Multimedia Tools and Applications (2021) 80:8423–8444
https://doi.org/10.1007/s11042-020-10035-z

PSNR vs SSIM: imperceptibility quality assessment for image steganography

De Rosal Igantius Moses Setiadi [1]

Received: 15 May 2020 / Revised: 20 August 2020 / Accepted: 6 October 2020 /
Published online: 3 November 2020

Abstract
Peak signal to noise ratio (PSNR) and structural index similarity (SSIM) are two measuring tools that are widely used in image quality assessment. Especially in the steganography image, these two measuring instruments are used to measure the quality of imperceptibility. PSNR is used earlier than SSIM, is easy, has been widely used in various digital image measurements, and has been considered tested and valid. SSIM is a newer measurement tool that is designed based on three factors i.e. luminance, contrast, and structure to better suit the workings of the human visual system. Some research has discussed the correlation and comparison of these two measuring tools, but no research explicitly discusses and suggests which measurement tool is more suitable for steganography. This study aims to review, prove, and analyze the results of PSNR and SSIM measurements on three spatial domain image steganography methods, i.e. LSB, PVD, and CRT. Color images were chosen as container images because human vision is more sensitive to color changes than grayscale changes. Based on the test results found several opposing findings, where LSB has the most superior value based on PSNR and PVD get the most superior value based on SSIM. Additionally, the changes based on the histogram are more noticeable in LSB and CRT than in PVD. Other analyzes such as RS attack also show results that are more in line with SSIM measurements when compared to PSNR. Based on the results of testing and analysis, this research concludes that SSIM is a better measure of imperceptibility in all aspects and it is preferable that in the next steganographic research at least use SSIM.

Keywords Imperceptibility · Image Quality assessment · Image steganography · PSNR · SSIM · Image histogram

1 Introduction

Steganography is the science of data hiding that aims to secure the data by embedding data (message) on the container media. Container media are generally in the form of multimedia

✉ De Rosal Igantius Moses Setiadi
moses@dsn.dinus.ac.id

[1] Department of Informatics Engineering, Dian Nuswantoro University, Semarang 50131, Indonesia

files such as images, text, audio, or video [13, 21, 30]. Image is one of the most widely used file types as container media. In steganography in images, at least it takes input in the form of a container image and the message to be embedded. This message is generally in the form of text or images that are smaller than the container media, the results of the embedding process will produce one output, namely the stego image. The stego image is a container image that has been embedded with the message. Embedding the message in the container image is done by manipulating the container image so that it can result in changes in the value of the pixels, structure, histogram, and can produce noise or artifacts in the stego image. If manipulation is too excessive, the human sense of vision may be able to detect changes in the image. This is what is called the quality of imperceptibility in the stego image.

Image steganography currently have a variety of methods and approaches, based on the ability to recontainer data there are reversible and irreversible steganography [11], and based on domain there are spatial and transform [43]. Reversible steganography means that both, container image and message can be returned in full during the extraction process, whereas irreversible is generally only a message that can be returned in full. Reversible steganography generally uses the shifting histogram method where this method has a relatively smaller payload compared to the irreversible method. While based on the domain several methods are popular in the spatial domain such as the least significant bit (LSB), pixel value differencing (PVD), Chinese remainder theorem(CRT), exploiting modification direction (EMD) [3, 25, 36, 48], whereas, in the transformation domain, wavelet, cosine, and singular value decomposition are popular transformations [15]. Each of the existing methods has advantages and disadvantages, however, various methods are proposed to improve the quality of the image stego, on one or several aspects such as increased imperceptibility, payload capacity, or security [13, 15, 21, 23, 27, 28].

Referring deeper to the imperceptibility aspect, this aspect can be measured by several measurement tools, of which the most popular are PSNR and SSIM [36, 37], some other research also suggests using image histograms [3, 8, 13, 18, 32, 38]. Other measuring tools can be used to measure the quality of imperceptibility, such as visual information fidelity (VIF), which was first published by Sheikh and Bovik. VIF has a default range value of 0 to 1, but the resulting value can be more than 1 when there is an increase in image quality, so this measuring tool can be used to measure the quality of image enhancement. VIF is designed more specifically for natural imagery which is mostly 'consumed' by humans, this reason may make this measuring tool unpopular and rarely used in data hiding research [39] so that this research will be more concentrated on PSNR and SSIM. PSNR and SSIM are not only used in image steganography but are also widely used in various digital image processing such as image compression [29], image restoration [4], image denoising [40], and various other image processing. PSNR is a measurement tool that is more popular and more widely used than SSIM. In steganography research, several studies use PSNR measurement tools but do not use SSIM measurement tools, for example in research [1, 5–8, 11, 14, 16, 17, 22, 32–34, 38, 41, 44, 48, 49], all of which were published in 2015–2020. Motivation to only use PSNR measurement tools is possible because PSNR has been tested and is considered valid in various steganography researches in the world.

PSNR formula is also produced from MSE formula which is easy to calculate and understand, besides the square root is a valid distance metric calculation in symmetric, convex, can be distinguished and suitable for orthogonal and unitary transformation, these things are the expected mathematical properties owned by MSE [10, 50]. But, MSE can be a measuring tool that has poor performance when used to predict fidelity or imperceptibility signal quality

[50]. So in some researchers say the need for other measuring instruments besides PSNR to validate the quality of stego images, in this case, is SSIM [10, 19, 20, 35, 47, 51]. SSIM was first developed by Wang et al. [51]. SSIM is designed based on the image distortion model using three factors of loss of correlation, luminance distortion, and contrast distortion, to measure the similarity of the two images. This makes SSIM more correlated with the human visual system [19, 20]. Based on research conducted by [20], it is said that PSNR is more sensitive to degradation that occurs in the image due to the addition of Gaussian noise, while SSIM is more sensitive to degradation in JPEG image compression. However, in other degradations such as Gaussian blur and JPEG 2000 compression the sensitivity level between PSNR and SSIM is a bit similar. In contrast to PSNR and SSIM, image histograms can be used to find out the imperceptibility and resilience of stego statistical attacks. [13, 21], here what is observed is the difference from the original container image histogram with the stego image, where a good steganography method will certainly not change the histogram significantly.

Until now the implementation of various steganographic methods will always produce changes in pixel values, structures, histograms, or generate additional noise in stego images, even though a lot of research has tried to minimize this. This is why mandatory measurement of imperceptibility is required. In various steganographic studies, the explanation of PSNR and SSIM is only explained normatively and only explains that the PSNR value that can be accepted is at least above 30 dB [12, 43], or better above 40 dB [13], while the ideal SSIM value is close to one [37, 43]. On research [10, 19, 20, 35, 47, 51] has been studied about image quality assessment but has not been specifically reviewed about the need to use both of these measuring instruments for image steganography. Indeed, there are not many theories that can provide certainty in steganographic images that if the quality of PSNR is good, then the SSIM is also good. If this is true, then just one measurement can guarantee the quality of imperceptibility. But in fact, in many recent studies, PSNR is still only used as a measure of imperceptibility. Other more modern measuring instruments such as SSIM is still not used for various reasons. So in this study, further analysis was carried out to determine whether using PSNR alone could obtain indicators that were in line with SSIM. If a contrasting value is produced, of course, in the next study, it is mandatory to use at least two measuring instruments to measure imperceptibility. This research consists of six main parts, namely 1) Introduction, in this Section, 2) Preliminaries, discussing related work and basic theories, 3) Methods, discussing the method of embedding messages and measurements used, 4) Experiments, which discusses the source dataset to results, 5) Discussions, which discuss and provide a more detailed analysis based on the hypotheses that have been described, 6)Conclusions, in the section to provide conclusions.

2 Preliminaries

Many survey papers have been carried out comparing several popular methods of steganography, especially in the spatial domain. Why the spatial domain? Because steganography is more focused on imperceptibility, payload capacity, and security. The transform domain is superior in terms of resistance to manipulation so it is more suitable for use in image watermarking because it can maintain the data embedded in the image container from manipulation damage [3, 13, 21, 37]. Of the many methods of steganography, LSB is the most widely used method in the decades to date. LSB is a method that is very simple and superior in terms of imperceptibility and payload, this is because by default this method only

makes a very small change of 1-bit in each pixel of the image container [11, 30, 37]. Changes in pixel values of 1-bit are very difficult to detect by human vision. Based on PSNR measurements the standard LSB method generally can produce values of 40 dB or more. This is the basic thing why the LSB method is so popular in image steganography. In terms of payload, the LSB method by default can hold data of one-eighth the size of the container image, assuming one pixel holds one message bit. LSB method is more developed in terms of security because by default the insertion technique is done in order so that it is easy to guess. In some research [8, 38] LSB method was developed to increase the security and payload capacity. PSNR measurement results for the method proposed in the two studies are indeed quite good, namely above 50 dB, but from the histogram presented it appears that there is a histogram sample that changes visibly. This makes this method less good and can cause suspicion of the attacker. For more details, see Fig. 1.

