Soft Computing (2024) 28:8963–8976
https://doi.org/10.1007/s00500-023-09130-8

APPLICATION OF SOFT COMPUTING

Digital image steganography: challenges, investigation, and recommendation for the future direction

Alan Anwer Abdulla[1]

Accepted: 17 August 2023 / Published online: 1 September 2023

Abstract

Performance measurements which characterize digital image steganography techniques include payload capacity, stego image quality, and security (secret message detectability). Increasing payload capacity leads to diminishing both stego image quality and security. Conversely, a high stego image quality and a high security cannot be obtained without compromising payload capacity. It has become essential but increasingly challenging to achieve a balance between these image steganography requirements. The direction of recent contributions in the area of image steganography can be classified into two different approaches. The first approach is the development of techniques based on embedding efficiency in which the secret message hides while minimizing the embedding distortion in the cover image. The second approach is the development of techniques based on distortion function related to statistical detectability in which the secret message conceals in certain parts of the cover image determined by the defined distortion function such as textured or noisy regions. This study aims to provide the insight for the researchers about future works and pave away for them to design efficient steganography techniques. It practically analyzes and investigates which of the two approaches can attain all the requirements of image steganography simultaneously. Comprehensive experiments have been conducted on a large-scale benchmark dataset which demonstrate that increasing the embedding efficiency reflects on increasing stego image quality as well as security without compromising payload capacity. The experimental findings reveal that the virtual designed steganography technique, LSB_EE_20, achieved the optimum results, with an embedding efficiency of 20, a PRNR of 62, and a message detectability of 0.11%. Consequently, this paper recommends that the researchers in this area concentrate on developing embedding techniques in which the embedding efficiency increases rather than focusing on distortion function.

Keywords Adaptive steganography · Distortion function · Embedding efficiency · Steganalysis · Stego image

1 Introduction

The dramatic developments in digital communication technologies and significant computer power increase contributed to an exponential evolution in Internet use for various governmental, economic, and social communications that involve transmission of a wide variety of multimedia files and complex data. It became a major challenge to secure the content of confidential and personal transactions on open networks. Thus, the multimedia and information security research area attract considerable interest, and its application scope is expanding rapidly. Communication protection mechanisms have been developed and investigated with encryption and digital steganography being the two extreme apparent approaches to secure information and multimedia privacy. Encryption turns a secret message into a noise-like, visible yet meaningless data, whereas digital steganography focuses on hiding the existence of secret information during routine communication sessions. Despite the fact that steganographers tend to develop successful and hard-to-reveal steganography techniques, steganalyzers attempt to defeat the purpose of steganography by revealing the existence of the concealed secrets, even though they cannot retrieve them.

✉ Alan Anwer Abdulla
alananwer@yahoo.com

[1] Department of Information Technology, College of Commerce, University of Sulaimani, Sulaimani, Iraq

Digital image steganography is useful in protecting sensitive communications for many applications such as intelligence and law enforcing agencies to prevent crime, military purposes such as exchanging military maps, in healthcare systems to maintain the privacy of critical information such as medical records, and in financial and business organizations such as banks to prevent customers' account information from being accessed illegally by unauthorized users, or identity cards, where individuals' details are embedded in their photographs (Cox et al. 2007).

In general, the object to be used to conceal the secret messages is called the cover medium, and the object in which the information is hidden is referred to as the stego medium. Multimedia files such as videos, images, and audio are rich cover file sources as these files contain vast quantities of redundancies, covering messages without any considerable impact on the contents of the information or the quality of stego file. Additionally, images are frequently exchanged over the Internet and attract less suspicion as opposed to other digital media. The criteria of success of image steganography techniques are the list of very competitive demands on: (1) stego image quality; (2) payload capacity; and (3) message detectability (Cox et al. 2007). Mostly, the essential shortcoming of the most image steganography techniques is that modifies the statistics of an image post secret embedding perhaps discover by steganalysis techniques (Lin et al. 2010).

In modern image steganography techniques, two approaches are explored, namely distortion function and embedding efficiency, to produce a robust stego image to withstand against steganalysis techniques. The strategy that constrains secret embedding in noisy or textured regions and avoiding smooth and clean edge regions can be determined by a function called distortion functions (Ker et al. 2013). The concept is established on the fact that noisy regions or complex texture is not easy to model directly, but certain functions that relate a pixel to its surrounding region can estimate their distortion (Holub and Fridrich 2012; Holub et al. 2014). Steganography techniques based on defining distortion functions to determine the noisy regions and texture have a characteristic of decreasing the message detectability for the steganography techniques, but restrict the payload capacity especially if the cover image consists of a high rate of smooth regions. In contrast, steganography techniques based on embedding efficiency aim to minimize the embedding distortion without reducing the amount of the concealed information, producing a robust stego image to withstand steganalysis attacks. Meanwhile, decreasing the amount of modified cover pixels after information concealment improves the opportunity of success. Indeed, decreasing the ratio of modified pixels to the payload capacity has recently proposed as an indicator of lower message detectability and higher stego image quality. Consequently, the embedding efficiency (EE) of a hiding technique can be defined as (Abdulla 2015; Abdulla et al. 2019):

$$\mathrm{EE} = \frac{1}{\text{ratio of modified pixels}} \tag{1}$$

where ratio of modified pixels refers to the noise added in cover image as a result of message hiding for a given secret information length and can be measured by bit per pixel (bpp). For example, if the ratio of pixel change for a given steganography technique is 0.5, such technique adds $0.5p$ of the noise in the cover image pixels, where p is the concealing rate in bpp. The embedding efficiency for such a steganography technique is equal to 2 based on Eq. (1). The higher EE means the less detectable traces is introduced in the stego image, and the more robust the technique is against steganalysis techniques.

The research problem in this area is increasing payload capacity leads to diminishing both stego image quality and security. Conversely, a high stego image quality and a high security cannot be obtained without compromising payload capacity. The gap in the previous techniques is increasingly challenging to achieve a balance between these image steganography requirements. The importance and the essential objective of this study were to provide the insight for the researchers about future works and pave away for them to design efficient steganography techniques by analyzing and investigating which of the two mentioned approaches above plays a significant role in image steganography and fulfills all the required image steganography measurements. The main contribution of this study is practically demonstrated and justified the suggested recommendation in this paper for the future direction. The rest of the paper is organized as follows. Section 2 gives the background. Section 3 provides literature survey. The success criteria for image steganography techniques are described in Sect. 4. Section 5 illustrates the practical analyses and investigation. Finally, concluding remarks and future direction recommendation are drawn in Sect. 6.

2 Background

In image steganography techniques, the secret bit-stream can be concealed due to substituting the bit of the chosen bit-plane of the cover image pixel with the secret bit based on the agreed order of the cover image pixels. The binary representation of pixels' value of the cover image consists of eight bit-planes for the grayscale images, and the most significant bit-plane (MSB) involves most important information, while the least significant bit-plane (LSB) involves the least important information. The most common image steganography technique that uses cover pixel's LSB to represent the secret bit was first explored by Bender et al. (1996), and its details are explained in Chan and Cheng (2004); Thien and Lin (2003). In the literature, this technique is known as the least significant bit replacement (LSBR) and the reason behind its widely used stems from simplicity of implementation and visual imperceptibility. LSBR provides full payload capacity since each pixel of the cover image can be exploited to hide information, and it is hard to notice a modification in the pixel value by the naked eye. It was first used by replacing the secret bits with cover pixels' LSB in sequential order, and it is called LSBR sequentially. This technique has a limitation of security, since steganalysis techniques can simply extract the LSB of the cover pixels to quickly recover the concealed information (Hempstalk 2006). This deficiency of the LSBR sequentially can therefore be resolved by using the pseudorandom number generator (PRNG) to randomly spread the secret information through the cover image on the basis of a seed set by the sender, rather of concealing the secrets in sequential order (Hempstalk 2006), and such technique refers as LSBR randomly (Provos and Honeyman 2003). The receiver should use the same PRNG to extract the secret bits from the pixels' LSB of the stego image.

