Journal of Circuits, Systems, and Computers

Toward a Unified Performance Metric for Benchmarking Steganography Systems

Tamer Rabie
Department of Electrical & Computer Engineering, University of Sharjah
Sharjah, United Arab Emirates
trabie@sharjah.ac.ae

Mohammed Baziyad
Research Institute of Sciences & Engineering
Sharjah, United Arab Emirates
mbaziyad@sharjah.ac.ae

Talal Bonny
Department of Electrical & Computer Engineering, University of Sharjah
Sharjah, United Arab Emirates
tbonny@sharjah.ac.ae

Raouf Fareh
Department of Electrical & Computer Engineering, University of Sharjah
Sharjah, United Arab Emirates
rfareh@sharjah.ac.ae

Received (Day Month Year)
Revised (Day Month Year)
Accepted (Day Month Year)

Recent advances in network speeds for exchanging multimedia data over insecure networks has resulted in an increased interest in steganography techniques. These techniques are usually evaluated based on their performance in three attributes; namely capacity, imperceptibility, and robustness. Each of these attributes has its own measurement metric. Hence, comparing two different steganography schemes based on these individual metric tools becomes inconsistent. In this paper a novel measurement metric tool is introduced for benchmarking steganography schemes. This new tool, named the "Combined Capacity-Quality-Robustness Effectiveness" (CCQRE) metric, combines the three opposing attributes of a steganography system into one conglomerate performance measure. Comparative results demonstrate the effectiveness of the proposed CCQRE metric for benchmarking various steganography schemes based on the researcher's interest in capacity, imperceptibility, or robustness.

Keywords: Comparative steganography measurement; Combined Capacity-Quality-Robustness effectiveness; Conglomerate performance metric; Benchmarking steganography systems; Trade-off triangle measures.

1. Introduction

Steganography systems are a class of information hiding techniques that deal with concealing the existence of a secret communication between two entities by hiding the secret medium into an "innocent" cover medium to produce a stego medium that should be inconspicuous to an eavesdropper [1].

Implementations of steganography that lack a shared secret key are forms of security through obscurity, while key-dependent steganographic schemes follow Kerckhoffs's principle. In cryptography, Kerckhoffs's principle states that "a cryptosystem should be secure even if everything about the system, except the key, is public knowledge". In security engineering, "security through obscurity is the reliance on the secrecy of the design or implementation as the main method of providing security for a system".

The importance of data security techniques such as steganography schemes, encryption techniques and watermarking techniques has widely grown in recent years with the enormous increase in exchanged multimedia data over the internet and insecure wireless networks [2,3,4,5,6,7,8,9,10,11,12,13,14]. Therefore, steganography techniques have become a focus point of research in the information security field. Researchers are striving to develop steganography techniques that improve all or some of the opposing stego attributes; namely capacity, imperceptibility, and robustness [1,15,16,17].

Imperceptibility refers to the amount of noise presented in the stego medium due to the hiding process. For steganography systems, the imperceptibility attribute is highly correlated to the security of the stego medium, as increasing the imperceptibility level of a steganography system, makes it tougher for an attacker to detect the existence of the secret communication, which leads to increasing the security level of the steganography system [18].

The capacity attribute refers to the size of the hidden data in a cover medium. Robustness refers to the solidity of the stego medium, and its ability to keep the secret information undestroyed with the existence of noise and impairments [15].

The three opposing attributes; namely the capacity, imperceptibility, and robustness form together a tri-trade-off problem. Increasing the capacity reduces the imperceptibility of a steganography system. That is because hiding more secret data means removing more details of the stego medium which results in a degraded stego medium (reduced imperceptibility) [18]. On the other hand, robustness can be enhanced by increasing the strength of the embedded watermark, but because of this strengthening process, visible distortions would be increased as well in the stego medium (reduced imperceptibility) [19].

The three opposing attributes have their own measurement tools. Capacity can be expressed using the rate of "secret-bits-per-sample". The imperceptibility (stego quality) has many measurement tools, such as the Peak-Signal-to-Noise-Ratio (PSNR), the Structural SIMilarity (SSIM) index (for images), and the Feature SIMilarity measure (for images). Robustness can be measured by calculating

the Bit-error-rate (BER) of the extracted secret data. More discussion on these measurements will be presented later in this paper.

Most recent research in the area of steganography endeavor to develop systems that can overcome this tri-trade-off challenge. Many published work claim to have introduced a better steganogrphy system that has come closer to solving the trade-off problem, and they compare with other systems published in the literature [20,18,21,1,15,16,17].

Usually, comparing the three different attributes of two different steganography systems is not a straightforward process. Researchers must keep two attributes constant, and check the third attribute's performance. This will require tedious experimental checks for every attribute. Moreover, these types of comparisons may be invalid because it becomes impossible - in some cases - for the two systems being compared to fix an attribute to a certain level, since they may be operating in two different ranges.

Hence, the need for a unified performance metric to combine the three opposing attributes of a steganography system; namely capacity, imperceptibility, robustness, into one conglomerate performance measure has become a must. This unified measure will help researchers rationally compare two different steganography systems even if they have different range values for their attributes. Moreover, having a comprehensive evaluation metric can assist choosing correctly the optimization technique since the comprehensive metric will point to the weak aspect of the technique. Later, the optimization technique will be responsible to improve that certain aspect which will improve the performance of the overall system [22].

This paper presents a novel conglomerate performance measure, the "Combined Capacity-Quality-Robustness Effectiveness" (CCQRE) metric. This measurement tool evaluates a steganography system based on its performance in the three attributes jointly. The idea behind the proposed CCQRE tool is to compute an efficiency percentage calculated by combining basis metric values of the three stego attributes using a parameter-controlled weighted average formulation. In other words, the proposed CCQRE measure gives the three attributes a proper weight based on the basis metric used (PSNR, SSIM, BER, etc..). Then, each attribute metric can be given a weight based on the type of comparison the researcher is interested in. Otherwise, if the interest is equal for all of the three attributes, the proposed CCQRE metric will reduce to the average of these measurement metrics.

The rest of this paper is organized as follows. In section 2 a quick background on various steganography measurement metrics is presented. The novel CCQRE metric is explained in detail in section 3, while section 4 presents some performance evaluation results using the proposed CCQRE measure and its variations.

2. Technical Background and Models

2.1. *Capacity Measurements*

Capacity refers to the size of the hidden secret data in reference to the cover medium. It is known that capacity is a critical attribute that has a major effect on the imperceptibility and robustness.

A digital image is a two-dimensional digital signal that represents an acquired scene. The smallest addressable element that forms up a digital image is the pixel, which can be represented by the number of bits that quantizes each pixel. The higher the number of bits used, the better the quality of the image. For images, there is a well-know formula to compute the embedding capacity in bits-per-pixel (bpp), which can be expressed as:

$$E_C = \frac{P_{sec} \times N}{P_{cover}} \times B, \tag{1}$$

where E_c is the actual embedding capacity calculated in bpp, P_{sec} is the number of secret pixels, P_{cover} is number of cover pixels, N is number of bits per pixel, and B is the number of image bands (channels). The default values used in this paper for P_{cover}, N, and B are 512×512, 8, and 3 for 3-band color images respectively, while $B = 1$ for grey-scale images.