Another method, namely PVD, is a newer method compared to LSB, this method also works in the spatial domain by utilizing the difference between neighboring pixel values. This method has a way of working that is quite similar to the LSB method based on edge detection, wherein the edge area is embedded in more data bits than non-edge areas [3, 36, 37]. In the PVD method the capacity is determined by the difference in the value of neighboring pixels, the larger the difference the more bits of data that can be embedded [3], and generally the PVD method has a greater capacity than LSB. In the survey conducted on [3], compared to the LSB and PVD methods in grayscale baboon images, where the embedded message is 1.6769 bits per pixel (bpp) or equivalent to the maximum payload of the PVD method. Because the message is greater than 1bpp, then in the LSB method 1 bpp message is embedded in LSB (eighth bit) and the rest is embedded in the second bit of LSB (seventh bit). Based on PSNR measurements, the PVD method only produces 34.0230 dB, while LSB produces 45.2930 dB, meaning that LSB is far superior based on the PSNR measurement tool. However, if observed in Fig. 2, visually there is no difference in the results of the stego image, but when viewed from

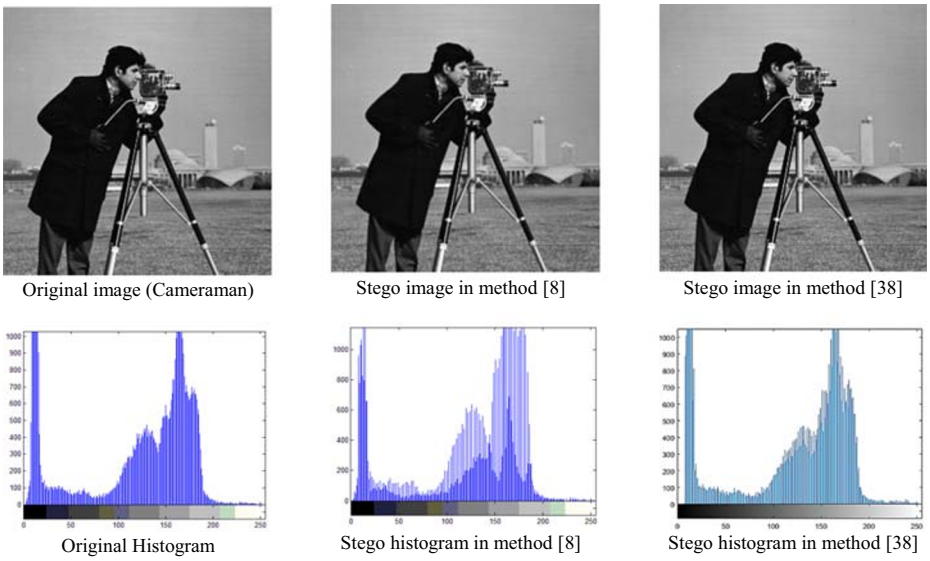

Fig. 1 Sample histogram of previous LSB method. Original image (Cameraman), Stego image in method [8], Stego image in method [38], Original Histogram, Stego histogram in method [8], Stego histogram in method [38]

the histogram, the PVD method has a much better histogram and is more similar to the original image histogram compared to the LSB method. These results are quite similar to the method LSB proposed in the research [8, 38] which results in a very satisfying PSNR value but the image histogram changes quite significantly.

These results are very tickling, so it is interesting to study again. How a PSNR value generates fantastic values but changes the histogram quite a lot. A histogram is a pixel distribution plot that is presented with a graph with a range of pixel values and the frequency of existing pixel values [42]. Logically if there is a change in the histogram there should be a change in structure, luminance, contrast, and can cause noise in the image. Based on the results of SSIM measurements performed on baboon images (see Fig. 2), the LSB method is also still superior with a value of 0.9952 and PVD only yields 0.9817. But keep in mind that the research only tests on a grayscale image. In the paper written by [46], it is said that color images are more sensitive to the human visual system when compared to grayscale images, besides embedding data in color images will produce different effects [2].

In other, more advanced research such as that conducted by Liao et al. [28], proposed a new strategy for dividing messages into three partitions for three color channels using amplifying channel modification probabilities (ACMP). This is because each channel has a different payload, besides that it also serves to concentrate message embedding in certain areas so that better steganographic performance can be obtained. Another research was also developed by Liao et al. [27], proposes a technique that can adaptively distribute the payload based on the texture features of the image. Both of these studies have succeeded in increasing the security of the steganography method, although from the imperceptibility aspect it is not discussed further, logically, of course, imperceptibility should be increased and these two methods indirectly imply that imperceptibility is not sufficiently measured with a standard measuring instrument based on square error, such as PSNR, but it needs to be measured with another measuring instrument that takes into account more things like SSIM.

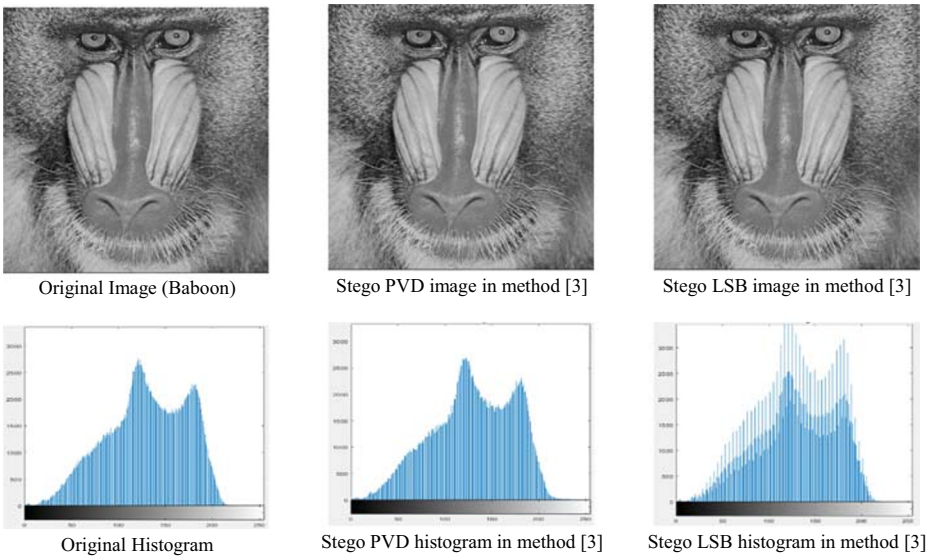

Fig. 2 Comparison of PVD histogram and LSB histogram. Original Image (Baboon), Stego PVD image in method [3], Stego LSB image in method [3], Original Histogram, Stego PVD histogram in method [3], Stego LSB histogram in method [3]

So in this research will be further investigated about the effect of embedding on the color image of the imperceptibility aspect, based on the PSNR and SSIM measurement tools that will be tested on methods in the spatial domain based on several theories below.

2.1 Red green blue (RGB) color image

Human vision is more sensitive to color than grayscale. Color images generally consist of three color channels where each channel is a grayscale image with a depth of 8-bits. So when the three channels are combined the color image depth is 24-bits. There are various color space models, namely RGB, XYZ, YIQ, YCbCr, HIS, etc. [46]. The RGB color space model is the most popular model used as an image storage format on computers. Each channel (R, G, and B) has the same relative intensity so that the processing can be done separately for each channel, after completion, all three can be combined again. Another way of processing RGB images is by converting RGB images to separate intensity components from color components, then intensity components can be processed using different algorithms with image components, after all, components can be recombined after processing [9, 46].

2.2 Image histogram

The histogram is one of the basics used to design many operations in digital image processing. The histogram is a plot of the frequency of occurrence of pixel values based on grayscale images. An image histogram (*Hi*) can be written explicitly with Eq. 1.

$$Hi(k) = J \tag{1}$$

Where i is an image that has an MN dimension that contains J is the number of times the occurrence of value on the scale k, where for each $k = 0, \ldots, K-1$, and K is the gray level which is commonly 2^8. Histograms are useful for expressing many things about images, especially to find out the pixel frequency distribution of images on a grayscale [9, 42]. Histograms also have a relationship with contrast and luminance in an image, because histogram shifts can also affect image contrast. In a steganographic image, a histogram shift can occur due to changes in pixel values due to the embedding of messages. So some steganography research also uses image histograms to measure the quality of the steganography method.

2.3 Peak signal to noise ratio (PSNR)

Much research related to image and signal processing uses PSNR as a quality measurement tool [47, 50]. PSNR results from the calculation of the logarithm of the mean square error (MSE) of an image. Where MSE traditionally uses the summation method as its main component. In MSE grayscale images are calculated based on $M \times N$ dimensions, whereas in RGB MSE color images RGB images can be calculated based on $M \times N \times O$ dimensions, see Eq. 2.

$$MSE = \frac{1}{M \times N \times O} \sum_{x=1}^{M} \sum_{y=1}^{N} \sum_{z=1}^{O} \left[\left(I_{(x,y,z)} - I'_{(x,y,z)} \right)^2 \right] \tag{2}$$

Where M and N are image resolution, O is the number of image channels, $I(x, y, z)$ is the pixel value of the original image at the x, y coordinates and channel z, $I'$is the output image/

processing result, in this research I' is a stego image. From Eq. 2, it can be seen that the MSE formula is generated from the sum of the square of the original image pixel value minus the stego image pixel. MSE has a close relationship with PSNR because the MSE value is used to calculate the PSNR value, see Eq. 3.

$$PSNR = 10log10\left(\frac{max^2}{MSE}\right) \tag{3}$$

Where *max* is the highest scale value of the 8-bits grayscale. Based on Eqs. 2 and 3 as a formula used to calculate the PSNR it can be seen that the PSNR is composed of the error squared value as the main component. The error value is generated by the difference in pixel values at the same coordinates and channels. PSNR will produce an infinity value that also does not change the pixel value, conversely if more differences in the pixel value between the two images will produce a PSNR with a smaller value.

2.4 Structural similarity index (SSIM)

SSIM is another measurement tool used to measure the quality of imperceptibility in steganographic images [37]. SSIM was first published by [51], in his research it was stated that SSIM was built based on three main factors, namely luminance, contrast, and structure. These three factors replace the summation method used as the basis for calculating PSNR [20]. In RGB color images, SSIM can be defined with Eq. 4.

$$SSIM(i, i') = l(i, i')c(i, i')s(i, i') \tag{4}$$

Where

$$l(i, i') = \frac{2\mu_i\mu_{i'} + C1}{\mu_i^2 + \mu_{i'}^2 + C1} \tag{5}$$

$$c(i, i') = \frac{2\sigma_i\sigma_{i'} + C2}{\sigma_i^2 + \sigma_{i'}^2 + C2} \tag{6}$$

$$s(i, i') = \frac{\sigma_{ii'} + C3}{\sigma_i\sigma_{i'} + C3} \tag{7}$$

$$\mu_i = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N}\sum_{z=1}^{O} i_{xyz}}{MNO} \tag{8}$$

$$\sigma_i^2 = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N}\sum_{z=1}^{O}\left(i_{xyz} - \mu_i\right)^2}{MNO} \tag{9}$$

$$\sigma_{ii'} = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N}\sum_{z=1}^{O}\left(i_{xyz}-\mu_i\right)\left(i'_{xyz}-\mu_{i'}\right)}{MNO} \tag{10}$$

$$\mu_{i'} = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N}\sum_{z=1}^{O} i'_{xyz}}{MNO} \tag{11}$$

$$\sigma_{i'}^2 = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N}\sum_{z=0}^{O}\left(i'_{xyz}-\mu_{i'}\right)^2}{MNO} \tag{12}$$

$$\sigma_{i'i} = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N}\sum_{z=1}^{O}\left(i'_{xyz}-\mu_{i'}\right)\left(i_{xyz}-\mu_i\right)}{MNO} \tag{13}$$