Both LSBR sequentially and LSBR randomly have a limitation of asymmetry problem. The asymmetry issue can be defined as the imbalance that produced due to increasing/decreasing even/odd pixel values either by one or leave unmodified; as a result, this creates distorting the statistical distribution in the pixel values (0, 1); (2, 3);... (254, 255) (Luo et al. 2010). The issue of asymmetry can be exploited, even at a low rate of embedding, to reveal the presence of the concealed information using some targeted steganalysis techniques. To resolve the unwanted asymmetry drawback of LSBR-based embedding techniques, the decision of altering the least significant bit can be randomized, i.e., if the secret bit does not match the pixel's LSB of the cover image, then randomly increase or decrease the cover pixel value by one. This technique is commonly referred to as LSB Matching (LSBM) that was proposed by Sharp (2001). Once the secret information is concealed, the stego pixel's LSB reflects a hidden bit and the message can be retrieved simply by extracting it from the recipient side. The embedding technique based on LSBM has a property over LSBR, in which the asymmetry issue does not occur. Additionally, with good visual imperceptibility, LSBM has the same payload capacity as LSBR has. Ker (2005) has indicated that by only randomizing the modification, the LSBM-based embedding technique fixes the asymmetric downside.

Generally, image steganography approaches are categorized into adaptive and non-adaptive (Agaian et al. 2007). In adaptive approaches, the embedding capacity and locations rely on the statistical features of the cover image, i.e., some parts/regions of the cover image are excluded for hiding purposes (Westfeld 2001). Steganography techniques based on defined distortion function are considered as an adaptive approach. In non-adaptive approaches, concealing the secrets is not based on the cover image features and each pixel of the cover image can be exploited for information concealment. Steganography techniques based on embedding efficiency are considered as non-adaptive approach. Accordingly, embedding capacity is higher in non-adaptive steganography techniques than in adaptive techniques.

In the literature, however, it is argued that adaptive based steganography techniques are stronger toward steganalysis techniques, because the secrets are concealed in noisy regions, but they have a disadvantage in terms of payload capacity (Westfeld 2001). In image steganography techniques, message detectability can be recognized as the most considerable criterion.

In Wang et al. (2010) specified two potential approaches to improve the security of image steganography techniques: (1) increasing the embedding efficiency, i.e., reducing the embedding modifications at a specified rate of embedding, and (2) hiding the secret bit into the pixels of the cover image only in the unnoticeable regions of the cover image such as the noisy regions of an image based on defined distortion function (Wang et al. 2010).

In 2013, Ker et al. recognized and identified the shortcomings of steganography and steganalysis techniques that need to be addressed seriously in future studies. The two key drawbacks highlighted, which are important for the image steganography, are: (1) developing embedding efficiency-based techniques that conceal the secrets while minimizing embedding distortion and (2) developing distortion function-based techniques in which secrets are concealed in the cover image parts specified by the defined distortion function (Ker et al. 2013).

3 Literature survey

This section concerns with reviewing the works relating to the two security-related issues of image steganography techniques, namely distortion function and embedding efficiency. It first reviews the image steganography techniques that based on distortion function and then reviews techniques based on embedding efficiency.

3.1 Distortion function-based Image steganography techniques

To improve the un-detectability of the embedded secret message, steganography techniques have been created to conceal the information in texture regions and regions that could be confused with noise, but undoubtedly at the cost of shortening payload capacity. In most adaptive steganography techniques, data hiding modifications are distributed in the complex and noisy regions of an image through heuristically defining low concealing costs in such regions. The edge regions display more complicated statistical characteristics and are highly dependent on the image content. Thus, modifications in edge regions are harder to realize than in smooth regions. Images that consist of high ratio of edge regions might approximately exceed the shortcoming of capacity but not completely. In contrast, embedding in smooth or flat regions leads to reducing visual quality as well as message un-detectability particularly for those images that contain high ratio of smooth regions (Luo et al. 2010).

The Laplacian, Prewitt, Canny, and Sobel are the most common edge detection operators that can assist in determining edge pixels to be used for concealing the secret message, yet also other kinds of gradient methods are used by researchers for detecting edge pixels. In (Chen et al. 2010), using the Canny edge detector, an embedding technique is proposed, and the authors say that this leads to increasing capacity since the ratio of edge pixels is higher than that of other edge detection operators. Nevertheless, edge-based steganography techniques restrict the identification by the recipient part of the same edge pixels, since the act of concealing data in edge pixels could turn the original edge pixels into non-edge pixels. Meanwhile, a pixel detected as an edge point before concealing the secret bit might not be detected as an edge point after concealing the secrets and this causes certain hidden message pieces to be lost. Different approaches of dealing with this restriction have been suggested in the literature, but in any case, when an edge pixel is selected for concealing a secret bit, one must make sure that the act of concealing the message does not render a non-edge pixel. Hempstalk et al. proposed the steganography technique based on the strategy which is known as FilterFirst that aims to solve the drawback of retrieving the secret bit from the right edge pixels by first setting the LSB to zero for each cover pixel. Then Sobel edge detector is used to detect edge pixels. Later, LSBR is used for concealing the message in the edge pixels (Hempstalk 2006). Consequently, FilterFirst can assure to extract the message from the same edge pixels used for concealing, as the bit-planes used for filtering are not modified due to the act of embedding secrets. Although this technique can hide the secret information in sharper edge pixels and can achieve high message un-detectability. However, it has low payload capacity. Geetha et al. proposed the steganography technique that adopts a variable embedding ratio (VER) strategy to hide information with higher rate in edge pixels that aimed to improve payload capacity and achieve high un-detectability of the concealed information (Geetha and Giriprakash 2012). To detect higher rate of edge pixels and hide four bits in edge pixels and two bits in non-edge pixels, the Canny edge detector is implemented three times for increased capacity. But, this technique assumes the recipient part has the original cover image to retrieve the concealed information. Huang et al. state that aside from smooth regions, some edge regions are also sensitive to be used for message concealment (Huang and Ouyang 2010). This proposed technique avoids concealing the message in cover image pixels belonging to fragile regions, pixels for which concealing one bit results in modifications to its differences with many of its neighbors. Fragile regions refer to the regions such as smooth or frequent figure patterns, and a region with regular modifications in pixel values. The algorithm extends the use of absolute difference to all eight candidate-pixel neighbors. It counts the number of surrounding pixels for which differences with the center exceed a given threshold T, and if the count exceeds a constant C, a secret bit can be concealed. Meanwhile, this technique attempts to preserve local texture in the stego image, and thus, it is secure due to less possibility of detection. Once the regions are selected, LSB matching revisited (LSBMR) scheme is used for concealing the information in the non-fragile pixels. Details about LSBMR scheme is explained in Sect. 3.2. At the receiver part, the technique first determines non-fragile pixels in the same way and retrieves the concealed information from these pixels. The technique is achieved more withstand to the steganalysis attack and obtained high message un-detectability, but it has a shortcoming of payload capacity. In (Iranpour 2013), an embedding technique is proposed that revised the FilterFirst strategy using a particular method to identify the sharpness of the edge pixels determined using the Sobel edge detector after the first p bit-planes are neglected. This proposed technique also differs from FilterFirst in that it conceals up to p-bits in the first p bit-planes relying on the degree of sharpness of the edge pixels, so that the number of bits concealed in the sharper edges will be greater than those in the weaker edges. The threshold T value for sharpness relies on the size of the secret information, and concealing process is first done in the sharper edge pixels before concealing in the weaker edge pixels. As author claimed, this technique has significantly improved the message un-detectability against steganalysis technique and increased payload capacity.