2.2. *Imperceptibility Measurements*

The stego quality, or the imperceptibility, is a critical attribute of a steganography system; it is highly related to security, and it determines the workability of a steganography system. It is acceptable to have a system with low capacity and robustness levels, but certainly not imperceptibility. Having a poor imperceptibility level will make it easier for an eavesdropper to detect the presence of a secret message. This defeats the ultimate goal of steganography.

The importance of the stego quality (imperceptibility) attribute manifests in the huge number of stego measurements. This paper will focus on image steganography as an example of a steganography system. In general, image stego quality measurement tools can be classified into four main categories [23,24]:

(1) Pixel Difference-Based Measures.
(2) Correlation-Based Measures.
(3) Edge-Based Measures.
(4) Context-Based Measures.

(1) Pixel Difference-Based Measures: The pixel difference-based measures or the mean square distortion methods are the most famous techniques due to their simplicity and effectiveness. These techniques include:

   (a) Mean Square Error (MSE): MSE is a utility that measures the average of the squares of the errors between two signals to evaluate the similarities between

them. The MSE metric can be expressed as:

$$MSE(x, y) = \frac{1}{N} \sum_{i=1}^{N} (x_i - y_i)^2 , \tag{2}$$

where x and y are two discrete signals of finite-length, N is the number of signal samples (pixels, if the signals are images), and x_i and y_i are the values of the i_{th} samples in x and y respectively.
The MSE tool has many advantages that make it preferred in some cases. Firstly, its computational efficiency; all that is needed to compute the MSE is just a multiply and two additions per sample. Moreover, the method is memoryless; the evaluation can be evaluated at each sample independently. For images, MSE is not an accurate tool to determine the similarity of two images; it is just a pure mathematical operation that does not take into consideration the human visual perceptual system. [25].

(b) Mean Absolute Error (MAE): MAE is a tool that measures the difference between two signals by calculating the average vertical distance between each point and the Y=X line. In other words, MAE is simply summing the magnitudes of the errors and then dividing by the number of samples [26]. MAE can be expressed as:

$$MAE = \frac{\sum_{i=1}^{n} |e_i|}{n}, \tag{3}$$

where e_i is the model error calculated at the i_{th} sample, and n is the number of samples.

Similar to MSE, MAE has the advantage of simplicity, and the drawback of limited consideration for the human visual perceptual system.

(c) Peak-Signal-to-Noise-Ratio (PSNR): A more reliable measure that has been widely used by the signal processing community is the Peak-Signal-to-Noise-Ratio (PSNR) in decibels (dB) [27,28]. PSNR is calculated by finding the ratio between the maximum possible power of a signal and the power of corrupting noise. It is given by:

$$\text{PSNR} = 20 \log_{10} \left(\frac{L - 1}{MSE} \right), \tag{4}$$

where L is the number of gray levels in an image ($L = 256$ for 8-bit images), and MSE is the mean squared error described in equation (2).

PSNR has an advantage over MSE and MAE that it is less sensitive to minor differences between images which may not be observable by humans. Even though, PSNR does not fully exploit the human visual system principle.

(d) $L*a*b*$ Perceptual Error: The election of a color space for image quality testing is critical. This is because the color difference observed by a human must be harmonious with the intensity difference. This cannot be acheived with the standard RGB color space as it is a function of red, green, and blue channels. Instead, the $L*a*b*$ color space can be used. L for lightness and a and b represents colors. The similarity check can be achieved by the Euclidean distance [24]:

$$\begin{aligned} Euc_{L*,a*,b*} = \frac{1}{N^2} \sum_{r,c=0}^{N-1} [&\Delta L*(r,c)^2 \\ &+\Delta a*(r,c)^2 \\ &+\Delta b*(r,c)^2], \end{aligned} \tag{5}$$

where N is the number of pixels.

(e) Structural SIMilarity (SSIM): A recent approach to image fidelity measurement that tries to emulate the human visual perception of image structure, is the Structural SIMilarity (SSIM) index. Under the assumption that human visual perception is highly adapted for extracting structural information from a scene, SSIM was introduced as an alternative complementary framework for quality assessment based on the degradation of structural information [29,25]. Since that a human visual system is more sensitive to a change in the luminance or in the contrast channel, this new technique calculates the similarity based on some luminance and contrast measurements.
The SSIM value ranges between 1 (indicating two identical images) and 0 (indicating two completely different images) and is given by:

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}, \tag{6}$$

where x and y are the two images to be measured, μ_x is the average of image x, μ_y is the average of image y, σ_x^2 is the variance of image x, σ_x^2 is the variance of image y, σ_{xy} is the covarinace of x and y, c_1 and c_2 are used for division stabilization, and their default values are 0.01 and 0.03, respectively.

(2) Correlation-Based Measures: The second category is the correlation-based measures. These methods tend to find the similarity of two signals as a function of the displacement of one relative to the other. These techniques include:

(a) Normalized Cross-Correlation: Since the lighting and exposure conditions may vary for images, the images are first normalized. To find the similarity between

two digital images using the normalized cross-correlation method [30]:

$$NCC = \frac{1}{k}\sum_{k=1}^{k}\frac{\sum_{i,j=0}^{N-1} f(i,j)t(i,j)}{\sum_{i,j=0}^{N-1} f(i,j)^2}, \tag{7}$$

where t and f are the two images whose similarity is being measured, and k is the number of pixels.

(b) Czenakowski Distance: This tool suits comparing signals which are composed of positive elements only. That makes it applicable to digital image similarity checks [24].

$$C = \frac{1}{N^2}\sum_{i,j=0}^{N-1}(1 - \frac{2\sum_{k=1}^{k} min(f(i,j),t(i,j))}{\sum_{k=1}^{k}(f(i,j)+t(i,j))}), \tag{8}$$

where t and f are the two digital images to be compared, and N is the number of pixels.

The range of values of any metric in the cross-correlation category are $[0, 1]$. Two identical images will have a value of 1 (when the difference is zero). On the other hand, when the difference is high, the value of the metric will approach zero.

(3) Edge-Based Measures: Edges play an important role in the perception of an image for humans. Thus, vision techniques try to imitate this human behavior to have a better image understanding and perception level. To measure the quality of an image, or to study the similarity between two images, a check is made on edges of both images. This check compares the quality of edges in both images to determine the similarity. The edge quality is determined by the degradation and discontinuities presented in the edge [31]. A metric introduced by Pratt [32] takes into account both the precision of the edge position and the missing alarm edge elements. This measure operates by comparing an ideal reference edge map (of the cover image) with the distorted image edge map (of the stego image). The reference edge map is preferred to have a width of one pixel. The Pratt metric can be computed as:

$$P = \frac{1}{max(n_d, n_t)}\sum_{i=1}^{n_d}\frac{1}{1+ad_i^2}, \tag{9}$$

where a is a scale factor (normally $a = 1$), d_i is the distance from degraded edge to the reference edge, n_d is the number of detected edges in the degraded image, and n_t is the number of edges in the reference image.

The range of values of this metric are $[0, 1]$. The value increases with the quality of the degraded image. Thus, a value of 1 indicates two identical images.

(4) Context Measures: Similar to edges, the neighborhood information of the pixels are a critical piece of information that many image processing algorithms rely on to perform some tasks such as compression, and steganography. Image quality checks can also be performed using the neighborhood information of the pixels. Image distortion can be detected with the detection of any loss of information in the pixel neighborhoods. These kind of processes are highly based on context probabilities such as the probability mass function PMF of pixel neighborhoods. An image distortion can be detected when there is a change in the context probabilities [24].