Keep in mind that the first factor in Eq. 4 is $l(i, i')$, this is a function that compares luminance of image i and image i'. Maximum values of $l(i, i')$ is 1, which is obtained when the two luminance (μ) images are equal ($\mu_i = \mu_{i'}$). The second factor is $c(i, i')$, this is a function that compares the contrast of image i and image i'. The maximum value of $c(i, i')$ is 1, which is obtained when the two image contrasts, which are calculated based on the standard deviation (σ) are equal ($\sigma_i = \sigma_{i'}$). The third factor is $s(i, i')$, this is a function that compares structures of image i and image i' based on the correlation coefficient, for the record $\sigma_{ii'}$ is a covariance between image i and image i'. The maximum value of $s(i, i')$ is 1, this value is obtained if $\sigma_{ii'} = \sigma_i\sigma_{i'}$. So if the three-factor values are 1, the maximum value of SSIM is 1. Many studies say that the range of SSIM values is between 0 to 1, but actually, the minimum SSIM value can reach −1. This is because negative values are very rare and irrelevant. Constant values $C1$, $C2$, dan $C3$ are used to avoid the zero denominators [51] , so it is recommended to use the values $C1 = (0.01 \times 255)^2$, $C2 = (0.03 \times 255)^2$, and $C3 = C2/2$ as the default value. SSIM also has a relationship with PSNR that has been discussed in research [20] but because of the different ways of working and calculation, the SSIM has a different sensitivity.

2.5 Least significant bit (LSB)

LSB is a steganography method that has been used for a long time but is still very popular today. The LSB method is still being developed and combined with various approaches, such as edge detection [11, 31, 36, 37]. LSB is still popular until now because it is famous for its nature which has very good imperceptibility. This is evidenced by various studies that prove that the LSB method always gets a PSNR value above an acceptable value and even has a very good quality that is above 40 dB. The way LSB works in steganographic images is very simple, namely by changing the LSB value of the pixel image container with 1-bit messages, this process is called embedding on a pixel, for more detail see Fig. 3. Traditionally embedding is done sequentially from the first pixel (top left corner) to the last pixel (bottom right corner) of an image or until all bits of the message are embedded. By default, if a 1-bit message is embedded per pixel, the maximum message size that may be embedded is one-eighth of the size of the container image or can also be adjusted to the number of container image pixels. The number of image pixels can be calculated by knowing the dimensions of the image (generally stored in

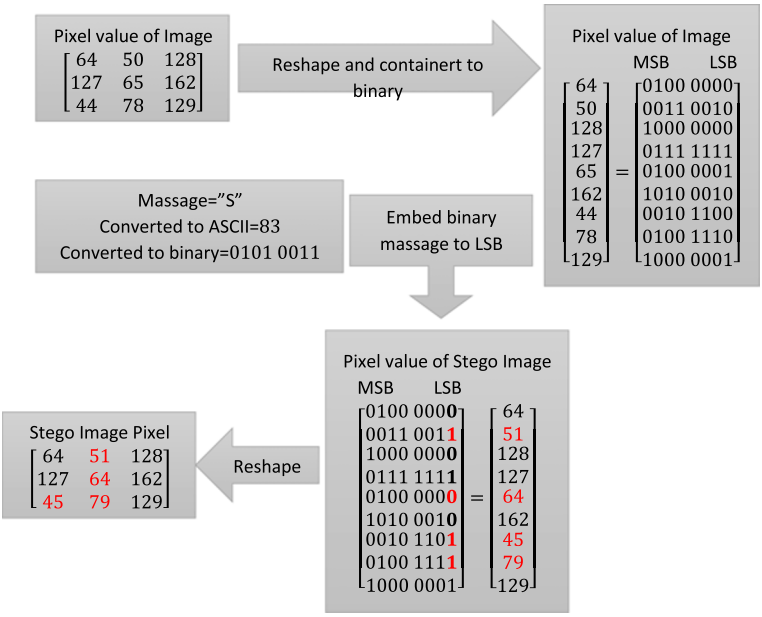

Fig. 3 Traditional LSB Image Steganography

variables M, N, and O, where M is width, N is height, and O is the number of channels, if the image is grayscale then the value O = 1 whereas if the image is color (RGB) then the value O = 3. If the size of the message does not fit to be accommodated on LSB or 8th bit, then the rest of the message can be accommodated on 7th and 6th bits, but keep in mind that if the bits get closer to Most Significant Bit (MSB) there will be distortion but if the embedding is only done on the 8th bit, then it will not appear visible distortion or if it is measured with PSNR. The distortion that occurs in the LSB is more apparent if you observe the histogram differences in the original image and the stego image. an example of how traditional LSB works in image steganography.

2.6 Pixel value differencing (PVD)

PVD is a method of steganography in the spatial domain that is newer and more complex than LSB. By default, PVD has an advantage in load capacity, which can store more messages when compared to the LSB method and is claimed to be able to embed messages more effectively. This is because the message embedding process is based on the difference between neighbor pixel values. This difference is then classified in the PVD quantization table, which is used to determine the number of bits that can be embedded in the pixel image containers. This method was first published by [52], in it are proposed two kinds of quantization tables. The first quantization table has a range of 8,8,16,32,64, and 128, this quantization table has a larger load capacity, also produces greater distortion when measured by PSNR. The second quantization table has a range of 2,2,4,4,4,8,8,16,16,32,32,64, and 64, in this table the resulting distortion is less but the load can be pinned even less. In this research, the first quantization table was chosen, with the aim that the PSNR produced is certainly no better than LSB, here will be further investigated about the difference between PSNR and SSIM, whether with a low

PSNR always results in a low SSIM. Table 1 shows the PVD quantization table used in this research.

Whereas the PVD embedding algorithm is described as follows:

1. Converting message data into an 8-bits binary form.
2. Take the values of two neighboring pixels in a sequence of container images (p_i and p_{i+1}). Assume that the values of p_i and $p_{i+1}$are g_i and g_{i+1}. Then find the difference (d), using Eq. 14

$$d = g_{i+1} - g_i \tag{14}$$

3. Determine the lower limit (I_k) and the number of bits (n), using Eq. 15

$$I_k \leq d_i \leq I_{k+1} \tag{15}$$

4. Take n-bits messages based on I_k, then change to decimal (b).
5. Calculate the new difference value (d') using Eq. 16.

$$d' \begin{cases} I_k + b, & d \geq 0 \\ -(I_k + b), & d < 0 \end{cases} \tag{16}$$

6. Get the new pixel value using Eq. 17.

$$f\left(g_i^{'}, g_{i+1}^{'}\right) \begin{cases} g_i - \left\lceil \frac{m}{2} \right\rceil, g_{i+1} + \left\lfloor \frac{m}{2} \right\rfloor, m = odd\ number \\ g_i - \left\lfloor \frac{m}{2} \right\rfloor, g_{i+1} + \left\lceil \frac{m}{2} \right\rceil, m = even\ number \end{cases} \tag{17}$$

$$(\text{Where}) m = d^{'} - d$$

2.7 Chinese remainder theorem (CRT)

The CRT algorithm uses the main operation of the residual quotient which aims to improve security. CRT algorithm can reconstruct integers with a certain range of values for each coprime number or number. Because of this, CRT algorithms can be applied in various fields of data security such as cryptography or steganography. Not only that, but CRT can also be

Table 1 PVD Quantization table used

The lower and upper limit	Range	Number of bits
0–7	8	3
8–15	8	3
16–31	16	4
32–63	32	5
64–127	64	6
128–255	128	7

used for authentication, image coding, and others. The process of inserting a message with a CRT will make the message encrypted indirectly, and has a shorter time during the embedding process and results in minimal distortion [45]. CRT algorithm can be expressed with Eq. 18 to Eq. 21.

$$\mu = \{X_1, X_2, \ldots, X_n\} \tag{18}$$

Where μ is a set of integers. Whereas X is a relatively prime pair. If suppose A is the value used to insert a message in steganography, then A can be obtained by Eq. 19.

$$A = \left(\sum_{i=1}^{r} R_i \frac{X}{X_i} J_i \right) (mod\ X) \tag{19}$$

Where the value $X = X1 \cdot X2 \cdot \ldots Xr$, then the value of J_i can be determined from Eq. 20.

$$J_i \frac{X}{x_i} = 1 (mod\ X_i) \tag{20}$$

Then the value of A can be concluded with Eq. 21.

$$A = R_i (mod\ X_i) \tag{21}$$

Where R is the residue. Although the CRT algorithm has advantages such as providing security of hidden messages, CRT also has the disadvantage that there can be reconstruction errors on large integers if an error occurs in the remainder of the quotient operation. Because of this, the CRT method is known to have a strong resistance to manipulation of an image [26].

3 Method

In this research, three methods that are popular in the spatial domain of image steganography used, i.e. LSB, PVD, and CRT. The container image used is a true-color 24-bits image that has an RGB color channel. Because it consists of three color channels before the embedding process is carried out, the separation process of each channel is carried out. Embedding is done by filling all pixels on one channel only (R or G or B) by using a message size that is adjusted to the number of pixels in a channel. Where each pixel is embedded 1-bit message or 1 bit per pixel (bpp) for each channel or 0.33 bpp in whole image. This size is determined based on the LSB method because by default 1 pixel is embedded 1 bit. This can also apply to the CRT method, whereas in the PVD method embedding cannot be done evenly (from the initial pixel to the last pixel image) because embedding is based on the difference in the value of neighboring pixels, so the message will be more concentrated in the upper area of the image. The results of embedding in the form of the stego image of each method are then measured by the quality of the imperceptibility using PSNR and SSIM. The results of imperceptibility measurements will then be further analyzed and discussed in the discussion section. For more details, see Fig. 4.