In order to achieve higher security and message un-detectability, in the recent years, Fridrich and her team have explored a mechanism to hide the information in textured or noisy regions, identified by a certain defined distortion function, and avoid to conceal the secrets in smooth and clean edge regions (Holub and Fridrich 2012; Holub et al. 2014). The concept is established on the truth that complex or noisy regions are hard to model directly, but their distortion can be approximated by appropriately functions that link a pixel to its surrounding region. The distortion function-based embedding techniques improve resistance to steganalysis techniques, especially those used rich models such as (Fridrich and Kodovsky 2012). In their latest technique, Fridrich et al. developed an image steganography technique based on a defined distortion function called universal wavelet relative distortion (UNIWARD) (Holub et al. 2014) that is similar to their previous proposed technique in Holub and Fridrich (2012), but it is proper for concealing the message in both spatial and frequency domain, and it is an extended version of Holub and Fridrich (2013). This proposed distortion function is defined as the sum of the relative modifications of all wavelet coefficients respecting to the cover image. Meanwhile, it is a sum of relative modifications between the stego and cover images represented in the wavelet domain (Holub et al. 2014). In order to achieve the so-called directional residuals, which are related to the predictability of the pixel in a certain direction, the UNIWARD function relies on a wavelet bank of multiple directional high-pass filters. By evaluating the influence of concealment on directional residual, it is predictable in at least one direction considered as smooth or clean edge pixel, while it is unpredictable in any direction considered as textured or noisy pixel. The limitation of all of Fridrich and her team's proposed steganography techniques based on a given distortion function is they are un-detectable only if the amount of the concealed information does not surpass 0.5 bpp.

Apart from Fridrich and her team, there are steganography techniques based on distortion function proposed by other authors. Recently, Ante S. et al. have spotted the limitation of the UNIWARD distortion function proposed in Holub et al. (2014) in terms of time-consuming. For this reason, they designed a steganography technique based on distortion function to reduce time complexity (Su et al. 2021). As they reported, their proposed technique reduces the embedding time by two-thirds with only slightly weakening the security compared to UNIWARD. There are also other steganography techniques based on distortion function developed for minimizing the distortion characterized by a statistical model, such as modification direction synchronization (MDS) (Li et al. 2015), controversial pixels prior (CPP) (Zhou et al. 2017), and multivariate Gaussian for residuals (MRG) (Qin et al. 2019). All the designed steganography techniques based on region selection and distortion function have a limitation of payload capacity.

Very recently, a distortion function-based steganography technique has been presented in Li et al. (2023). This technique first employs a given distortion model to generate the original cost map. The cost of each pixel is then dynamically adjusted with majority voting according to the modification directions of its neighboring pixels. Furthermore, different distortion calculation models are integrated to make the final decision on the distortion of each pixel.

3.2 Embedding efficiency-based image steganography techniques

In the Sect. 3.1, steganography techniques based on defining distortion function are reviewed and their properties as well as limitations are highlighted in which aimed at increasing the message un-detectability, but only at the expense of limited payload capacity especially if the cover image consists of high rate of smooth areas. In addition, all the steganography techniques proposed by Fridrich and her team on the basis of a defined distortion function are undetectable only when the amount of concealed information does not exceed 0.5 bpp. In this section, steganography techniques based on embedding efficiency approach are reviewed with highlighting their characteristics and limitations. The embedding efficiency is an important attribute of steganography techniques directly affecting their security and can be defined as the number of secret bits concealed per one change as a result of embedding. In other words, embedding efficiency is the ratio of cover image pixels whose values are changed, due to the impact of concealing the secrets, to the size of a secret information. Therefore, high embedding efficiency in image steganography refers to a decrease in the number of required pixel modifications of the cover image for a certain embedding rate.

The idea of embedding efficacy was initially proposed by Crandall (1998) and first adopted by Westfeld (2001) for a concealment of the secret information. Since less embedding modifications are less likely to harm the statistical characteristics of the cover image, steganography techniques that achieve a high embedding efficiency usually have better message protection. Meanwhile, steganography techniques employing high embedding efficiency are generating stego images with minimum distortion. In terms of detectability of the concealed information in a stego image, a formal definition of security for steganography techniques was given by Cachin (1998), and the principle of embedding efficiency is identified as an important indicator of steganography security. The detectability of the concealed information within a stego image is influenced by several factors such as: (1) selection of the cover object, (2) selection rule used to determine individual elements of the cover that might be altered while concealing the message, (3) type of the concealing mechanism which alters the pixels of the cover, and (4) amount of embedding modifications, directly related to the secret information size. Considering that two embedding techniques use the same source of cover object, the same selection, rule and concealing mechanism, the one that produces stego object with smaller embedding modifications would be less detectable because it reduces the change that any statistics used by the warden would be sufficiently disrupted to perform a successful steganalysis technique (Fridrich et al. 2007). The probability of pixel modification for the LSBR-based or LSBM-based embedding techniques is 0.5, i.e., on average, such techniques add 0.5p of the noise in the pixels of cover image, where p is the concealing rate in bpp. Meanwhile, the embedding efficiency of LSBR-based or LSBM-based embedding techniques is 2 (Westfeld 2001).

Ker et al. highlighted the key problems in the area of steganography and steganalysis in future research and addressed the development of embedding efficiency-based techniques as a major issue (Ker, et al. 2013). To present, image steganography techniques which concentrate with developing an increased embedding efficiency and minimizing the modification of cover pixels due to the concealment of secret information are very limited. The first attempt to propose an increased embedding efficiency-based steganography technique was done by Crandall (1998) which is known as *matrix encoding* in order to achieve high embedding efficiency. In matrix encoding, to conceal k bits of the secret information, $2^k - 1$ of cover pixels are required to be employed and at most one pixel is altered by one from each group. The following example shows how the matrix encoding technique conceals two bits (m_1 and m_2) of the secret information into three pixels of the cover image. Note that only one of three pixels of the cover image is meant to be modified. Let a = [a_1 a_2 a_3] be the LSB of the three cover pixels. This embedding technique works by modifying one of the values as follows:

$$m_1 = \mathrm{a}_1 \oplus \mathrm{a}_3, m_2 = \mathrm{a}_2 \oplus \mathrm{a}_3 \Rightarrow \text{modify nothing}$$

$$m_1 \neq \mathrm{a}_1 \oplus \mathrm{a}_3, m_2 = \mathrm{a}_2 \oplus \mathrm{a}_3 \Rightarrow \text{modify } \mathrm{a}_1$$

$$m_1 = \mathrm{a}_1 \oplus \mathrm{a}_3, m_2 \neq \mathrm{a}_2 \oplus \mathrm{a}_3 \Rightarrow \text{modify } \mathrm{a}_2$$

$$m_1 \neq \mathrm{a}_1 \oplus \mathrm{a}_3, m_2 \neq \mathrm{a}_2 \oplus \mathrm{a}_3 \Rightarrow \text{modify } \mathrm{a}_3$$

where $\oplus$ is the exclusive OR operator. It is quite obvious that in all four cases, only one cover pixel's LSB is changed at most. The most significant characteristic of using matrix encoding is that it reduces the amount of required pixels that must be modified, that is, 25% are modified when k = 2. Meanwhile, the ratio of pixel change for matrix encoding scheme after message concealment is 0.25 bpp and the embedding efficiency is reached 4. The shortcoming of this embedding technique is that it restricts the capacity of the embedding, that is, 67% on average. These types of steganography techniques are therefore not beneficial for applications which require full capacity, i.e., concealing one bit per cover pixel.