2.3. *Robustness Measurements*

Robustness refers to the solidity of the stego medium, and its ability to keep the secret information undestroyed with the existence of noise and impairments. In this paper, a new robustness measure is proposed. This measure is based on the quality measures described earlier in 2.2. The idea is to compute the quality of the secret medium without the presence of any kind of impairments, and compare it with the quality of the secret medium when the impairment exists. This robustness measure can be formulated as:

$$R = \frac{Q_d}{Q_i}, \tag{10}$$

where Q_i is the quality of an ideal secret medium; without having any kind of impairments, and Q_d is the quality of the extracted secret medium with degradations; when the communication is being attacked for example.

The highest value that Q_d can reach is Q_i. The value of R in that case is 1 which is an indication that the stego algorithm is "ideal" in terms of robustness. Q_i and Q_d can be computed using any quality measurement tool described earlier in 2.2. PSNR and SSIM are the most widely used tools in the literature to find the quality of the stego medium for digital images. We, thus, choose to adopt these measures to implement the proposed robustness measure.

The proposed CCQRE metric is the first metric that aims to give a comprehensive evaluation of a data hiding algorithm, and evaluate the performance in terms of the hiding capacity capabilities, the imperceptibility level and the robustness level jointly in a single conglomerate measure. There is not currently a metric that combines the three opposing attributes (capacity, imperceptibility and robustness), as all of the current evaluation metrics are simply based on individual attribute. The need of having a combined metric can be summarized as follows:
1- Without using the proposed CCQRE metric, comparing the three different attributes of two different steganography systems is not an easy task since two attributes must be fixed to make it valid to compare the third attribute's performance. This will require several experimental checks for every attribute.
2- Without using the CCQRE, comparisons may be invalid because it might be impossible for the two systems being compared to fix an attribute to a certain level,

since they may be operating in two different ranges. For example, we can have an algorithm A that has the ability to hide in the range of [0-10 bpp], while algorithm B can hide in the range [18-20 bpp]. If we want to compare the imperceptibility performance of both techniques, then the capacity of both techniques must be fixed at a certain capacity rate. Without the proposed CCQRE metric, the comparison is not valid because both techniques operate in different hiding capacity ranges. However, this comparison can be done with the proposed CCQRE metric, since it will simply give the hiding capacity ratio a certain weight that will contribute to the final score out of 100% as will be discussed in section 3.

3. The Proposed CCQRE Metric

It is clear from the previous discussion in section 2 that no conglomerate measure exists in the literature that combines the three opposing attributes in one steganography metric. The need for a unified performance measure to combine the three opposing attributes of a steganography system; namely capacity, imperceptibility, robustness into one conglomerate performance measure has become essential to objectively compare two steganography systems even if they have different range values of their attributes.

The idea behind the proposed CCQRE tool is to compute an efficiency percentage calculated by combining basis measurement values of the three stego attributes using a parameter-controlled weighted average technique. Initially, the proposed CCQRE measure gives the three attributes a proper weight based on the basis metric used (PSNR, SSIM, BER, etc..). Then, each attribute metric can be given a weight based on the type of comparison the researcher is interested in. Otherwise, if the interest is equal for all of the three attributes, the proposed CCQRE metric will reduce to the average of these measurement metrics.

3.1. *General CCQRE Formulation*

The general form of the proposed CCQRE equation is as follows:

$$CCQRE_{\alpha,\beta,\gamma} = (\alpha C + \beta Q + \gamma R) \times 100\%, \tag{11}$$

where C, Q and R are the capacity, quality, and robustness efficiency rates of the steganography system, and α, β, and γ are weights that can be controlled based on the researcher's interest, such that $\alpha + \beta + \gamma = 1$.

In general, the efficiency rates: the capacity rate C, the quality rate Q and the robustness rate R are computed by normalizing the actual capacity, quality, or the robustness value obtained using the algorithm by the highest possible "ideal" value respectively.

For images, C can be computed based on the bits-per-pixel (bpp) concept described in equation (1). To find the capacity efficiency rate, the embedding capacity rate in bpp is divided by the maximum embedding rate an algorithm can reach to. This is equivilant to hiding a secret image into a cover image both with the same

size and the same number of bits used to code a pixel. That is 24 bpp for an 8-bits/channel RGB color images. In that case:

$$C = \frac{E_c}{24}, \tag{12}$$

where E_c is the actual embedding capacity for the steganography system in bpp.

Note that the value of 24 bpp is the highest capacity for an 8-bits/channel RGB color image; each pixel in each of the R,G,B bands requires 8 bits to encode.

The quality rate Q can be computed using any quality measure described earlier in section 2.2. The same concept used in equation (12) also applies here, but the denominator needs to be defined objectively. When using PSNR to represent Q, the PSNR value ranges from 0 to ∞ dB. However it is impossible to achieve a stego image with ∞ dB. After exhaustive research, and several tests, the authors have come to the conclusion that an objective PSNR range for steganography systems will be located within the range $[0 - 100]$ dB.

Therefore, when using PSNR, the quality measure may be defined as the normalized rate:

$$Q_{PSNR} = \frac{PSNR}{100}. \tag{13}$$

When using SSIM:

$$Q_{SSIM} = \frac{SSIM}{1}, \tag{14}$$

since the range of possible values for SSIM is $[0, 1]$.

The quality rate Q can also be computed using a combination of PSNR and SSIM:

$$Q_{SSIM+PSNR} = \omega Q_{PSNR} + (1 - \omega) Q_{SSIM} \tag{15}$$

ω is a scaling factor that can be tuned based on the researcher's interest. If the researcher has an equal interest in both measures, ω will equal 0.5.
In this case, equation (11) can be expressed as:

$$CCQRE^{\omega}_{\alpha,\beta,\gamma} = (\alpha C + \beta(\omega Q_{PSNR} + (1 - \omega) Q_{SSIM}) + \gamma R) \times 100\%, \tag{16}$$

where the calculation of R is as described in section 2.3.

3.2. *Euclidean CCQRE*

A version of the proposed CCQRE measure where CCQRE is described as a point in 3D space may also be formulated. The coordinates of this 3D space are C, Q, and R, described earlier in this section. Figure 3.2 illustrates the Euclidean CCQRE measure.

$$CCQRE_{euc} = \frac{1}{\sqrt{3}} \sqrt{C^2 + Q^2 + R^2} \tag{17}$$

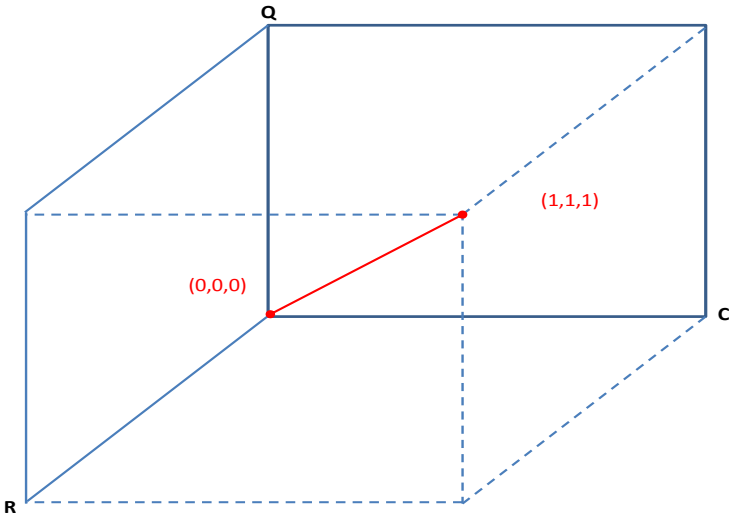

Fig. 1. The Euclidean CCQRE is equivilant of calculating the distance measure of the vector (C,Q,R) which describes a point in 3D space of the CQR-cube.