4 Experiments

Image data sets are taken from several web pages such as http://mmtg.fel.cvut.cz/sid-database/ [24], sipi.usc.edu/database, highreshdwallpapers.com, redleafbear.com/products, genchi.

info/japanese-garden-wallpaper, and cosentino.com/gallery. From these pages, an image that has a dimension ratio of 1: 1 is selected, then the entire image is resized to 512 × 512 pixels, this size was chosen because it refers to the standard image taken from http://mmtg.fel.cvut.cz/sid-database/ and sipi.usc.edu/database. The total images used are as many as 40 images, Fig. 5 shows the entire image used in this research.

Furthermore, as explained in Section 3, the color insertion process is carried out in each method. The message that is embedded in each channel is the same text message. The message is converted into message bits and then each bit is embedded in all pixels in one color channel. Embedding messages is done sequentially from the top-left pixel to the bottom-right pixel. In other words, the embedding capacity is 1 bpp for each channel, but if three color channels are combined into an RGB image, the message capacity is only 0.33 bpp. One thing to note is the PVD method, where embedding cannot be done evenly (1 bpp), this is because in the embedding algorithm the PVD method cannot be done in this way, in the end, embedding is not evenly distributed to the entire image. The 1-bpp size for each color channel was chosen because this is a high bpp size even by default the maximum capacity of the LSB and CRT methods. This is done because according to the theory that has been widely tested and verified, that the embedded payload capacity has a very close correlation to the imperceptibility quality, where the greater the embedded payload capacity makes more significant distortion in the container image which decreases the imperceptibility quality. Table 2 is the result of measuring the PSNR value of each method in the entire image, while Table 3 is the result of measuring the SSIM value.

Based on the results of the PSNR measurements presented in Table 2, the PSNR values in the LSB method have the best quality with an average value of 51.1 dB of all channels. PVD and CRT have a PSNR quality far below the LSB which is around 42 dB, but PVD is still slightly superior compared to CRT. The contrast appears in the SSIM measurement results presented in Table 3, where the PVD method has the best and dominant SSIM quality compared to the LSB method, except for the CRT method, the PSNR and SSIM results were consistent. Researchers, especially novice researchers, will be confused by this result, considering that PSNR and SSIM are the most popular and widely used measuring instruments, because the two imperceptibility measuring instruments produce contrasting values, although both of these measurement tools agree that the CRT method has imperceptibility quality that is not better than the LSB method and the PVD method.

To be more convincing the results presented in the first experiment were added more image datasets to be tested, 160 color images (RGB) were selected randomly from the page http://homepages.inf.ed.ac.uk/rbf/CVonline/Imagedbase.htm, where the selected image has a

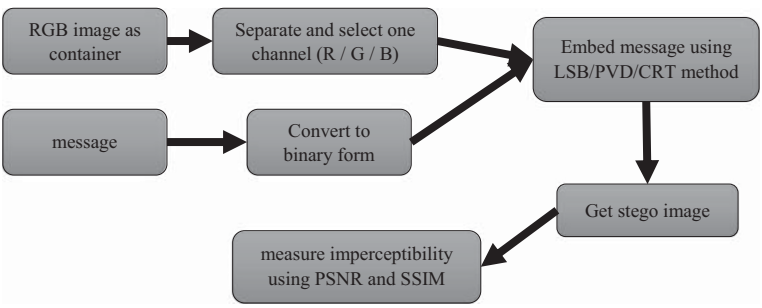

Fig. 4 Embedding and measurement method used

minimum size of 512 × 512 pixels or larger, then the entire selected images are resized to 512 × 512 pixels to facilitate the testing process. Based on the test results of these 160 images, an average value is similar to the results presented in Table 1 and Table 2. Where for the LSB method, the PSNR value is 51.1369 dB for the red channel, 51.1398 dB for the green channel, and 51.1440 dB for the blue channel, whereas for the SSIM value the value for the red channel is 0.9990, the green channel is 0.9992 and the blue channel is 0.9991, this value is very similar to the value presented with the value of 40 sample images. In the PVD method, the values are also close, the difference is not more than 0.5 dB for PSNR and 0.0001 for SSIM. Likewise, in the CRT method, the experimental value with 160 image datasets only has a difference of 0.3 dB for PSNR and a difference of 0.0001 for SSIM. Thus the use of 40 datasets is considered valid enough to do.

It has been said that in the first experiment only 1-bit value per pixel is embedded for the LSB and CRT methods, where 1-bit is embedded from the first pixel to the last pixel. Whereas the PVD method is not embedded embed in this way, so that it is possible for more than 1-bit in the initial pixels, and in the final pixels the message is not containered. So in the second experiment below is done by different embedding, namely by calculating the value of the PVD max payload on each channel, then embedded messages the size of the PVD max payload both on the LSB method and the PVD method. The max payload size of PVD is more than 1 because, in theory, presented in Section 2.6, it is stated that the PVD capacity is based on the difference in pixel values between neighbors and the results can be more than 1-bit per pixel, so the LSB method will overcapacity. The solution is to pin the 1-bit message in the smallest bits of the initial pixel to the end sequentially, then the rest is embedded the same way in the second smallest pixel bit. In the second experiment the CRT method was not tested because it was based on the PSNR and SSIM values, it was agreed that CRT was not better than PVD and LSB in imperceptibility. The results of the second experiment are presented in Table 4 for PSNR and Table 5 for SSIM.

Based on the results of the experiment with the maximum PVD payload presented in Table 4 and Table 5, the same indication also reappeared that PVD is superior based on SSIM and LSB is still superior based on LSB. If this is not analyzed further, it will lead to multiple perceptions and perhaps a lot of research can lead to wrong conclusions if not using the measuring instrument correctly.

5 Discussions

In this section, several important points are discussed for some of the problems outlined in Section 2 and tested in Section 4. The first point discussed is the problem of implementing the LSB and PVD methods in grayscale and color (RGB) images. Based on the results of previous research [3], the LSB method in the grayscale image is superior in both measuring instruments, both PSNR and SSIM. But because of research [2] stated that steganography in color images will produce different effects compared to grayscale images. This statement is corroborated by the theory written in the publication [46] that the human visual system is more confident of the distortions that occur in color images. Based on the results of tests conducted in Section 4, prove that the statement on the research [2, 46] it is true even though this research uses a different embed method with the method [2]. In this research, the results of the experiment show a contrast, where LSB is superior based on PSNR and PVD values are superior to SSIM values. This will make it difficult for novice researchers to conclude, although based on the PSNR theory it is used to measure imperceptibility based on noise that occurs in the stego

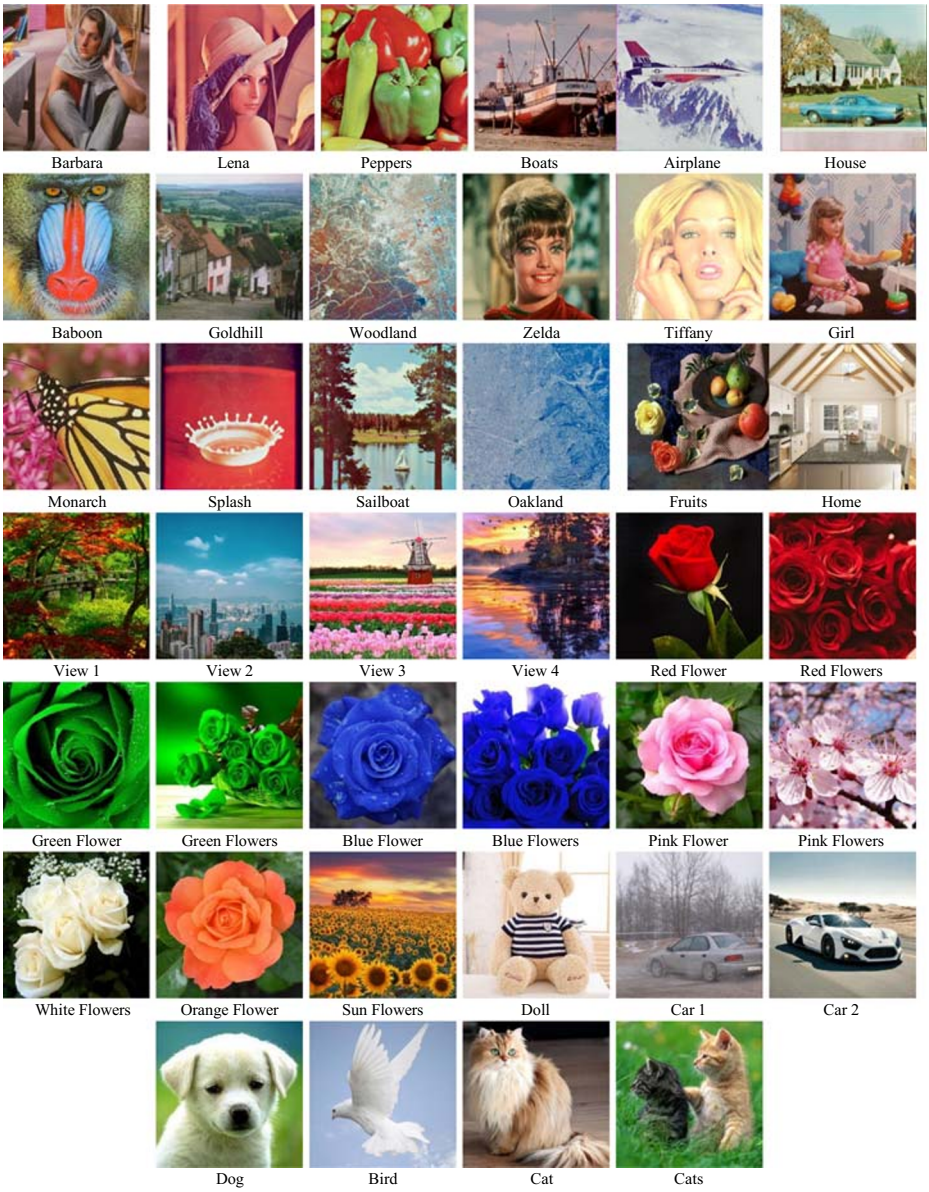

Fig. 5 Image Dataset Used

image and SSIM is used to measure imperceptibility based on the human visual system on the stego image, it must be proven more explicitly what the relationship between these two measuring instruments is with other measuring instruments so that it can be concluded which measuring instrument is better. So in the second point below explained further about the contradiction of the results of LSB and PVD measurements based on existing theories.