Mielikainen J. developed a version of LSBM, known as LSB matching revisited (LSBMR), which employs the binary function in Eq. (2) to further increase the embedding efficiency to hide two secret bits, namely m_i and $m_{\mathrm{i}+1}$, in a pair of cover pixels x_i and $x_{\mathrm{i}+1}$ (Mielikainen 2006).

$$f(x_i, x_{i+1}) = \mathrm{LSB}\left(\left\lfloor \frac{x_i}{2} \right\rfloor + x_{i+1}\right) \tag{2}$$

This leads to the production of two stego pixels, y_i and $y_{\mathrm{i}+1}$, in which at most one of them differs from the cover pair. The LSB of the ith stego pixel y_i represents the ith secret bit m_i, and the LSB of the result of the binary function represents the (i + 1)th secret bit $m_{\mathrm{i}+1}$. The advantage of LSBMR technique is reducing the probability of modifying pixel values from 0.5 to 0.375 in comparison with LSBR and LSBM. In other words, the embedding efficiency of LSBMR has been increased to 2.66, and this reflects on achieving better resistance to steganalysis techniques for message detectability. Such improvements, however, are made at the cost of the reduction of payload capacity since the LSBMR technique cannot use saturated pixels of the cover image for embedding purposes; saturated pixels are those pixels with a minimum or a maximum value (0 or 255). This shortcoming is minimal in comparison with the matrix encoding-based embedding technique. Another image steganography technique is proposed by Chan (2009) with the goal of further reducing the amount of changed pixels in the cover image, and like above steganography technique uses binary function identified consecutive pixels, but tries to conceal a number of secret bits by applying the function successively to a number of consecutive pixels until the function output differs from the secret bit associated with the last pixel. The function is specified in Eq. (3) by XORing the previous pixel's 2nd bit-plane with the current pixel's LSB, if the result matches the next secret bit. Then, it proceeds to the next pixel without making any modification. Otherwise, either add 1 or − 1 depending on whether the result of the function applied to the next pixel matches or not.

$$XF(y_i) = LSB\left(\left\lfloor \frac{y_{i-1}}{2} \right\rfloor\right) \oplus LSB(y_i) \tag{3}$$

where y_i indicates the pixel value at the location i and $\oplus$ is the exclusive OR operator. This proposed image steganography technique not only exceeds the embedding technique in Mielikainen (2006) in terms of increasing the embedding efficiency, but also has higher capacity as each cover pixel can be used to conceal the information. The experimental results reported in Chan (2009) showed that this embedding technique is achieved higher embedding efficiency in comparison with LSBMR. The author states that concealing a secret Lenna image of size 256 × 128 (i.e., 262,144 bits) in a Lenna cover image of size 512 × 512, only 87,374 cover pixels are altered, while in the LSBMR embedding technique 98,176 cover pixels are modified (Chan 2009). In brief, the advantages of this image steganography technique are reducing the ratio of changing pixel values, with maintaining the payload capacity, by approximately 0.335. Consequently, the embedding efficiency of such a technique is reached around 3. This reflects on achieving better resistance to steganalysis techniques for message detectability.

Iranpour et al. combined the idea of the last two mentioned image steganography techniques to increase the embedding efficiency, and three binary functions are used to conceal three secret bits in three pixels of the cover image in a similar mechanism to the LSBMR embedding technique. Note that the secret bits are not directly embedded/extracted into/from the LSB of the cover/stego pixels, but conceal or retrieve from the results of the following three functions (Iranpour 2013):

$$f_1(x,y,z) = LSB\left(\left\lceil \frac{x}{2} \right\rceil + \left\lceil \frac{y}{2} \right\rceil + \left\lceil \frac{z}{2} \right\rceil\right) \tag{4}$$

$$f_2(x,y,z) = LSB\left(\left\lfloor \frac{x}{2} \right\rfloor + \left\lfloor \frac{y}{2} \right\rfloor + \left\lfloor \frac{z}{2} \right\rfloor\right) \tag{5}$$

$$f_3(x,y,z) = LSB\left(\left\lfloor \frac{x}{2} \right\rfloor + \left\lfloor \frac{y}{2} \right\rfloor + \left\lfloor \frac{z}{2} \right\rfloor\right) \tag{6}$$

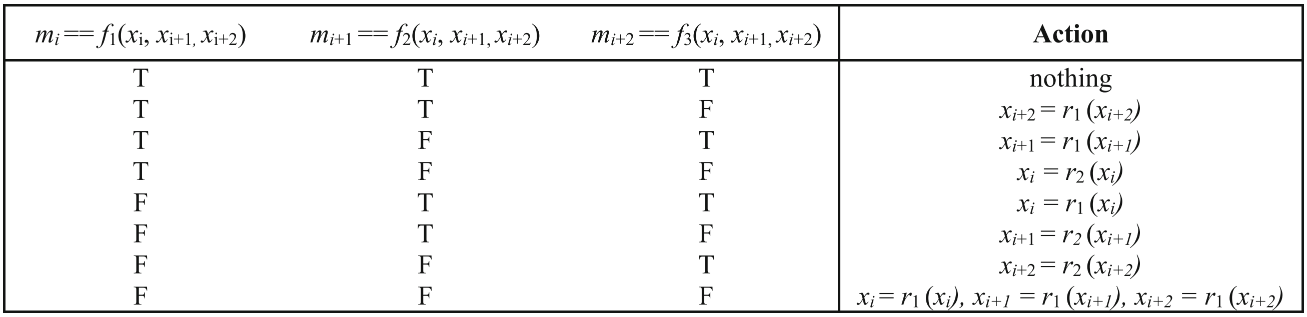
To conceal three secret bits into three pixels of the cover image, eight cases with any combination of three secret bits with the results of three defined functions will occur. If no match is found, the scheme adds either 1 or − 1 depending on Eqs. (7) and (8). Figure 1 displays the eight cases arising when three secret bits (m_{i}, $m_{\mathrm{i}+1}$, and $m_{\mathrm{i}+2}$) are concealed in three pixels of the cove image (x_{i}, $x_{\mathrm{i}+1}$, and $x_{\mathrm{i}+2}$) depending on the following two specified rules for changing a pixel value (Iranpour 2013):

$$r_1(\mathrm{t}) = \begin{cases} t+1 & \textit{if t is even} \\ t-1 & \textit{if t is odd} \end{cases} \tag{7}$$

$$r_2(\mathrm{t}) = \begin{cases} t-1 & \textit{if t is even} \\ t+1 & \textit{if t is odd} \end{cases} \tag{8}$$

From Fig. 1, one can see that at most one pixel out of three pixels is changed in all cases, except for one case, either increased or decreased by one. Moreover, only in one case all three cover pixels should be changed, and this is not a significant issue with this proposed technique, as the probability of this occurrence is experimentally investigated at < 4.2% (Iranpour 2013). In addition, the probability of changing cover pixel value in this embedding technique is 0.375 bpp, i.e., the embedding efficiency is 2.66. The payload capacity is the only shortcoming of this embedding technique, since the saturated pixels are not allowed for concealing purposes. Concisely, this embedding technique has the same amount of payload capacity to be concealed, and the same embedding efficiency as LSBMR embedding technique in Mielikainen (2006) has.