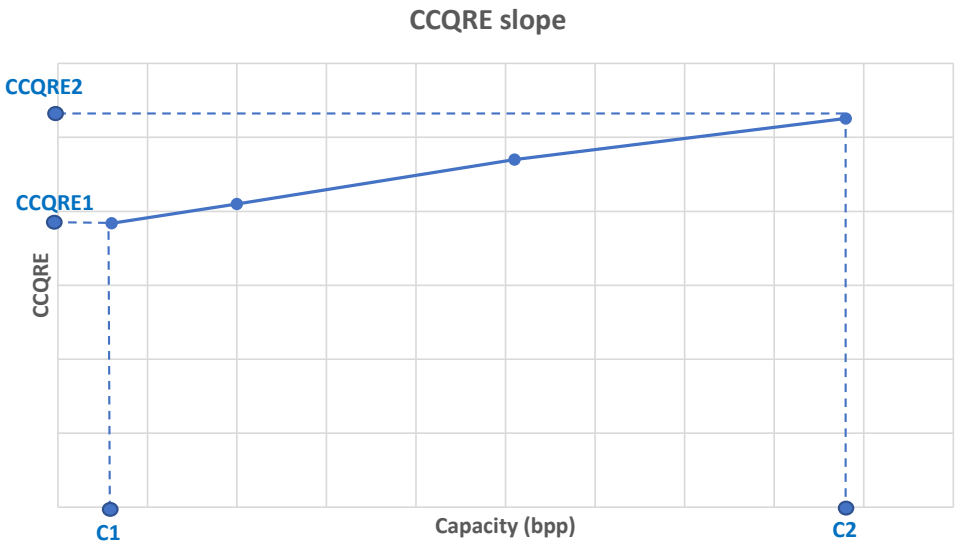

Fig. 2. The CCQRE slope.

3.3. *The CCQRE Slope*

A well-known trade-off between capacity and imperceptibility had become a major challenge for researchers in the steganography systems research area [20,33,34,18,21,1,15]. An additional measure that CCQRE can provide is the CCQRE slope. This measure is to check the efficiency of dealing with the capacity-imperceptibility trade-off problem by a steganography system. Figure 2 illustrates the idea of the CCQRE slope. Initially, The CCQRE is calculated at different capacity levels of the same scheme. Then, the CCQRE slope can be calculated by the following equation:

$$CCQRE_{slope,d} = \frac{CCQRE_2 - CCQRE_1}{C_2 - C_1}, \tag{18}$$

where C_2 is a chosen higher-extreme capacity value obtained by the scheme, C_1 is a chosen lower-extreme capacity value obtained by the scheme. $CCQRE_2$ is the CCQRE value calculated when the capacity is equal to C_2, $CCQRE_1$ is the CCQRE value calculated when the capacity is equal to C_1. The distance d is $C_2 - C_1$. Figure (2) visualizes these points.

If the $CCQRE_{slope,d}$ is a positive value, then this is an indication that the system is performing well in terms of dealing with the trade-off; the CCQRE is increasing even though the capacity is increasing. That can happen if the increase in the capacity is much faster than the decrease in the stego quality, or even in some rare cases, the capacity is increasing, and the stego quality is also increasing, as in the steganography scheme proposed by Rabie *et. al.* in [15]. In general, $CCQRE_{slope}$ can range from $[-\infty,\infty]$, the higher the value, the better the system in dealing with the trade-off. Note that to have a valid comparison of the $CCQRE_{slope,d}$ between two systems, the distance d between C_2 and C_1 must be constant for both systems. Another note to be considered is the larger the value of the distance d, the more accurate the $CCQRE_{slope,d}$ value will be.

4. Experimental Evaluations

The ultimate goal behind the CCQRE measure is to provide a utility that can assist researchers in comparing between steganography systems based on the researcher's interest in Capacity, Imperceptibility (stego quality), and Robustness.

To show the effectiveness of the proposed measure, table 1 shows comparative results of various steganography systems, and shows the achieved capacities and stego qualities in PSNR and SSIM by each system. It is clear from the table that it is hard to compare between these schemes, and decide which is better since none of the attributes are constant. In general, when comparing two systems for a feature, all other features must be constant, and only then will the comparison be valid.

For steganography systems, it might be hard to fix all attributes to a certain level between two systems as they may operate in two different attribute ranges. For example, a scheme such as DWT-LPAR (2017) [17] cannot hide below 18 bpp, while

Table 1. Comparative results expressed as maximum Capacity (bpp), PSNR (dB), SSIM values for the various methods. Highest Capacities and PSNR values are emphasized in a bold font.

Method	Capacity	PSNR	SSIM
Lin *et. al.* (2010) [35]	6.0	**54.22**	**0.9953**
Padmaa *et. al.* (2010) [36]	9.901	**38.61**	0.9849
Bhattacharyya *et. al.* (2012) [37]	0.5	34.92	0.9834
Ghebleh & Kanso (2014) [38]	4.39	**52.30**	**0.9982**
Balasubramanian *et. al.* (2014) [39]	12	**35.56**	0.8000
Qin *et. al.* (2015) [40]	2.74	**37.62**	0.9844
Adi *et. al.* (2015) [41]	1.5	**52.38**	**0.9976**
Wu *et. al.* (2015) [42]	6.0	27.8	0.8447
Gao *et. al.* (2015) [43]	6.0	34.6	0.9079
Rabie FB-GAR (2016) [21]	**20.83**	27.24	0.9766
Rabie QTAR (2016) [1]	**21.01**	27.21	0.9767
Rabie CF-FB-GAR (2017) [15]	**21.71**	29.20	0.9875
Rabie CF-QTAR (2017) [15]	**22.52**	28.16	0.9515
Al-Dhamari *et. al.* (2017) [44]	11.0	33.84	**0.9908**
Kocak & Cemal (2017) [45]	5.72	**33.37**	**0.9940**
CF-LPAR [3-point] (2017) [16]	**18.1**	**44.6**	0.9890
CF-LPAR [5-point] (2017) [16]	**19.5**	32.0	**0.9960**
DWT-LPAR (2017) [17]	**20.57**	**42.4**	**0.9980**

another scheme, such as Lin*et. al.* (2010) [35] cannot hide above 18 bpp. Therefore comparing both schemes will not be valid based on hiding capacity as their payload capability range is not the same. To be more clear, it is obvious from table 1, that the steganography system proposed by Lin*et. al.* (2010) [35] cannot reach the capacity achieved by Rabie's CF-FB-GAR method (2017) [15]. Thus, it will not be valid to compare these two systems using traditional performance measures.