Before discussing further the results of PSNR and SSIM measurements on the LSB and PVD methods, a histogram image of the baboon image is presented in Fig. 6. The baboon image was chosen as the sample because the PSNR and SSIM values were very contrast in the

Table 2 The PSNR measurement results of each channel image with the LSB method, PVD and CRT

No.	Image	LSB			PVD			CRT		
		Red	Green	Blue	Red	Green	Blue	Red	Green	Blue
1	Lena	51.1323	51.1383	51.1427	44.2833	43.6105	43.5510	42.2077	42.1202	42.1863
2	Peppers	51.1375	51.1722	51.1629	42.6342	41.7204	43.3743	42.3006	41.5044	41.5087
3	House	51.1307	51.1442	51.1308	41.3861	41.3122	41.5997	42.2928	42.0661	41.7099
4	Baboon	51.1477	51.1386	51.1483	36.3776	35.5023	36.2262	42.3602	42.1879	42.3432
5	Bird	51.1430	51.1496	51.1335	43.9549	43.8892	43.3582	42.4301	42.5892	41.9011
6	Oakland	51.1432	51.1371	51.1407	38.8431	42.4378	44.4909	41.7142	42.2449	43.2630
7	Sailboat	51.1377	51.1513	51.1423	42.7913	39.8237	40.0300	42.2243	42.1443	41.9506
8	Splash	51.1497	51.1559	51.1262	44.1600	42.5928	40.9913	42.4066	41.2653	41.7591
9	Tiffany	51.0017	51.1229	51.1265	44.5507	43.7309	44.2100	40.6768	42.1663	41.9235
10	Woodland	51.1480	51.1295	51.1378	41.4952	38.7577	38.5930	42.1729	42.0814	42.2228
11	Car	51.1440	51.1473	51.1416	43.7578	43.7445	43.7741	42.2842	42.3545	42.4341
12	Car2	51.1630	51.1440	51.1253	40.6220	40.5950	40.5510	42.1787	42.2483	42.0509
13	View	51.1449	51.1403	51.2134	36.9822	36.9329	41.9419	42.1325	41.9427	39.3308
14	View2	51.1277	51.1395	51.1380	39.3562	39.5862	39.7300	41.4041	42.3826	42.0278
15	View3	51.1156	51.1363	51.1299	39.5953	39.2522	39.9708	42.2358	42.4024	41.8322
16	View4	51.1333	51.1259	51.1431	43.6927	43.7748	43.9454	42.3914	42.3418	42.3456
17	Doll	51.0970	51.0844	51.1027	39.9239	39.9533	40.4549	41.9866	41.4522	41.7320
18	Cats	51.1436	51.1351	51.1510	42.4196	42.4605	42.5757	42.2447	42.1014	42.3336
19	Cat	51.1399	51.1372	51.1218	43.2695	43.1207	43.1088	42.1204	42.0160	42.1272
20	Blue flower	51.1459	51.1484	51.1443	42.8428	42.6752	42.9102	42.3445	42.3507	42.2138
21	Blue flowers	51.1302	51.1151	51.1114	43.6404	43.5881	43.4052	41.4523	41.4694	41.9412
22	Green flower	51.1903	51.1477	51.1852	43.3105	41.7645	43.1752	40.5307	41.8740	41.2902
23	Green flowers	51.1807	51.1484	51.1903	42.5539	43.4947	42.5030	39.0945	42.1930	38.9667
24	Pink Flower	51.1400	51.1447	51.1463	44.0119	43.7735	43.8448	42.5294	42.1211	41.8851
25	Pink flowers	51.1420	51.1420	51.1432	42.9537	42.6500	42.2061	42.3823	42.3879	42.3368
26	White flowers	51.1467	51.1392	51.1699	40.5874	41.2132	40.9316	41.4712	41.6118	40.6820
27	Sun Flowers	51.1519	51.1364	51.1394	39.5955	40.3877	42.8717	42.5274	42.1663	41.2517
28	Orange Flower	51.1065	51.1537	51.1444	43.1044	43.8110	43.9414	42.4036	42.2226	41.9323
29	Red flower	51.1457	51.1562	51.1599	42.1715	43.2894	43.5268	41.5023	41.2150	41.2728
30	Red flowers	51.1361	51.1321	51.1313	42.7532	43.7071	43.8749	42.5027	42.1127	40.8516
31	Airplane	51.1429	51.1397	51.1362	41.0653	41.4685	42.2137	41.7996	41.8515	41.5889
32	Barbara	51.1252	51.1378	51.1441	43.1727	43.0782	42.9454	42.3372	42.3625	42.2683
33	Boats	51.1500	51.1469	51.1473	43.3244	43.6385	44.0118	42.3867	41.9252	41.5548
34	Goldhill	51.1462	51.1326	51.1573	42.2373	43.5951	43.0021	42.2875	42.3992	42.3600
35	Girl	51.1408	51.1332	51.1360	44.1235	44.1005	44.2202	42.2963	42.4092	42.1023
36	Zelda	51.1286	51.1408	51.1428	44.3256	44.3321	44.4932	42.2162	42.3066	42.3258
37	Monarch	51.1369	51.1384	51.1441	43.6537	43.6919	43.8780	42.3817	42.3179	42.2923
38	Home	51.1298	51.1332	51.1379	41.8568	41.6685	41.5912	42.3274	42.2053	42.3058
39	Dog	51.1501	51.1293	51.1479	44.1105	44.1458	44.1019	42.2931	42.2187	42.1850
40	Fruits	51.1420	51.1425	51.1329	40.0709	40.2314	40.2120	42.1231	42.1860	41.9621
Average		51.1372	51.1392	***51.1438***	42.1390	42.0776	*42.4084*	42.0239	*42.0880*	41.8138

two methods. Based on the results of the histogram presented in Fig. 6, it appears that there are visible changes in the LSB method, whereas the PVD histogram method is still similar to the original image histogram.

The results presented in Fig. 6 are that baboon images have contrasting PSNR and SSIM values, but looking at the histogram presented it appears that the quality of the PVD method imperceptibility is superior compared to LSB. This can be concluded because the histogram is a basic measurement tool that has an important role in image processing. Even shuffling of pixels in the image will not change the image histogram plot. Histogram analysis is also widely used as a basic measuring tool for security and imperceptibility aspects of steganography, even

Table 3 The SSIM measurement results of each channel image with the LSB method, PVD and CRT

No.	Image	LSB			PVD			CRT		
		Red	Green	Blue	Red	Green	Blue	Red	Green	Blue
1	Lena	0.9992	0.9993	0.9992	0.9999	0.9999	0.9999	0.9928	0.9941	0.9932
2	Peppers	0.9967	0.9989	0.9989	0.9999	0.9991	0.9999	0.9936	0.9846	0.9853
3	House	0.9994	0.9993	0.9993	0.9999	0.9999	0.9999	0.9946	0.9947	0.9936
4	Baboon	0.9997	0.9997	0.9998	0.9999	0.9999	0.9999	0.9974	0.9978	0.9981
5	Bird	0.9986	0.9985	0.9985	0.9999	1.0000	0.9999	0.9881	0.9881	0.9875
6	Oakland	0.9998	0.9997	0.9991	0.9999	1.0000	1.0000	0.9981	0.9975	0.9940
7	Sailboat	0.9994	0.9995	0.9993	0.9999	0.9999	0.9999	0.9948	0.9953	0.9936
8	Splash	0.9986	0.9979	0.9987	0.9999	0.9988	0.9999	0.9891	0.9716	0.9881
9	Tiffany	0.9991	0.9993	0.9990	0.9991	0.9999	0.9999	0.9906	0.9943	0.9913
10	Woodland	0.9998	0.9998	0.9998	0.9999	0.9999	0.9999	0.9978	0.9982	0.9983
11	Car	0.9992	0.9993	0.9993	0.9999	1.0000	0.9999	0.9936	0.9938	0.9939
12	Car2	0.9988	0.9988	0.9988	0.9999	0.9999	0.9999	0.9885	0.9889	0.9882
13	View	0.9999	0.9998	0.9988	0.9999	0.9999	0.9980	0.9986	0.9978	0.9640
14	View2	0.9987	0.9986	0.9985	0.9999	0.9999	0.9999	0.9873	0.9888	0.9882
15	View3	0.9992	0.9993	0.9992	0.9997	0.9999	0.9999	0.9942	0.9941	0.9922
16	View4	0.9996	0.9995	0.9996	0.9999	0.9999	0.9999	0.9958	0.9551	0.9960
17	Doll	0.9990	0.9991	0.9992	0.9999	0.9999	0.9999	0.9922	0.9914	0.9930
18	Cats	0.9994	0.9994	0.9995	0.9999	0.9999	0.9999	0.9946	0.9933	0.9955
19	Cat	0.9985	0.9986	0.9989	0.9996	0.9997	0.9997	0.9828	0.9845	0.9878
20	Blue flower	0.9990	0.9990	0.9991	0.9999	0.9999	0.9999	0.9893	0.9899	0.9901
21	Blue flowers	0.9991	0.9991	0.9996	0.9998	0.9998	0.9998	0.9905	0.9902	0.9962
22	Green flower	0.9986	0.9992	0.9987	0.9989	0.9988	0.9993	0.9683	0.9864	0.9791
23	Green flowers	0.9967	0.9991	0.9966	0.9896	0.9999	0.9908	0.8754	0.9919	0.8807
24	Pink Flower	0.9990	0.9993	0.9991	0.9997	0.9999	0.9995	0.9915	0.9918	0.9854
25	Pink flowers	0.9996	0.9997	0.9997	0.9999	0.9999	0.9999	0.9962	0.9967	0.9970
26	White flowers	0.9981	0.9982	0.9980	0.9997	0.9998	0.9991	0.9642	0.9657	0.9540
27	Sun Flowers	0.9995	0.9995	0.9992	0.9999	0.9999	0.9997	0.9961	0.9947	0.9889
28	Orange Flower	0.9987	0.9990	0.9991	0.9994	1.0000	0.9999	0.9895	0.9896	0.9881
29	Red flower	0.9981	0.9974	0.9975	0.9999	0.9961	0.9988	0.9825	0.9496	0.9665
30	Red flowers	0.9996	0.9985	0.9987	0.9999	0.9999	0.9999	0.9968	0.9852	0.9801
31	Airplane	0.9991	0.9991	0.9989	1.0000	0.9999	0.9999	0.9910	0.9913	0.9894
32	Barbara	0.9995	0.9994	0.9995	0.9999	1.0000	0.9999	0.9956	0.9953	0.9956
33	Boats	0.9993	0.9992	0.9985	0.9999	0.9999	0.9983	0.9921	0.9859	0.9707
34	Goldhill	0.9996	0.9995	0.9994	0.9999	0.9999	0.9999	0.9968	0.9959	0.9954
35	Girl	0.9994	0.9994	0.9993	1.0000	1.0000	0.9999	0.9948	0.9946	0.9933
36	Zelda	0.9995	0.9994	0.9993	0.9999	1.0000	0.9999	0.9953	0.9942	0.9939
37	Monarch	0.9994	0.9994	0.9994	0.9999	1.0000	0.9999	0.9933	0.9929	0.9939
38	Home	0.9990	0.9991	0.9991	0.9999	0.9999	0.9999	0.9924	0.9924	0.9934
39	Dog	0.9988	0.9988	0.9989	0.9997	0.9997	0.9997	0.9892	0.9891	0.9897
40	Fruits	0.9995	0.9995	0.9996	0.9999	0.9999	0.9999	0.9952	0.9951	0.9948
Average		0.9990	*0.9991*	0.9990	0.9996	***0.9997***	0.9995	0.9885	*0.9891*	0.9860