Alan et al. set approaches in a new state-of-the-art regarding improving the embedding efficiency by exploiting Fibonacci series for cover image pixel values decomposition instead of using usual binary system. In their first attempt, a compression-like scheme, known as secret image size reduction (SISR), was presented to minimize the size of the bit-stream of the secret image by nearly 30% without losing information (Abdulla et al. 2014). In this image steganography technique, two significant issues are observed in which the resulted bit-stream after SISR algorithm is applied contains 57% of the bits that have a zero value. Furthermore, Fibonacci series is used for decomposing the cover image pixel values instead of traditional binary in which produced 61% of 0 s in the LSB of the cover image pixels. Thus, concealing SISR secret bit-stream in the Fibonacci decomposed cover image LSB plane yields in reducing the probabilities of changing the cover pixels' value and in improved embedding efficiency compared to LSBR embedding technique. On the basis of the above observations, Alan et al. invented and explored the idea of increasing similarity between secret image bit-stream and cover image pixel's LSB to reduce the probabilities of modifying the cover pixels' value and this leads to improve the embedding efficiency. In their recent work, an image steganography technique is proposed by developing two novel steps for both secret and cover images (Abdulla et al. 2019). For the secret images, two image preprocessing mechanisms are developed to transform the bit-stream of the secret image for increasing the ratio of 0 s. One of them is performed in the spatial domain and the other one is performed in the integer wavelet transformed domain (IWTD). In both mechanisms, the most frequent pixels' values are mapped onto bytes with more 0 s. These mechanisms produce a significant increase of 0 s ratio in the bit-stream of the secret image; the one established on the wavelet domain is the best-performing with 80% ratio of 0 s. In contrast, the Fibonacci series is used to decompose the cover pixel values instead of usual binary scheme, and this yields in increasing the 0 s ratio in cover image pixel's LSB from 50 to 77% compared to usual binary-based decomposition. As they reported that the experimental results of their work demonstrate that the combination of the two steps strategy produces stego images that have minimum distortion, i.e., minimizing the number of



$m_i == f_1(x_i, x_{i+1}, x_{i+2})$	$m_{i+1} == f_2(x_i, x_{i+1}, x_{i+2})$	$m_{i+2} == f_3(x_i, x_{i+1}, x_{i+2})$	**Action**
T	T	T	nothing
T	T	F	$x_{i+2} = r_1(x_{i+2})$
T	F	T	$x_{i+1} = r_1(x_{i+1})$
T	F	F	$x_i = r_2(x_i)$
F	T	T	$x_i = r_1(x_i)$
F	T	F	$x_{i+1} = r_2(x_{i+1})$
F	F	T	$x_{i+2} = r_2(x_{i+2})$
F	F	F	$x_i = r_1(x_i)$, $x_{i+1} = r_1(x_{i+1})$, $x_{i+2} = r_1(x_{i+2})$

Fig. 1 Illustration for the eight cases of the image steganography technique in (Iranpour 2013)

modifications of the cover pixels' value post information concealment and therefore increasing the embedding efficiency. Moreover, the advantages of this embedding techniques are reducing the probability of changing pixel values to 0.32 bpp. In other words, the embedding efficiency of this image steganography technique has been increased to 3.125, with maintaining payload capacity, and this reflects in achieving better resistance to steganalysis techniques for message detectability.

In recent years, an approach to improving embedding efficiency was proposed by Malathi et al. (2021) using various linear block codes. Linear block coding algorithms such as binary hamming code, random linear code, cyclic code, and Reed–Solomon code are implemented to conceal sensitive information inside the cover image.

Very recently, a new image steganography technique was proposed based on modified matrix encoding by exploiting more pixel bit-planes in the data hiding process to improve the embedding efficiency (Nguyen and Le 2022). This work claimed that the number of used image layers depends on the size of the given secret message and the texture characteristic of the cover image. The complexity of the pixel block is identified by the difference between the middle pixel and its neighbors. By performing the suitable embedding solutions of modified matrix encoding, the complexity is unchanged by the data hiding stage.

4 Success criteria for image steganography techniques

The three success criteria that must be addressed by image steganography techniques are: (1) stego image quality—minimizing the perceptual gap between the stego and the cover images; (2) payload capacity—the quantity of information which can be concealed within the cover image; and (3) secret message detectability—preventing detection by steganalyzers. The first two criteria are, however, at odds with one another. In other words, it is hard to increase the payload capacity while preserving the quality of a stego image, and vice versa. The third criterion relates to the first one. Meanwhile, the steganography technique becomes less detectable by improving the quality of the stego image. It is a challenge for image steganography techniques to attain an appropriate balance between all these image steganography criteria. The above-mentioned three criteria are directly influenced by the number of modified pixels of the cover image after the information is concealed. Hence, in the literature, minimizing this modification has been addressed as the most significant criterion. The amount of modification must be regarded proportional to the payload capacity. Therefore, it is natural to model this criterion by the ratio of modified pixels to the concealed information size. In the recent proposed image steganography techniques, the low ratio of modifying the value of the cover image pixels post the information concealment while preserving the payload capability has been used as an indication of higher quality of the stego image and lower detectability of the concealed secret information.

Assessing the ratio of modified cover image pixels is called *embedding efficiency* in the literature, which can be defined as the number of secret bits concealed per one embedded change. In addition, embedding efficiency can be considered as the fourth and the most significant criterion for image steganography techniques. Once the embedding efficiency is increased, the less detectable traces are placed in the stego image, and therefore, the embedding technique is able to withstand against steganalysis techniques, with preserving payload capacity. This paper aims to highlight the role of those image steganography techniques that employed increasing the embedding efficiency in terms of message detectability and stego image quality compared to those techniques that employed distortion function. Although steganography techniques aim to conceal the secret information in a way that is difficult to disclose, steganalysis techniques by exposing the existence of a concealed information attempt to defeat the purpose of steganography techniques. Steganalysis techniques aim to exploit the fact that any embedding technique would result in a kind of local random distortions, though difficult to notice by the naked eye, yet computable, certain statistical and correlation models which are known to hold among the various components of the cover images. There are a range of current image steganalysis techniques which are widely used to reveal the existence of the concealed information and to measure its amount. These techniques can be categorized in different ways, whereas some target specific steganography techniques, while others are created to reveal the existence of concealed information without providing knowledge about the embedding technique. These techniques target specific steganography techniques and are thus called targeted steganalysis techniques in the literature. For example, regular and singular (RS) (Fridrich et al. 2001), pairs of value (PoV) (Westfeld and Pfitzmann 2000), the two versions of the weighted stego (WS) (Fridrich et al. 2005; Ker and Bohme 2008), and difference image histogram (DIH) (Zhang and Ping 2003) techniques are designed to break some specific steganography techniques. In recent years, interest in non-targeted steganalysis techniques, also called blind steganalysis, has increased dramatically, whereby no knowledge about the scheme or its effect is assumed. While the targeted techniques are being developed to overcome specific steganography techniques, blind steganalysis techniques are being developed to reveal the presence of hidden information in the digital image independently of steganography techniques (Luo et al. 2008). This kind of steganalysis is also known as *universal* in which it aims to detect different types of steganography techniques, for example, the spatial rich model (SRM) designed by Fridrich and Kodovsky (2012) to break different steganography techniques. These steganalysis techniques are dependent on the assumption that any steganography technique creates different minor local distortions, referred to as features, that could help detect the existence of concealed information in the cover image and model these features (i.e., quantifying the relationship between a pixel and its neighbors). However, universal techniques are not able to obtain any knowledge about the size or amount of the concealed messages (Ker and Bohme 2008) and they are only able to decide whether the tested image is cover or stego image. In this study's experiments, the SRM is chosen to be used for evaluating the message detectability for the tested embedding techniques since it is commonly used in the recent publications in this area, and it can also be used for different embedding techniques as a non-target steganalysis technique. Regarding the stego image quality evaluation, peak-signal-to-noise ratio (PSNR) (Gonzalez and Woods 2002) is used to measure the difference between the cover and stego image. PSNR can be defined as a measurement of similarity between two images. It is commonly used and popular, since the computation of these two metrics is easy and fast. It is a logarithmic function of mean square error (MSE) and is measured in decibels (dB) units (Stoica et al. 2003):

$$\mathrm{PSNR} = 10.log_{10}\frac{I^2}{MSE} \tag{9}$$

where I refers to the maximal pixel value. For the grayscale image, $I = 255$. The value of PSNR is a decimal value between 0 and infinity ($\propto$). For two identical images, the PSNR value is $\propto$. In addition, the higher the PSNR value means better similarity between the cover and the stego image.