So now, which steganography system can be considered as performing "the best"? Is it the system proposed by Lin *et. al.* (2010) [35]?, as it has achieved a very high PSNR value, or is it the system proposed by Ghebleh & Kanso (2014) [38] with its high SSIM value?, or can it be the CF-QTAR scheme proposed by Rabie (2017) [15] which achieved a very large capacity? Also, what does "the best" signify? Does it indicate that the proposed scheme is the best in capacity?, or best in imperceptibility (PSNR or SSIM)?, or best in robustness? The proposed CCQRE performance measure tool may bring some rational answers to these questions.

4.1. *Theoretical and Practical Analysis*

Case 1: Equal Interest Between Capacity and Quality
Assume that a proposed stego scheme's interest is equal between the Capacity, Quality, but there is no interest in Robustness. In that case the CCQRE metric may be formulated as:

$$CCQRE_{0.5,0.5,0} = \frac{1}{2}C + \frac{1}{2}Q + 0 \times R \tag{19}$$

Case 1-a: Equal Interset Between PSNR and SSIM
In this case, the interest is assumed to be equal between PSNR and SSIM. Thus:

$$Q = \frac{1}{2} \times \frac{PSNR}{100} + \frac{1}{2} \times SSIM \tag{20}$$

Then the full equation for the CCQRE, using $CCQRE^{\omega}_{\alpha,\beta,\gamma}$ notation described in equation (16), will be:

$$CCQRE^{0.5}_{0.5,0.5,0} = \frac{1}{2}(\frac{E_c}{24}) + \frac{1}{2}(\frac{1}{2} \times \frac{PSNR}{100} + \frac{1}{2} \times SSIM), \tag{21}$$

where E_c is the embedding capacity achieved by the system.
The CCQRE calculation based on equation (21) is added to table 2.

It is now clear, based on the criteria mentioned earlier in equation (21), that the DWT-LPAR algorithm is "the best" among other algorithms listed in the table. Recall that the interest was equal for capacity and quality, and equal for PSNR and SSIM. Now, the phrase "the best" is well defined and not an ambiguous phrase anymore.

Case 1-b: Interest in PSNR Only
Let us change the preferences used in equation (21), and assume that the interest is still equal between capacity and quality, but the interest is only in PSNR. In this case, the CCQRE (equation (16)) will be :

$$CCQRE^{1}_{0.5,0.5,0} = \frac{1}{2}(\frac{E_c}{24}) + \frac{1}{2}(\frac{PSNR}{100}) \tag{22}$$

Table 3 now shows the new CCQRE calculations based on equation (22). Based on the new criteria, DWT-LPAR achieved the highest score with an efficiency of 64.05%, followed by Rabie CF-QTAR (2017) [15] with 61.0%. In the third place, CF-LPAR [3-point] with 60.0%.

Case 1-c: Interest in SSIM Only
Now, consider the researcher's interest in a quality measure that takes into consideration the human visual system and its concepts. In this case the SSIM quality metric may be preferred over PSNR. However, if the interest is equal between capacity and quality, then in such a case the CCQRE (equation (16)) will be:

$$CCQRE^{0}_{0.5,0.5,0} = \frac{1}{2}(\frac{E_c}{24}) + \frac{1}{2}(SSIM) \tag{23}$$

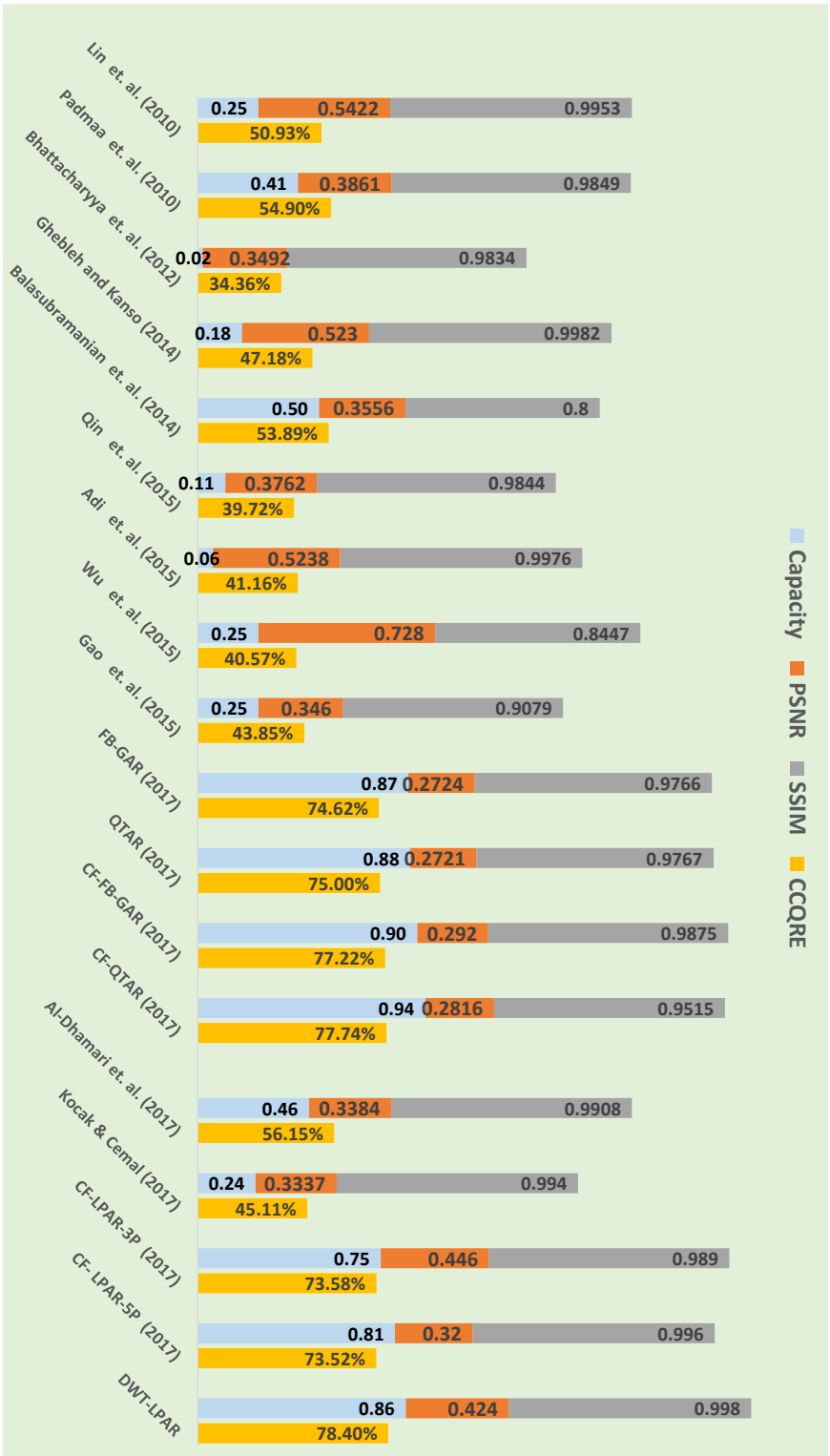

Fig. 3. Comparative results expressed as maximum Capacity, PSNR, SSIM, and CCQRE values for the various methods. CCQRE is calculated using equation (21)