in some more recent steganographic methods suggest modifying the histogram to embed messages.

Besides, more specifically, security tests were also carried out in this research considering that a steganographic method, in general, must meet imperceptibility, capacity, and security aspects [13, 21, 28]. The security test is carried out using the Regular and Singular (RS) analysis, which is a type of statistical analysis on steganography, which, if briefly explained, uses a small modification of the LSB value of the image pixels and a differentiation function to classify the pixels of the stego image into regular and singular groups. In this way, the probability of the message size embedded in the group frequency will be detected. So with

Table 4 The PSNR measurement results (Max Payload) of each channel image with the LSB and PVD method

No.	Image	Max Payload (in BPP)			PSNR (dB)					
		Channel			PVD	LSB	PVD	LSB	PVD	LSB
		Red	Green	Blue	Red		Green		Blue	
1	Lena	1.5118	1.5246	1.5243	42.5188	45.7495	41.8079	45.6981	41.8624	45.6869
2	Peppers	1.5364	1.5409	1.5262	40.4276	45.6737	39.9221	45.5947	41.3738	45.6110
3	House	1.5586	1.5567	1.5461	39.7468	45.6068	39.8018	45.6445	40.2909	45.6412
4	Baboon	1.6721	1.7080	1.6967	34.1093	45.2907	32.9464	45.1873	33.4548	45.2511
5	Bird	1.5044	1.5030	1.5024	42.2024	45.7786	42.1400	45.7773	41.7918	45.7910
6	Oakland	1.6727	1.5965	1.5114	36.1913	45.2796	40.4681	45.5090	42.7234	45.7509
7	Sailboat	1.5505	1.5945	1.5804	41.0545	45.6344	37.5519	45.4595	37.0865	45.5029
8	Splash	1.5033	1.5171	1.5185	42.2692	45.7737	40.4314	45.6533	39.1665	45.7189
9	Tiffany	1.5143	1.5259	1.5130	42.7659	44.6846	41.9275	45.5146	42.2714	45.7095
10	Woodland	1.5920	1.6151	1.6276	39.6321	45.5030	37.4838	45.4310	37.0998	45.4309
11	Car	1.5246	1.5249	1.5256	41.8075	45.7539	41.7780	45.7453	41.7854	45.7027
12	Car2	1.5451	1.5446	1.5439	38.6039	45.6386	38.6636	45.6554	38.5178	45.6075
13	View	1.6737	1.6694	1.5656	34.5616	45.2779	34.4631	45.3129	40.0942	45.4473
14	View2	1.5654	1.5613	1.5589	37.8510	45.5578	37.9941	45.6344	38.1659	45.6255
15	View3	1.5955	1.5975	1.6021	36.8015	45.3744	36.6532	45.5078	36.3397	45.4909
16	View4	1.5403	1.5350	1.5349	41.5113	45.6065	41.8100	45.6789	41.9498	45.6940
17	Doll	1.5357	1.5375	1.5378	38.7941	45.1724	38.7483	45.1430	39.1869	45.1673
18	Cats	1.5433	1.5437	1.5448	40.7899	45.6295	40.8564	45.6619	40.8998	45.6511
19	Cat	1.5163	1.5164	1.5163	41.7062	45.7211	41.5456	45.7239	41.5280	45.7649
20	Blue flower	1.5149	1.5166	1.5170	41.2244	45.7309	41.1033	45.7299	41.3034	45.7047
21	Blue flowers	1.5201	1.5206	1.5343	41.8443	45.4242	41.7363	45.4324	41.4888	45.3414
22	Green flower	1.5242	1.5374	1.5258	41.1648	45.6664	39.9841	45.7021	40.9246	45.6440
23	Green flowers	1.5312	1.5385	1.5240	40.5393	45.7136	40.7118	45.6368	40.9985	45.7149
24	Pink Flower	1.5086	1.5110	1.5115	42.1271	45.6233	41.9899	45.7389	42.0255	45.7277
25	Pink flowers	1.5252	1.5298	1.5349	41.1662	45.6648	40.7679	45.6942	40.2045	45.6550
26	White flowers	1.5350	1.5354	1.5391	38.7295	45.6621	39.2402	45.6726	38.9773	45.6379
27	Sun Flowers	1.5847	1.5779	1.5564	37.6078	45.4922	38.4609	45.5641	40.9474	45.5879
28	Orange Flower	1.5086	1.5081	1.5080	41.3747	45.4511	42.0070	45.7518	42.1295	45.7512
29	Red flower	1.5144	1.5089	1.5065	40.4289	45.7479	41.1360	45.8240	41.5949	45.6297
30	Red flowers	1.5307	1.5077	1.5074	41.2957	45.6697	41.9681	45.7407	42.0894	45.7714
31	Airplane	1.5316	1.5369	1.5213	39.6941	45.6866	39.7589	45.6298	40.5864	45.6585
32	Barbara	1.5605	1.5560	1.5615	41.2980	45.6049	41.2742	45.6142	41.1789	45.6044
33	Boats	1.5351	1.5313	1.5294	41.5284	45.6626	41.8503	45.6879	42.1785	45.7118
34	Goldhill	1.5527	1.5288	1.5333	40.6097	45.6240	41.8687	45.7031	41.3051	45.6918
35	Girl	1.5120	1.5106	1.5109	42.3544	45.7466	42.2890	45.7542	42.4270	45.7572
36	Zelda	1.5130	1.5078	1.5058	42.5622	45.7533	42.5367	45.7731	42.7440	45.7593
37	Monarch	1.5309	1.5290	1.5242	41.7004	45.6776	41.7285	45.7134	41.8909	45.7096
38	Home	1.5405	1.5422	1.5447	40.3138	45.5806	40.1051	45.6349	40.0430	45.6568
39	Dog	1.5055	1.5037	1.5040	42.2791	45.7332	42.3146	45.6867	42.2730	45.7324
40	Fruits	1.5720	1.5714	1.5819	38.3270	45.5826	38.3186	45.5962	38.5118	45.5540
Average					40.2879	**45.5801**	40.2036	**45.6203**	40.5353	**45.6312**

RS analysis can detect whether or not a message [21]. Fig. 7 is presented the data from the RS analysis where each container image is embedded with a 1-bpp text message on each channel so that from 40 container images a message is embedded six times using the LSB and PVD methods on each color channel. The 1-bpp capacity on each color channel is one-third bpp for each whole image. The value of RS analysis states that the average value of embedded messages in the stego image is 38.03% for LSB and 7.15% for PVD. The probability of the message size embedded in the measurement results of the RS analysis shows that the results

Table 5 The SSIM measurement results (Max Payload) of each channel image with the LSB and PVD method