The next section will practically analyze and investigate which of the modern steganography approaches, namely distortion function-based techniques and embedding efficiency-based techniques, is adequate to achieve all the required steganography criteria. The above-mentioned two measurements, namely SRM and PSNR, are used to evaluate the performance of the tested image steganography techniques in terms of message detectability and stego image quality, respectively.

5 Analyses and investigations

This section practically attempts to analyze and investigate the influence of increasing the embedding efficiency of image steganography techniques on achieving high security and high stego image quality. For this purpose, the BOSSBase version 1.0 dataset of grayscale images with the size of (512 × 512) is used. This dataset includes images of, but not limited to, landscapes, plants, people, and building, and it contains 10,000 images (Bas et al. 2011). In this experiment, the Lenna image of size (128 × 256) is considered as a secret message to be hidden inside the 10,000 cover images of BOSSBase dataset producing 10,000 stego images. The reason behind resizing the Lenna secret image to (128 × 256) is to make the number of bits that represent a secret image (262,144 bits) equivalent to the number of cover images' pixels which their sizes are (512 × 512). In each experiment, seven different payload ratios 5%, 10%, 20%, 40%, 60%, 80%, and 100% of the size of the secret stream are tested. In addition, the produced stego images are evaluated in terms of message detectability/security using the widely used SRM universal steganalysis technique (Fridrich and Kodovsky 2012) and stego image quality using PSNR.

In this experiment, three steganography techniques are designed virtually with different amounts of increased embedding efficiency. In this context, 'Virtually' is defined as the assumption that embedding lesser ratio of the secret bits which reflects the smaller number of cover pixels to be modified due to the impact of the information concealment, so that increasing the embedding efficiency leads to the smaller number of cover pixel to be altered. Meanwhile, instead of concealing the entire secret bits, only some of its bits are concealed to see the impact of increasing the embedding efficiency on both the secret message un-detectability and the stego image quality. The usual LSB scheme is used in all the three techniques to replace the LSB of the cover pixels with the secret bit. For this purpose, three assumptions are taken into account, which are:

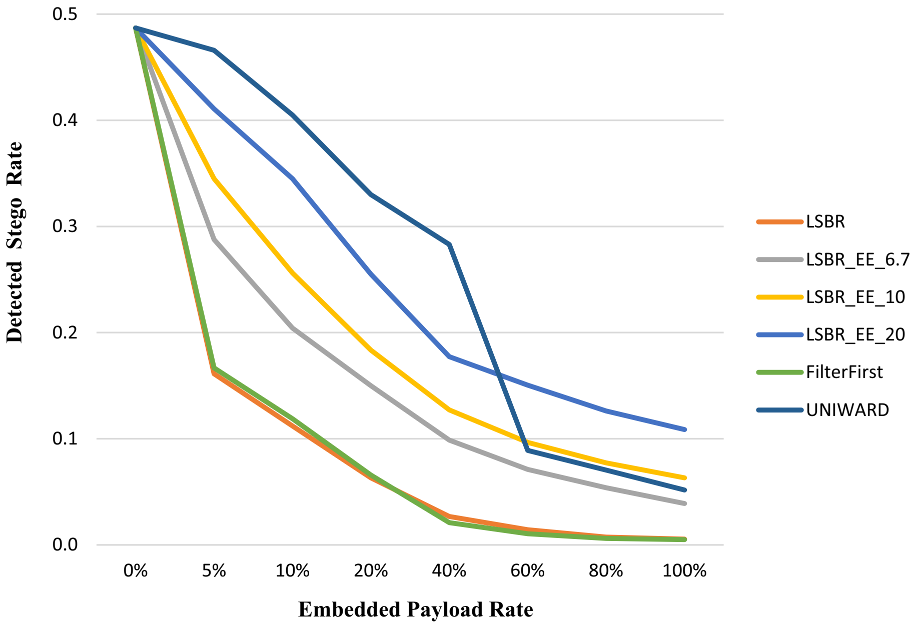
1) LSB_EE_6.7: In this technique, 30% of the secret bits (i.e., 0.3 × 262,144 = 78,643 bits) are concealed. Depending on the experiments, in such a case, on average, 39,321 of cover pixels are modified and this equals 0.15 of the total number of cover pixels. In other words, 15% of cover pixels are modified. Thus, based on Eq. (1) in Sect. 1, the embedding efficiency of this technique is equal to 6.7. In addition, different ratios of payload are tested, see Figs. 2 and 3. For example, for the ratio of 10%, 7864 bits are concealed (0.1 × 78,643 = 7864 bits).
2) LSB_EE_10: In this technique, 20% of the secret bits (i.e., 0.2 × 262,144 = 52,428 bits) are embedded. Based on the experiments, on average, 26,214 of cover pixels are changed and this equals 0.10 of the total number of cover pixels. Meanwhile, 10% of cover pixels are changed. Accordingly, regarding Eq. (1), the embedding efficiency of this technique is equal to 10. Additionally, different ratios of payload are considered to be tested, see Figs. 2 and 3. For example, for the ratio of 10%, 5242 bits are embedded (0.1 × 52,428 = 5242 bits).
3) LSB_EE_20: In this technique, 10% of the secret bits are hidden (i.e., 0.1 × 262,144 = 26,214 bits) and embedded. On the basis of our experiments, on average, 13,107 of cover pixels are altered and this equals 0.05 of the total number of cover pixels. In other words, 5% of cover pixels are modified. Hence, based on Eq. (1), the embedding efficiency of this technique is equal to 20. In addition, different ratios of payload are taken into consideration, see Figs. 2 and 3. For instance, for the ratio of 10%, 2621 bits (0.1 × 26,214 = 2621) are concealed.

The effects of the above different amounts of increased embedding efficiency on the secret message detectability and the stego image quality are displayed in Figs. 2 and 3, respectively. Apart from the above three mentioned increased embedding efficiency techniques, another three image steganography techniques are also tested, which are: the usual LSBR (Chan and Cheng 2004), FilterFirst (Hempstalk 2006) that embeds the secrets in edge regions, and UNIWARD (Holub et al. 2014) that embeds the message based on distortion function to highlight the advantages and limitations of embedding efficiency-based techniques and distortion function-based (region-based) techniques.

5.1 Stego image detectability evaluation

The SRM, as a universal steganalysis, is used to evaluate the performance of the tested image steganography techniques in terms of stego image detectability. Universal steganalysis techniques are a two-class pattern recognition issue and contain two stages, feature extraction and pattern

