tian Y. Guided filtering based color image reversible data hiding. J Vis Commun Image Represent. 2017;43(Supplement C):152–163. https://doi.org/10.1016/j.jvcir.2017.01.004
Yao H, Mao F, Tang Z, Qin C. High-fidelity dual-image reversible data hiding via prediction-error shift. Signal Process. 2020;170:107447. https://doi.org/10.1016/j.sigpro.2019.107447
Yu C, Zhang X, Li G, Zhan S, Tang Z (2022a) Reversible data hiding with adaptive difference recovery for encrypted images. Inf Sci 584:89–110. https://doi.org/10.1016/j.ins.2021.10.050
Yu C, Zhang X, Zhang X, Li G, Tang Z (2022b) Reversible data hiding with hierarchical embedding for encrypted images. IEEE Trans Circuits Syst Video Technol 32(2):451–466. https://doi.org/10.1109/TCSVT.2021.3062947
Yuan L, Li M, Guo C, Hu W (2016) Secret image sharing scheme with threshold changeable capability. Math Probl Eng 1:9576074. https://doi.org/10.1155/2016/9576074

Publisher's Note