No.	Image	Max Payload (in BPP)			SSIM					
		Channel			PVD	LSB	PVD	LSB	PVD	LSB
		Red	Green	Blue	Red		Green		Blue	
1	Lena	1.5118	1.5246	1.5243	0.9999	0.9968	0.9999	0.9974	0.9999	0.9969
2	Peppers	1.5364	1.5409	1.5262	0.9999	0.9971	0.9983	0.9963	0.9986	0.9962
3	House	1.5586	1.5567	1.5461	0.9999	0.9979	0.9999	0.9979	0.9999	0.9978
4	Baboon	1.6721	1.7080	1.6967	0.9999	0.9987	0.9999	0.9990	0.9999	0.9990
5	Bird	1.5044	1.5030	1.5024	0.9999	0.9944	1.0000	0.9942	0.9999	0.9941
6	Oakland	1.6727	1.5965	1.5114	0.9998	0.9992	1.0000	0.9988	1.0000	0.9966
7	Sailboat	1.5505	1.5945	1.5804	0.9999	0.9978	0.9999	0.9980	0.9999	0.9973
8	Splash	1.5033	1.5171	1.5185	0.9999	0.9952	0.9956	0.9912	0.9999	0.9956
9	Tiffany	1.5143	1.5259	1.5130	0.9986	0.9964	0.9998	0.9972	0.9999	0.9964
10	Woodland	1.5920	1.6151	1.6276	0.9999	0.9990	0.9999	0.9992	0.9999	0.9992
11	Car	1.5246	1.5249	1.5256	0.9999	0.9976	1.0000	0.9976	0.9999	0.9974
12	Car2	1.5451	1.5446	1.5439	0.9998	0.9949	0.9999	0.9945	0.9999	0.9945
13	View	1.6737	1.6694	1.5656	0.9998	0.9995	0.9998	0.9995	0.9970	0.9958
14	View2	1.5654	1.5613	1.5589	0.9999	0.9933	0.9999	0.9922	0.9998	0.9923
15	View3	1.5955	1.5975	1.6021	0.9995	0.9961	0.9999	0.9960	0.9999	0.9958
16	View4	1.5403	1.5350	1.5349	0.9999	0.9982	0.9999	0.9984	0.9999	0.9986
17	Doll	1.5357	1.5375	1.5378	0.9995	0.9962	0.9996	0.9966	0.9996	0.9969
18	Cats	1.5433	1.5437	1.5448	0.9999	0.9978	0.9999	0.9974	0.9999	0.9978
19	Cat	1.5163	1.5164	1.5163	0.9992	0.9926	0.9995	0.9936	0.9996	0.9952
20	Blue flower	1.5149	1.5166	1.5170	0.9999	0.9962	0.9999	0.9965	0.9999	0.9966
21	Blue flowers	1.5201	1.5206	1.5343	0.9996	0.9972	0.9997	0.9972	0.9997	0.9983
22	Green flower	1.5242	1.5374	1.5258	0.9985	0.9946	0.9987	0.9965	0.9990	0.9946
23	Green flowers	1.5312	1.5385	1.5240	0.9848	0.9971	0.9999	0.9958	0.9859	0.9777
24	Pink Flower	1.5086	1.5110	1.5115	0.9997	0.9959	0.9999	0.9972	0.9993	0.9968
25	Pink flowers	1.5252	1.5298	1.5349	0.9999	0.9985	0.9999	0.9987	0.9999	0.9989
26	White flowers	1.5350	1.5354	1.5391	0.9953	0.9942	0.9954	0.9945	0.9943	0.9946
27	Sun Flowers	1.5847	1.5779	1.5564	0.9999	0.9977	0.9999	0.9976	0.9995	0.9968
28	Orange Flower	1.5086	1.5081	1.5080	0.9991	0.9947	1.0000	0.9965	0.9998	0.9967
29	Red flower	1.5144	1.5089	1.5065	0.9999	0.9922	0.9960	0.9868	0.9985	0.9893
30	Red flowers	1.5307	1.5077	1.5074	0.9999	0.9986	0.9999	0.9942	0.9999	0.9950
31	Airplane	1.5316	1.5369	1.5213	1.0000	0.9968	0.9999	0.9967	0.9999	0.9961
32	Barbara	1.5605	1.5560	1.5615	0.9999	0.9982	1.0000	0.9981	0.9999	0.9982
33	Boats	1.5351	1.5313	1.5294	0.9996	0.9975	0.9995	0.9970	0.9961	0.9967
34	Goldhill	1.5527	1.5288	1.5333	0.9999	0.9986	0.9999	0.9981	0.9999	0.9978
35	Girl	1.5120	1.5106	1.5109	1.0000	0.9980	1.0000	0.9978	0.9999	0.9975
36	Zelda	1.5130	1.5078	1.5058	1.0000	0.9981	1.0000	0.9979	0.9999	0.9977
37	Monarch	1.5309	1.5290	1.5242	0.9999	0.9972	1.0000	0.9971	0.9999	0.9974
38	Home	1.5405	1.5422	1.5447	0.9999	0.9965	0.9999	0.9968	0.9999	0.9972
39	Dog	1.5055	1.5037	1.5040	0.9996	0.9952	0.9996	0.9950	0.9997	0.9955
40	Fruits	1.5720	1.5714	1.5819	0.9999	0.9985	0.9999	0.9985	0.9999	0.9985
Average					**0.9993**	0.9968	**0.9995**	0.9965	**0.9991**	0.9960

are closer to the LSB method, so it can be concluded that the LSB method is easier to detect the presence or absence of a message, on the other hand the PVD method has better performance in terms of message security.

From the various tests that have been done above, it can be concluded that SSIM is more logical for measuring the quality of imperceptibility in image steganography, because the results are closer to various aspects. However, it would be better if the imperceptibility measurement of a stego image is measured by at least two measuring instruments, namely

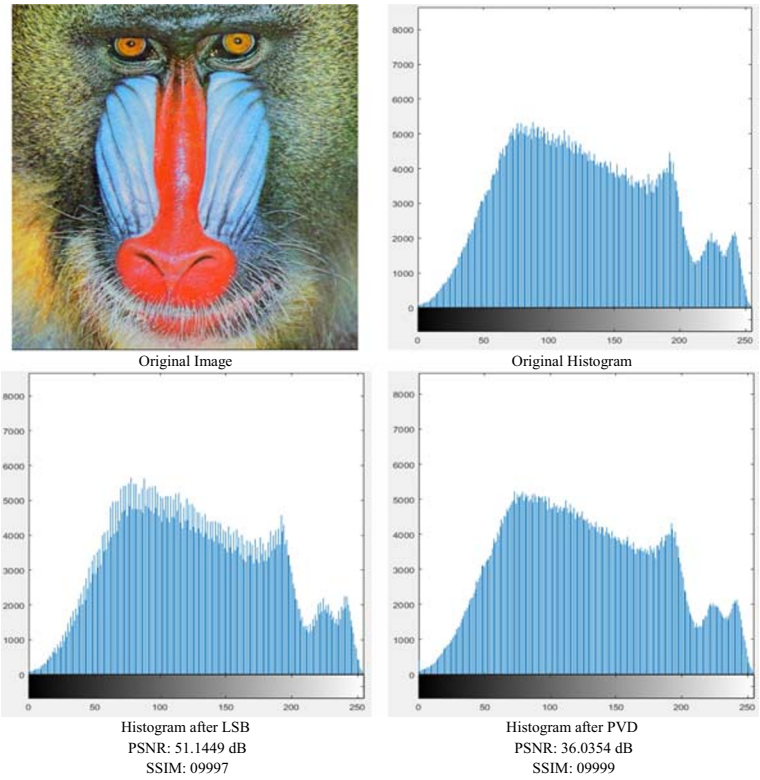

Fig. 6 Histogram of Baboon Image

SSIM and PSNR to obtain more complete data. Another thing to note is that based on the analysis and experiments that have been carried out, a very small difference in value may not

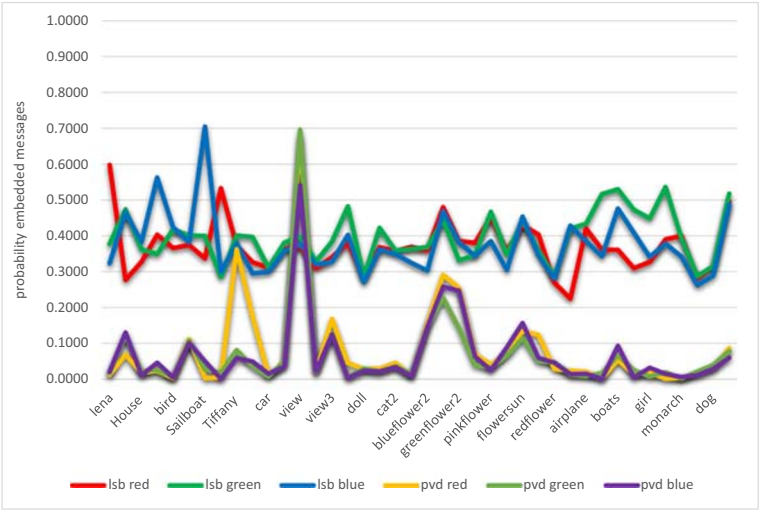

Fig. 7 RS analysis results of All Image

even be significant in SSIM (because it is more than two digits behind the comma) can produce values that are far different if measured by PSNR. This means that measurement with SSIM should be measured at least four digits behind the comma because the change in the SSIM value that is very small is also sensitive to changes in image histograms and image degradation. For example, in Fig. 6 the difference in the SSIM value of only 0.0002 results in a PSNR difference of more than 15 dB. The last thing that needs to be underlined is that steganographic images on grayscale images and color images have different effects, on research conducted [3] the same comparison is done on the grayscale baboon image, the result is PSNR and SSIM agree that the LSB method is better, while the color baboon image produces different values. This confirms that the theory stated in the article written by [2, 46] proven valid and following the results of this research.

6 Conclusions

Measurement of the quality of imperceptibility in the steganography image method is something that must be done to measure the contribution of the proposed steganography method. Several measuring tools have been used to measure imperceptibility, i.e. PSNR, SSIM, and image histogram. PSNR is the most favorite measurement tool because it has simple computation and is considered valid because it has been used in many image processing types of research in the world. But PSNR has a weakness to measure fidelity signal where it is very closely related to imperceptibility in steganographic images. Based on the results of tests on this research SSIM has a better sensitivity to detect distortions that occur due to embedding messages on steganographic color images when compared with PSNR, this is due to the way SSIM works that are designed based on the human visual system. SSIM is calculated based on the luminance, contrast, and structure of the original container image and stego image. The results of the image histogram plot also reinforce the assumption that, logically, SSIM is more suitable for measuring imperceptibility in steganographic images. So with the results of this research, it is recommended the use of SSIM measurement tools in all research data hiding especially image steganography in the spatial domain.

Acknowledgments The author received no financial support for the research, authorship, and/or publication of this article.