Fig. 2 Stego image detectability using SRM steganalysis technique



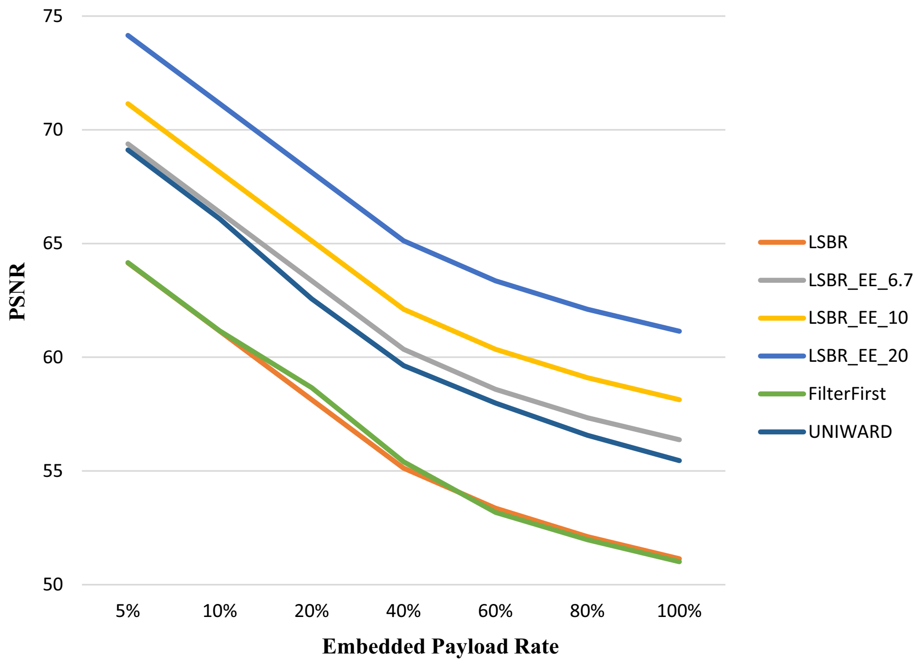


Fig. 3 Stego image quality using PSNR

classification. It aims to categorize the given images into two groups: the cover and stego images. Most of the existing universal steganalysis techniques first extract certain features from the images, then select or build a classifier, and train the classifier using the features extracted from training image sets. Finally, they classify the features. In general, classification techniques such as a Fisher linear discriminants (FLDs) or support vector machine (SVM) are used (Luo et al. 2008). The SRM steganalysis technique uses half of the cover image set together with the same number of stego images for training and the rest for testing. This technique requires the input of a large set of cover images together with their respective stego images. In this study, the input is the 10,000 cover images of BOSSBase dataset, and the corresponding 10,000 stego images after the Lenna image is concealed. The SRM is a binary-based classification in which an input image is identified as a cover or a stego using a considerable number of local distortion features. Figure 2 shows the average rate of the detected stego images to the number of tested images. The lower value of SRM means a higher rate of stego images is detected, and the higher value of SRM indicates a lower rate of stego images is detected.

From Fig. 2, it is clear that LSBR and FilterFirst techniques provide the worst case for all embedded ratios. Meanwhile, the techniques that embed in clean edge regions, such as FilterFirst, cannot provide resistance to universal steganalysis. Furthermore, one can see that both the virtual increased embedding efficiency-based techniques, LSBR_EE_20 and LSBR_EE_10, provide better resistance in comparison with the distortion function-based technique, UNIWARD, for embedding rate $> 40\%$. Consequently, the UNIWARD embedding technique has the robustness against SRM only for embedding rate $< 40\%$. Furthermore, high embedding efficiency-based techniques such as LSBR_EE_20 and LSBR_EE_10 are appropriate for those applications that required full payload capacity than distortion function-based techniques. This means that any steganography technique will attain a value of 10, or higher, of embedding efficiency score, which can achieve the robustness against universal steganalysis techniques without compromising payload capacity.

5.2 Stego image quality evaluation

The quality of the stego images for all the tested image steganography techniques is evaluated, with respect to the original cover images, using PSNR, see Fig. 3. The higher value of PSNR indicates the better quality, and vice versa.

Clearly, the PSNR of the LSBR_EE_20 scored the highest value in comparison with all other embedding techniques. This is because the lowest ratio of cover pixels is changed, due to the impact of embedding, compared to all other techniques. Moreover, the PSNR of the FilterFirst technique is near to that of the LSBR. Furthermore, the PSNR value of all the image steganography techniques based on embedding efficiency, namely LSBR_EE_6.7, LSBR_EE_10, and LSBR_EE_20, is higher than other techniques including UNIWARD, which is based on distortion function.

Having said that, techniques can be considered in future for enhancing embedding efficiency. For instance, (Li et al.

2016) considers cooperative kinematic control of multiple manipulators using distributed recurrent neural networks and provides a tractable way to extend existing results on individual manipulator control using recurrent neural networks to the scenario with the coordination of multiple manipulators; (Jin et al. 2022) analyzes a collaborative control problem of redundant manipulators with time delays and proposes a time-delayed and distributed neural dynamics scheme; and (Yang et al. 2023) proposes an extended Kalman filter-incorporated residual neural network-based calibration (ERC) model for kinematic calibration.

6 Conclusion and future direction recommendation

This section presents the conclusion and findings, research limitations, and future direction recommendation.

6.1 Conclusion and findings

There are two different approaches involved in modern image steganography techniques, namely distortion function and embedding efficiency. This paper practically analyzed and investigated to prove which of the two approaches is superior and plays a significant role in achieving all image steganography criteria/requirements at the same time. For this purpose, three virtual steganography techniques are designed as an assumption, based on three different amounts of increased the embedding efficiency. Developing image steganography techniques based on increasing the embedding efficiency along with minimizing pixel modification post embedding is recommended according to the results of this study. In addition, it is sufficient to achieve high security and stego image quality without compromising payload capacity. Meanwhile, to overcome the limitations of embedding techniques based on distortion function, namely payload capacity and message detectability, it would be ideal to develop image steganography techniques that produce little modification and have high embedding efficiency without the need to hide the secret except for any part of the cove image such as smooth or clean edge regions. Therefore, it can be said that the strength of image steganography techniques depends on embedding efficiency value. The experimental findings reveal that the virtual designed steganography technique, LSB_EE_20, achieved the optimum results, with an embedding efficiency of 20, a PRNR of 62, and a message detectability of 0.11%.

6.2 Research limitations

Digital imagine steganography technology performance evaluations include payload capacity, stego image quality, and security. Increasing payload capacity diminishes stego image quality and security. In contrast, ideal stego image quality and security cannot be accomplished without sacrificing payload capacity. It has become necessary, but more challenging to strike a compromise between these image steganography requirements.

6.3 Future direction recommendation

The key observations from the experiments are summarized as follows:

The image steganography techniques based on increased the embedding efficiency offer:

1. A better resistance to steganalysis techniques for embedding rate $> 40\%$ compared to image steganography techniques based on distortion function.
2. A higher PSNR value in comparison with image steganography techniques based on distortion function.
3. A full payload capacity in comparison with image steganography techniques based on distortion function.

Depending on the above three observations, researchers in this research area recommended to concentrate on increasing and enhancing the embedding efficiency of their proposed approaches rather than focusing on distortion function. This leads to achieving all the three image steganography requirements at a time, which are:

1. High/full payload capacity: Since distortion function-based embedding techniques have limitation of payload capacity especially if the cover image consists of high ratio of smooth regions. Conversely, embedding efficiency-based techniques have no such restriction. For instance, for the embedding efficiency-based technique, LSBR_EE_20, the ratio of the cover pixel used for embedding the secret bits is 100%. In other words, all of the cover pixels were used for concealing the secret bits.
2. High security: As the distortion function-based image steganography techniques are un-detectable only if the rate of the concealed information does not exceed 0.5 bpp. Otherwise, they are detectable. In contrast, embedding efficiency-based techniques are un-detectable for the high embedding rate. For instance, for the embedding efficiency-based technique, LSBR_EE_20, when 100 of cover pixels were contained the secret bit, the SRM steganalyzer technique detects only 10% of the embedded bits, see Fig. 2.

3. High stego image quality: Since in embedding efficiency-based techniques, the smaller number of cover pixels is modified and this leads to less impact on the quality of the produced stego images. For instance, for the embedding efficiency-based technique, LSBR_EE_20, when all of cover pixels were used for concealing the secret bits, the PSNR reached 62 db, see Fig. 3.

Eventually, despite this, Ker et al. identified the two key problems of image steganography techniques which need to be addressed in the future research, which are: (1) developing steganography techniques based on embedding efficiency and (2) developing steganography techniques based on distortion function (Ker et al. 2013). This paper recommends that developing and designing the steganography techniques based on the concept of increasing the embedding efficiency alone with minimizing the ratio of cover pixel change as much as possible, and without compromising payload capacity, is sufficient to meet all the image steganography requirements simultaneously.