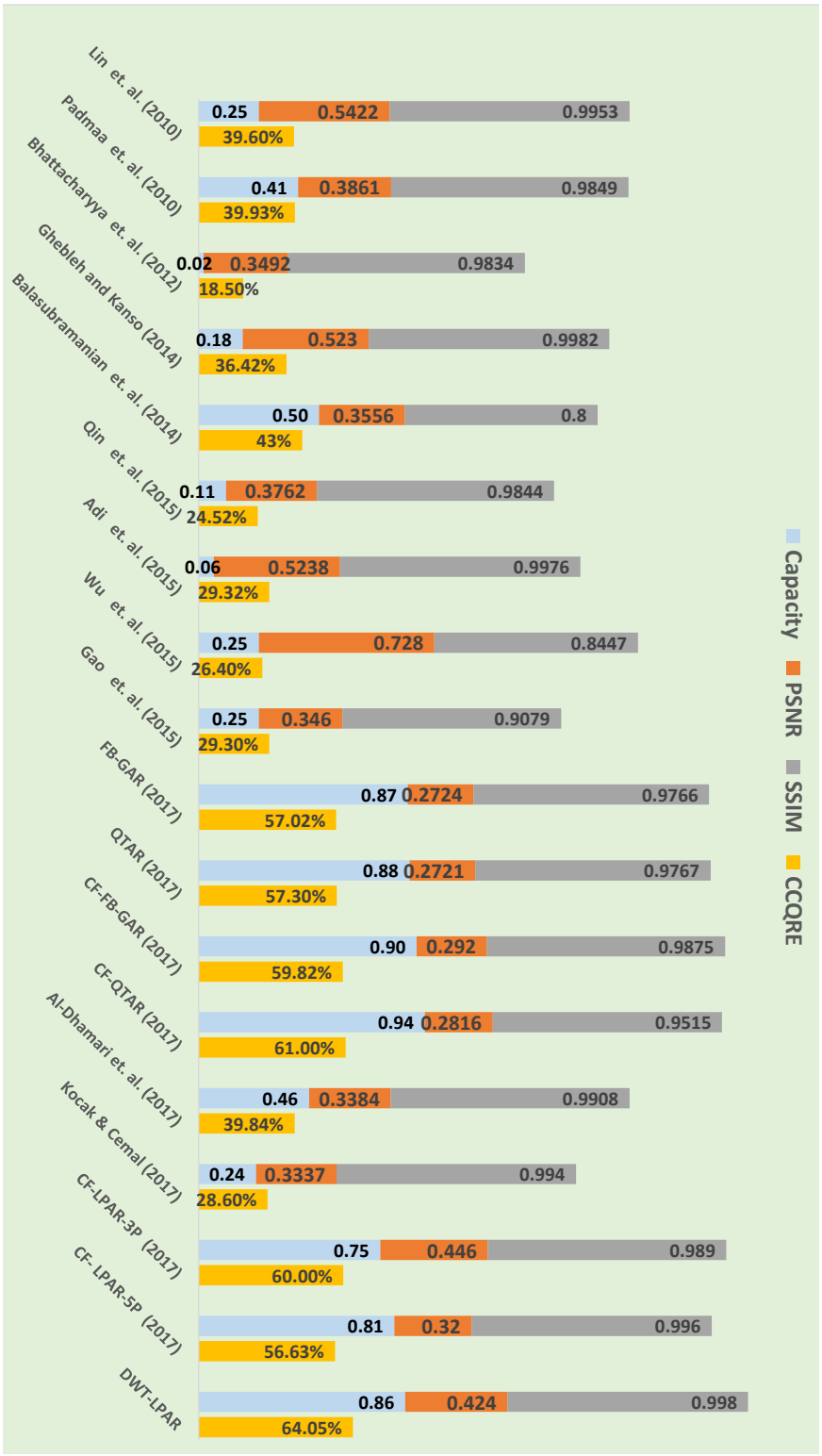

Fig. 4. Comparative results expressed as maximum Capacity, PSNR, SSIM, and CCQRE values for the various methods. CCQRE is calculated using equation (22)

Table 2. Comparative results expressed as maximum Capacity (bpp), PSNR (dB), SSIM, and CCQRE values for the various methods. Highest Capacities and PSNR values are emphasized in a bold font. $CCQRE^{0.5}_{0.5,0.5,0}$ is calculated using equation (21)

Method	Capacity	PSNR	SSIM	CCQRE
Lin *et. al.* (2010) [35]	6.0	**54.22**	**0.9953**	50.93%
Padmaa *et. al.* (2010) [36]	9.901	**38.61**	0.9849	54.90%
Bhattacharyya *et. al.* (2012) [37]	0.5	34.92	0.9834	34.36%
Ghebleh & Kanso (2014) [38]	4.39	**52.30**	**0.9982**	47.18%
Balasubramanian *et. al.* (2014) [39]	12	**35.56**	0.8000	53.89%
Qin *et. al.* (2015) [40]	2.74	**37.62**	0.9844	39.72%
Adi *et. al.* (2015) [41]	1.5	**52.38**	**0.9976**	41.16%
Wu *et. al.* (2015) [42]	6.0	27.8	0.8447	40.57%
Gao *et. al.* (2015) [43]	6.0	34.6	0.9079	43.85%
Rabie FB-GAR (2016) [21]	**20.83**	27.24	0.9766	**74.62%**
Rabie QTAR (2016) [1]	**21.01**	27.21	0.9767	**75.0%**
Rabie CF-FB-GAR (2017) [15]	**21.71**	29.20	0.9875	**77.22%**
Rabie CF-QTAR (2017) [15]	**22.52**	28.16	0.9515	**77.74%**
Al-Dhamari *et. al.* (2017) [44]	11.0	33.84	**0.9908**	56.15%
Kocak & Cemal (2017) [45]	5.72	33.37	**0.9940**	45.11%
CF-LPAR [3-point] (2017) [16]	**18.1**	**44.6**	0.9890	**73.58%**
CF-LPAR [5-point] (2017) [16]	**19.5**	32.0	**0.9960**	**73.52%**
DWT-LPAR (2017) [17]	**20.57**	**42.4**	**0.9980**	**78.40%**

Table 4 shows the new CCQRE calculations based on equation (23). Based on this new criteria, Rabie CF-FB-GAR (2017) [15] achieved the highest score with a CCQRE of 94.60%, followed by Rabie CF-QTAR (2017) [15] with 94.49%. In third place, DWT-LPAR with 92.75%.