References

1. Abdulla AA, Sellahewa H, Jassim SA (2019) Improving embedding efficiency for digital steganography by exploiting similarities between secret and container images. Multimed Tools Appl 78:17799–17823. https://doi.org/10.1007/s11042-019-7166-7
2. Abraham J, Paul V (2019) An imperceptible spatial domain color image watermarking scheme. J King Saud Univ - Comput Inf Sci 31:125–133. https://doi.org/10.1016/j.jksuci.2016.12.004
3. Aini DN, Setiadi DRIM, Putro SN, et al (2019) Survey of methods in the spatial domain image steganography based imperceptibility and payload capacity. In: proceedings - 2019 international seminar on application for Technology of Information and Communication: industry 4.0: retrospect, Prospect, and challenges, iSemantic 2019. Institute of Electrical and Electronics Engineers Inc., Semarang, pp 434–439
4. Akbar JM, Setiadi DRIM (2019) Joint method using Akamatsu and discrete wavelet transform for image restoration. Appl Comput Inform https://doi.org/10.1016/J.ACI.2019.10.002, ahead-of-print

5. Al-Dmour H, Al-Ani A (2015) Quality optimized medical image steganography based on edge detection and hamming code. In: Proceedings - international symposium on biomedical imaging. IEEE Computer Society, New York, pp 1486–1489
6. Aqeel I, Raheel M (2019) Digital image steganography by using a hash based LSB (3-2-3) technique. In: Communications in Computer and Information Science. Springer Verlag, Bahawalpur, pp 713–724
7. Arun C, Murugan S (2018) Design of image steganography using LSB XOR substitution method. In: Proceedings of the 2017 IEEE international conference on communication and signal processing, ICCSP 2017. Institute of Electrical and Electronics Engineers Inc., Chennai, pp 674–677
8. Astuti YP, Setiadi DRIM, Rachmawanto EH, Sari CA (2018) Simple and secure image steganography using LSB and triple XOR operation on MSB. In: 2018 International conference on information and communications technology, ICOIACT 2018. Yogyakarta
9. Bovik AC (2009) The essential guide to image processing. Academic Press, Austin
10. Brunet D, Vrscay ER, Wang Z (2012) On the mathematical properties of the structural similarity index. IEEE Trans Image Process 21:1488–1495. https://doi.org/10.1109/TIP.2011.2173206
11. Chakraborty S, Jalal AS, Bhatnagar C (2017) LSB based non blind predictive edge adaptive image steganography. Multimed Tools Appl 76:7973–7987. https://doi.org/10.1007/s11042-016-3449-4
12. Chatterjee A, Ghosal SK, Sarkar R (2020) LSB based steganography with OCR: an intelligent amalgamation. Multimed tools Appl 1–19. https://doi.org/10.1007/s11042-019-08472-6
13. Cheddad A, Condell J, Curran K, Mc Kevitt P (2010) Digital image steganography: survey and analysis of current methods. Signal Process 90:727–752
14. Darbani A, Alyannezhadi MM, Forghani M (2019) A new steganography method for embedding message in JPEG images. In: 2019 IEEE 5th conference on knowledge based engineering and innovation, KBEI 2019. Institute of Electrical and Electronics Engineers Inc., Tehran, pp 617–621
15. Douglas M, Bailey K, Leeney M, Curran K (2018) An overview of steganography techniques applied to the protection of biometric data. Multimed Tools Appl 77:17333–17373. https://doi.org/10.1007/s11042-017-5308-3
16. Grover R, Yadav DK, Chauhan DK, Kamya S (2018) Adaptive steganography via image complexity analysis using 3D color texture feature. In: 3rd international conference on innovative applications of computational intelligence on power, energy and controls with their impact on humanity, CIPECH 2018. Institute of Electrical and Electronics Engineers Inc., Ghaziabad, pp 125–129
17. Gupta A, Ahuja S (2018) An improved image steganography technique using block division least significant bit approach. In: Proceedings - IEEE 2018 international conference on advances in computing, communication control and networking, ICACCCN 2018. Institute of Electrical and Electronics Engineers Inc., Greater Noida, pp 335–339
18. Gutub A, Al-Ghamdi M (2020) Hiding shares by multimedia image steganography for optimized counting-based secret sharing. Multimed Tools Appl 1–35. https://doi.org/10.1007/s11042-019-08427-x
19. Hore A, Ziou D (2010) Image quality metrics: PSNR vs. SSIM. In: 2010 20th international conference on pattern recognition. IEEE, Istanbul, pp 2366–2369
20. Horé A, Ziou D (2013) Is there a relationship between peak-signal-to-noise ratio and structural similarity index measure? IET Image Process 7:12–24. https://doi.org/10.1049/iet-ipr.2012.0489
21. Hussain M, Wahab AWA, Bin IYI et al (2018) Image steganography in spatial domain: a survey. Signal Process Image Commun 65:46–66. https://doi.org/10.1016/j.image.2018.03.012
22. Islam AU, Khalid F, Shah M et al (2017) An improved image steganography technique based on MSB using bit differencing. In: 2016 6th international conference on innovative computing technology, INTECH 2016. Institute of Electrical and Electronics Engineers Inc., Dublin, pp 265–269
23. 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
24. Krasula L, Le Callet P, Fliegel K, Klima M (2017) Quality assessment of sharpened images: challenges, methodology, and objective metrics. IEEE Trans Image Process 26:1496–1508. https://doi.org/10.1109/TIP.2017.2651374
25. Lee CF, Weng CY, Chen KC (2017) An efficient reversible data hiding with reduplicated exploiting modification direction using image interpolation and edge detection. Multimed Tools Appl 76:9993–10016. https://doi.org/10.1007/s11042-016-3591-z
26. Li X, Wang W, Wang W, Ding XL, Yin Q (2014) Optimal estimates of common remainder for the robust Chinese remainder theorem. Commun Nonlinear Sci Numer Simul 19:2373–2381. https://doi.org/10.1016/J.CNSNS.2013.10.034
27. Liao X, Yin J, Chen M, Qin Z (2020) Adaptive payload distribution in multiple images steganography based on image texture features. IEEE trans dependable Secur Comput 1–1. https://doi.org/10.1109/tdsc.2020.3004708

28. Liao X, Yu Y, Li B, Li Z, Qin Z (2020) A new payload partition strategy in color image steganography. IEEE Trans Circuits Syst Video Technol 30:685–696. https://doi.org/10.1109/TCSVT.2019.2896270
29. Min X, Ma K, Gu K, Zhai G, Wang Z, Lin W (2017) Unified blind quality assessment of compressed natural, graphic, and screen content images. IEEE Trans Image Process 26:5462–5474. https://doi.org/10.1109/TIP.2017.2735192
30. Muhammad K, Ahmad J, Rehman NU, Jan Z, Sajjad M (2017) CISSKA-LSB: color image steganography using stego key-directed adaptive LSB substitution method. Multimed Tools Appl 76:8597–8626. https://doi.org/10.1007/s11042-016-3383-5
31. Mukherjee S, Sanyal G (2019) Edge based image steganography with variable threshold. Multimed Tools Appl 78:16363–16388. https://doi.org/10.1007/s11042-018-6975-4
32. Pak C, Kim J, An K, Kim C, Kim K, Pak C (2020) A novel color image LSB steganography using improved 1D chaotic map. Multimed Tools Appl 79:1409–1425. https://doi.org/10.1007/s11042-019-08103-0
33. Patel N, Meena S (2017) LSB based image steganography using dynamic key cryptography. In: 2016 International conference on emerging trends in communication technologies, ETCT 2016. Institute of Electrical and Electronics Engineers Inc., Dehradun
34. Rashid RD, Majeed TF (2019) Edge based image steganography: Problems and solution. In: 2019 3rd international conference on communications, signal processing, and their applications, ICCSPA 2019. Institute of Electrical and Electronics Engineers Inc., Sharjah
35. Rehman A, Wang Z (2012) Reduced-reference image quality assessment by structural similarity estimation. IEEE Trans Image Process 21:3378–3389. https://doi.org/10.1109/TIP.2012.2197011
36. Setiadi DRIM (2019) Payload enhancement on least significant bit image steganography using edge area dilation. Intl J Electron Telecommun 65:295–300. https://doi.org/10.24425/ijet.2019.126313
37. Setiadi DRIM (2019) Improved payload capacity in LSB image steganography uses dilated hybrid edge detection. J King Saud Univ - Comput Inf Sci https://doi.org/10.1016/j.jksuci.2019.12.007
38. Setiadi DRIM, Santoso HA, Rachmawanto EH, Sari CA (2018) An improved message capacity and security using divide and modulus function in spatial domain steganography. In: 2018 international conference on information and communications technology (ICOIACT). IEEE, Yogyakarta, pp 186–190
39. Sheikh HR, Bovik AC (2006) Image information and visual quality. IEEE Trans Image Process 15:430–444. https://doi.org/10.1109/TIP.2005.859378
40. Shukla AK, Pandey RK, Reddy PK (2020) Generalized fractional derivative based adaptive algorithm for image denoising. Multimed tools Appl 1–24. https://doi.org/10.1007/s11042-020-08641-y
41. Singh A, Singh H (2015) An improved LSB based image steganography technique for RGB images. In: Proceedings of 2015 IEEE international conference on electrical, computer and communication technologies, ICECCT 2015. Institute of Electrical and Electronics Engineers Inc., Coimbatore
42. Solomon C, Breckon T (2011) Fundamentals of digital image processing
43. Subhedar MS, Mankar VH (2019) Secure image steganography using framelet transform and bidiagonal SVD. Multimed tools Appl 1–22. https://doi.org/10.1007/s11042-019-08221-9
44. Subong RA, Fajardo AC, Kim YJ (2018) LSB Rotation and Inversion Scoring Approach to Image Steganography. In: Proceeding of 2018 15th international joint conference on computer science and software engineering, JCSSE 2018. Institute of Electrical and Electronics Engineers Inc., Nakhonpathom
45. Sudibyo U, Eranisa F, Rachmawanto EH, et al (2018) A secure image watermarking using Chinese remainder theorem based on haar wavelet transform. In: proceedings - 2017 4th international conference on information technology, computer, and electrical engineering, ICITACEE 2017
46. Sundararajan D (2017) Color image processing. In: Digital Image Processing. Springer Singapore, Singapore, pp 407–438
47. Tan HL, Li Z, Tan YH et al (2013) A perceptually relevant mse-based image quality metric. IEEE Trans Image Process 22:4447–4459. https://doi.org/10.1109/TIP.2013.2273671
48. Verma V, Muttoo SK, Singh VB (2019) Enhanced payload and trade-off for image steganography via a novel pixel digits alteration. Multimed tools Appl 1–20. https://doi.org/10.1007/s11042-019-08283-9
49. Wang W (2020) An efficient multiple-bit reversible data hiding scheme without shifting. Multimed Tools Appl 79:555–579. https://doi.org/10.1007/s11042-019-08065-3
50. Wang Z, Bovik AC (2009) Mean squared error: lot it or leave it? A new look at signal fidelity measures. IEEE Signal Process Mag 26:98–117. https://doi.org/10.1109/MSP.2008.930649
51. Wang Z, Bovik AC, Sheikh HR, Simoncelli EP (2004) Image quality assessment: from error visibility to structural similarity. IEEE Trans Image Process 13:600–612. https://doi.org/10.1109/TIP.2003.819861
52. Wu D-C, Tsai W-H (2003) A steganographic method for images by pixel-value differencing. Pattern Recogn Lett 24:1613–1626. https://doi.org/10.1016/S0167-8655(02)00402-6