Acknowledgements This work was supported by the University of Sulaimani.

Funding Not applicable.

Availability of data and materials Not applicable.

Declarations

Conflict of interest Not applicable.

References

Abdulla AA (2015) Exploiting similarities between secret and cover images for improved embedding efficiency and security in digital steganography. PhD dissertation, Dept. of Applied Computing, Buckingham Univ., Buckingham, UK. http://bear.buckingham.ac.uk/149/

Abdulla AA, Sellahewa H, Jassim SA (2014) Stego quality enhancement by message size reduction and Fibonacci bit-plane mapping. International Conerence on Research in Security Standardisation Research (SSR). Springer, UK, pp 151–166

Abdulla AA, Sellahewa H, Jassim SA (2019) Improving embedding efficiency for digital steganography by exploiting similarities between secret and cover images. Multimed Tools Appl 78:17799–17823

Agaian SS, Cherukuri RC, Sifuentes RR (2007) Key dependent covert communication system using fibonacci p-codes. International Conference on System of Systems Engineering. IEEE, p 1–5

Bas P, Filler T, Pevny T (2011) Break our steganographic system. Information Hiding, Springer, pp 59–70

Bender W, Gruhl D, Morimoto N, Lu A (1996) Techniques for data hiding. IBM Syst J 35:313–336

Cachin C (1998) An information-theoretic model for steganography. Information Hiding, Springer, pp 306–318

Chan C-S (2009) On using LSB matching function for data hiding in pixels. Fundamenta Informaticae, IOS Press 96:49–59

Chan C-K, Cheng L-M (2004) Hiding data in images by simple LSB substitution. Pattern Recognit 37:469–474

Chen W-J, Chang C-C, Le T (2010) High payload steganography mechanism using hybrid edge detector. Expert Syst Appl 37:3292–3301

Cox I, Miller M, Bloom J, Fridrich J, Kalker T (2007) Digital Watermarking and Steganography. Morgan Kauffman

Crandall R (1998) Some notes on steganography. Posted on steganography mailing list 1998(1):6

Fridrich J, Kodovsky J (2012) Rich models for steganalysis of digital images. IEEE Trans Inf Forensics Secur 7:868–882

Fridrich J, Goljan M, Du R (2001) Reliable detection of LSB steganography in color and grayscale images. Workshop on Multimedia and Security: New Challenges. ACM, pp 27–30

Fridrich J, Goljan M, Lisonek P, Soukal D (2005) Writing on wet paper. IEEE Trans Signal Process 53:3923–3935

Fridrich J, Lisonek P, Soukal D (2007) On steganographic embedding efficiency. Information Hiding, Springer, pp 282–296

Geetha C, Giriprakash H (2012) Image steganography by variable embedding and multiple edge detection using canny operator. Int J Computer Appl Citeseer 48(16):15–19

Gonzalez RC, Woods RE (2002) Digital image processing, 2nd edn. Publishing House of Electronics Industry, Beijing

Hempstalk K (2006) Hiding behind corners: Using edges in images for better steganography. Computing Women's Congress, Hamilton, New Zealand, p 1119

Holub V, Fridrich JJ (2012) Designing steganographic distortion using directional filters. IEEE International Workshop on Information Forensics and Security (WIFS). pp 234–239

Holub V, Fridrich J (2013) Digital image steganography using universal distortion. 1st ACM workshop on Information hiding and multimedia security, pp 59–68

Holub V, Fridrich J, Denemark T (2014) Universal distortion function for steganography in an arbitrary domain. EURASIP J Inf Secur 2014:1–13

Huang Q, Ouyang W (2010) Protect fragile regions in steganography LSB embedding. 3rd International Symposium on Knowledge Acquisition and Modeling (KAM). pp 175–178

Iranpour M (2013) A novel steganographic method based on edge detection and adaptive multiple bits substitution. 18th International Conference on Digital Signal Processing (DSP). pp 1–6

Jin L, Zheng X, Luo X (2022) Neural dynamics for distributed collaborative control of manipulators with time delays. IEEE/CAA J Autom Sin 9:854–863

Ker AD (2005) Steganalysis of LSB matching in grayscale images. Signal Process Lett 12:441–444

Ker AD, Bohme R (2008) Revisiting weighted stego-image steganalysis. Electron Imaging Forens Steganography Watermarking Multimed Contents SPIE 6819:681905–681905

Ker AD et al (2013). Moving steganography and steganalysis from the laboratory into the real world. ACM workshop on Information hiding and Multimedia Security. pp 45–58

Li B, Wang M, Li X, Tan S, Huang J (2015) A strategy of clustering modification directions in spatial image steganography. IEEE Trans Inf Forensics Secur 10:1905–1917

Li S, He J, Li Y, Rafique M (2016) Distributed recurrent neural networks for cooperative control of manipulators: a game-theoretic perspective. IEEE Trans Neural Netw Learn Syst 28:415–426

Li F, Yu Z, Wu K, Qin C, Zhang X (2023) Multi-modality ensemble distortion for spatial steganography with dynamic cost correction. IEEE Trans Depend Secure Comput IEEE

Lin G-S, Chan Y-T, Lie W-N (2010) A framework of enhancing image steganography with picture quality optimization and anti-steganalysis based on SimulatedAnnealing algorithm. IEEE Trans Multimed 12:345–357

Luo X-Y, Wang D-S, Wang P, Liu F-L (2008) A review on blind detection for image steganography. Signal Process 88:2138–2157

Luo W, Huang F, Huang J (2010) Edge adaptive image steganography based on LSB matching revisited. Trans Inf Forensics Secur IEEE 5:201–214

Malathi P, Sridhar A, Paliwal A, Kumar G (2021) Maximizing the embedding efficiency using linear block codes in spatial and transform domains. Procedia Computer Sci 167:302–312

Mielikainen J (2006) LSB matching revisited. Signal Process Lett 13:285–287

Nguyen T, Le HQ (2022) A secure image steganography based on modified matrix encoding using the adaptive region selection technique. Multimed Tools Appl 81(81):25251–25281

Provos N, Honeyman P (2003) Hide and seek: An introduction to steganography. Security and Privacy 1:32–44

Qin X, Li B, Huang J (2019) A new spatial steganographic scheme by modeling image residuals with multivariate gaussian model. In: 2019 IEEE International Conference on Acoustics, Speech and Signal Processing

Sharp T (2001) An implementation of key-based digital signal steganography. Information Hiding, Springer, pp 13–26

Stoica A, Vertan C, Fernandez-Maloigne C (2003) Objective and subjective color image quality evaluation for JPEG 2000 compressed images. Int Symp Signal Circuit Syst 1:137–140

Su A, Ma S, Zhao X (2021) Fast and secure steganography based on J-UNIWARD. IEEE Signal Process Lett 27:221–225

Thien C-C, Lin J-C (2003) A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function. Pattern Recognit 36:2875–3288

Wang C et al (2010) A content-adaptive approach for reducing embedding impact in steganography. IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP), pp 1762–1765

Westfeld A (2001) F5—a steganographic algorithm. Information Hiding, Springer, pp 289–302

Westfeld A, Pfitzmann A (2000) Attacks on steganographic systems. Information Hiding, Springer, pp 61–76

Yang W, Li S, Li Z, Luo X (2023) Highly-accurate manipulator calibration via extended Kalman filter-incorporated residual neural network. IEEE Transactions on Industrial Informatics. IEEE

Zhang T, Ping X (2003) Reliable detection of LSB steganography based on the difference image histogram. Int Conf Acoust Speech Signal Process IEEE 3:545–548

Zhou W, Zhang W, Yu N (2017) A new rule for cost reassignment in adaptive steganography. IEEE Trans Inf Forensics Secur 12:2654–2667

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.