Case 2: Watermarking Schemes

For the case of watermark embedding systems, achieving high capacities is not a critical issue. Instead, imperceptibility (stego quality) is a much more important issue for such watermarking system. The proposed CCQRE can help elect the most suitable watermarking scheme. That can be done by tuning the parameters α, β, and γ described in equation (3). α can be given a small value since capacity is not

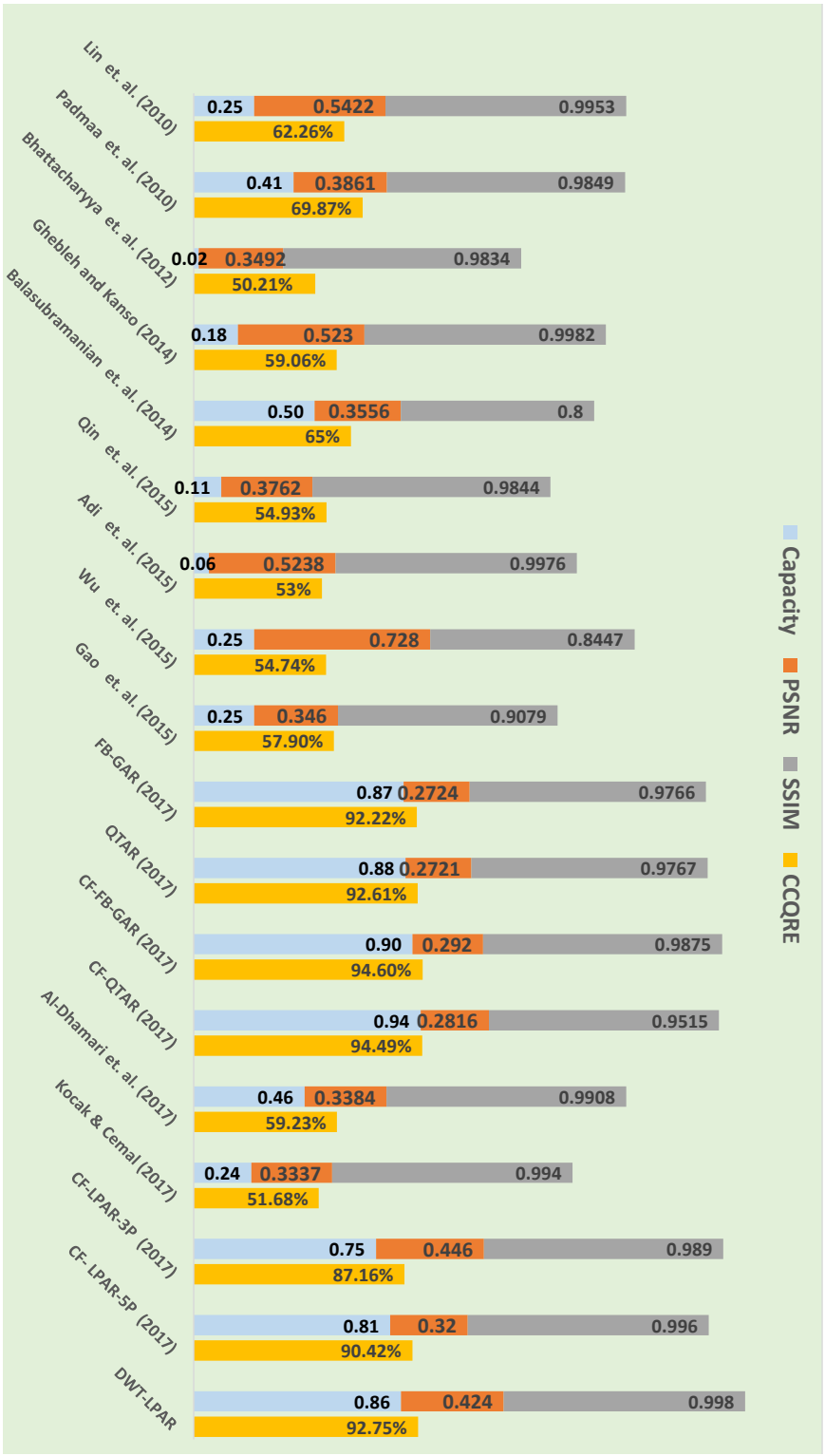

Fig. 5. Comparative results expressed as maximum Capacity, PSNR, SSIM, and CCQRE values for the various methods. CCQRE is calculated using equation (23)

Table 3. Comparative results expressed as maximum Capacity (bpp), PSNR (dB), SSIM, and CCQRE values for the various methods. Highest Capacities and PSNR values are emphasized in a bold font. $CCQRE^{1}_{0.5,0.5,0}$ is calculated using equation (22)

Method	Capacity	PSNR	SSIM	CCQRE
Lin *et. al.* (2010) [35]	6.0	**54.22**	**0.9953**	39.60%
Padmaa *et. al.* (2010) [36]	9.901	**38.61**	0.9849	39.93%
Bhattacharyya *et. al.* (2012) [37]	0.5	34.92	0.9834	18.50%
Ghebleh & Kanso (2014) [38]	4.39	**52.30**	**0.9982**	36.42%
Balasubramanian *et. al.* (2014) [39]	12	**35.56**	0.8000	42.78%
Qin *et. al.* (2015) [40]	2.74	**37.62**	0.9844	24.52%
Adi *et. al.* (2015) [41]	1.5	**52.38**	**0.9976**	29.32%
Wu *et. al.* (2015) [42]	6.0	27.8	0.8447	26.40%
Gao *et. al.* (2015) [43]	6.0	34.6	0.9079	29.3%
Rabie FB-GAR (2016) [21]	**20.83**	27.24	0.9766	**57.02%**
Rabie QTAR (2016) [1]	**21.01**	27.21	0.9767	**57.3%**
Rabie CF-FB-GAR (2017) [15]	**21.71**	29.20	0.9875	**59.82%**
Rabie CF-QTAR (2017) [15]	**22.52**	28.16	0.9515	**61.0%**
Al-Dhamari *et. al.* (2017) [44]	11.0	33.84	**0.9908**	39.84%
Kocak & Cemal (2017) [45]	5.72	33.37	**0.9940**	28.6%
CF-LPAR [3-point] (2017) [16]	**18.1**	**44.6**	0.9890	**60.0%**
CF-LPAR [5-point] (2017) [16]	**19.5**	32.0	**0.9960**	**56.63%**
DWT-LPAR (2017) [17]	**20.57**	**42.4**	**0.9980**	**64.05%**

an important aspect for watermarking. The CCQRE (equation (16)) will be:

$$CCQRE^{0.5}_{0.1,0.9,0} = 0.1(\frac{E_c}{24}) + 0.9\ (0.5 \times \frac{PSNR}{100} + 0.5 \times SSIM), \tag{24}$$

where α is equal to 0.1, and β is equal to 0.9. The interest is equal for PSNR and SSIM, so both are given a scale of 0.5.

Table 5 shows the new CCQRE calculations based on equation (24). Based on the new criteria, DWT-LPAR achieved the highest score with an efficiency of 72.56%, followed by CF-LPAR [3-point] with 94.49%. In the third place, Lin *et. al.* (2010) [35] with 71.69%. Lin *et. al.* (2010) [35] got a very high percentage even though the capacity achieved is very low (6 bpp) which is much lower than other schemes (in 20's bpp). That is an indication that the CCQRE is performing precisely based on the criteria preferred.

Figrue 7 summarizes tables 2, 3, 4, and 5 in a single bar graph. The figure clearly

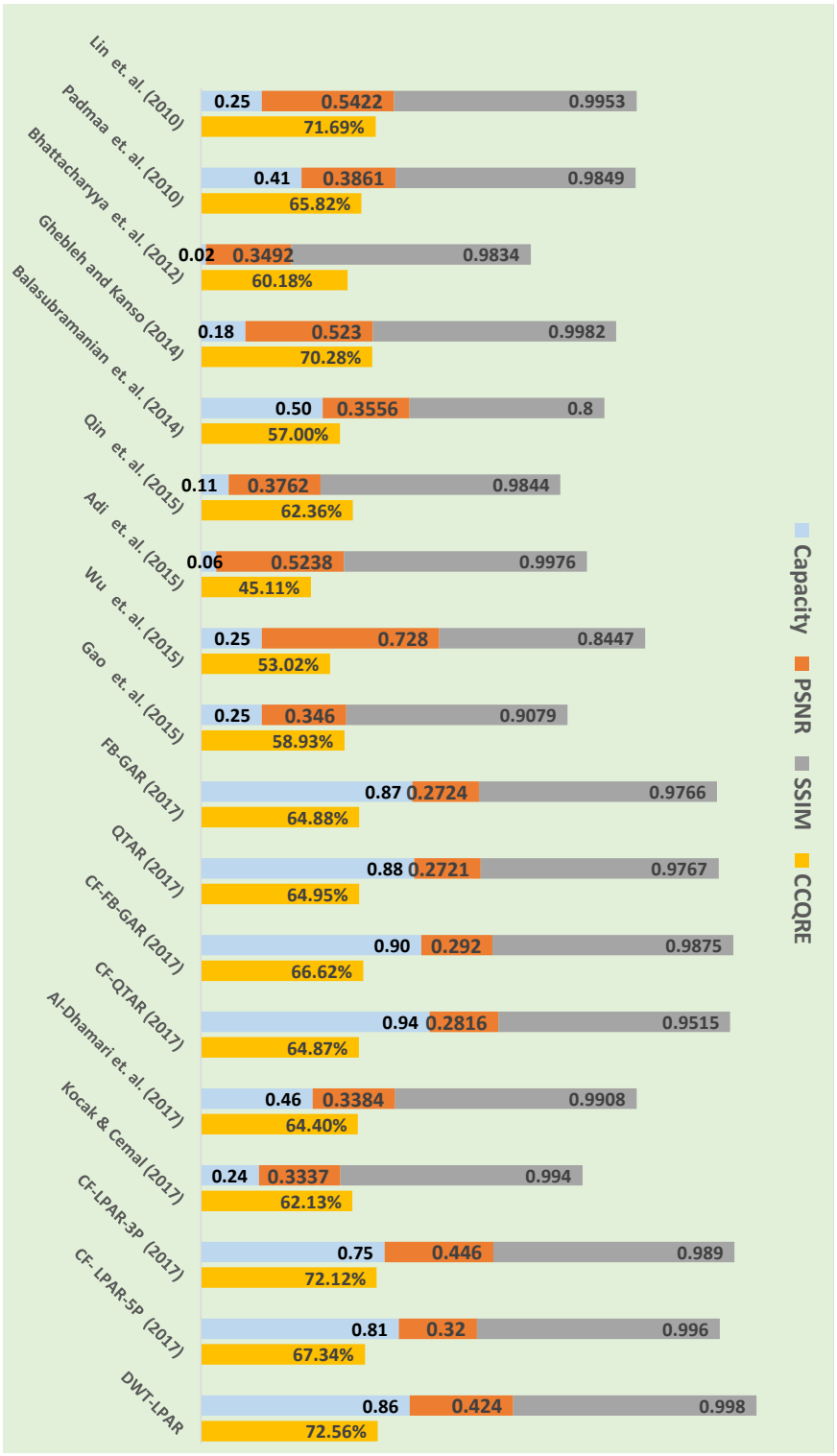

Fig. 6. Comparative results expressed as maximum Capacity, PSNR, SSIM, and CCQRE values for the various methods. CCQRE is calculated using equation (24)

Table 4. Comparative results expressed as maximum Capacity (bpp), PSNR (dB), SSIM, and CCQRE values for the various methods. Highest values are emphasized in a bold font. $CCQRE^{0}_{0.5,0.5,0}$ is calculated using equation (23)

Method	Capacity	PSNR	SSIM	CCQRE
Lin *et. al.* (2010) [35]	6.0	**54.22**	**0.9953**	62.26%
Padmaa *et. al.* (2010) [36]	9.901	**38.61**	0.9849	69.87%
Bhattacharyya *et. al.* (2012) [37]	0.5	34.92	0.9834	50.21%
Ghebleh & Kanso (2014) [38]	4.39	**52.30**	**0.9982**	59.06%
Balasubramanian *et. al.* (2014) [39]	12	**35.56**	0.8000	65%
Qin *et. al.* (2015) [40]	2.74	**37.62**	0.9844	54.93%
Adi *et. al.* (2015) [41]	1.5	**52.38**	0.9976	53.0 %
Wu *et. al.* (2015) [42]	6.0	27.8	0.8447	54.74%
Gao *et. al.* (2015) [43]	6.0	34.6	0.9079	57.90%
Rabie FB-GAR (2016) [21]	**20.83**	27.24	0.9766	**92.22%**
Rabie QTAR (2016) [1]	**21.01**	27.21	0.9767	**92.61%**
Rabie CF-FB-GAR (2017) [15]	**21.71**	29.20	0.9875	**94.60%**
Rabie CF-QTAR (2017) [15]	**22.52**	28.16	0.9515	**94.49%**
Al-Dhamari *et. al.* (2017) [44]	11.0	33.84	**0.9908**	59.23%
Kocak & Cemal (2017) [45]	5.72	**33.37**	**0.994**	51.68%
CF-LPAR [3-point] (2017) [16]	**18.1**	**44.6**	0.989	**87.16%**
CF-LPAR [5-point] (2017) [16]	**19.5**	32.0	**0.9960**	**90.42%**
DWT-LPAR (2017) [17]	**20.57**	**42.4**	**0.9980**	**92.75%**

illustrates the benefits of having different CCQRE calculations. The first column to the left of each embedding scheme is simply a cumulative sum of capacity rate, PSNR rate, and the SSIM. From the first sight, and based on the cumulative sum, DWT-LPAR scheme might be thought of to be the "best hiding scheme". The phrase "best hiding scheme", sounds ambiguous and misleading. The main idea of CCQRE is to compare different hiding schemes based on some criterias specified by the researcher. Based on the figure, although DWT-LPAR got the highest cumulitve sum, the CF-QTAR has acheived the highest CCQRE (calculated using equation (23)). Equation (23) represents a quality measure that takes in consideration the human visual system and its perception. Thus, it focuses on SSIM rather than PSNR. On the other hand, the interest is equal between capacity and quality. So if a researcher is more interseted in visiual perception, CCQRE equation (23) can help in choosing precisely the scheme that will meet this interest. Another in-

Table 5. Comparative results expressed as maximum Capacity, PSNR, SSIM, and CCQRE values for the various methods. Highest values are emphasized in a bold font. $CCQRE^{0.5}_{0.1,0.9,0}$ is calculated using equation (24)

Method	Capacity	PSNR	SSIM	CCQRE
Lin *et. al.* (2010) [35]	6.0	**54.22**	**0.9953**	**71.69%**
Padmaa *et. al.* (2010) [36]	9.901	**38.61**	0.9849	65.82%
Bhattacharyya *et. al.* (2012) [37]	0.5	34.92	0.9834	60.18%
Ghebleh & Kanso (2014) [38]	4.39	**52.30**	**0.9982**	**70.28%**
Balasubramanian *et. al.* (2014) [39]	12	**35.56**	0.8000	57%
Qin *et. al.* (2015) [40]	2.74	**37.62**	0.9844	62.36%
Adi *et. al.* (2015) [41]	1.5	**52.38**	0.9976	45.11%
Wu *et. al.* (2015) [42]	6.0	27.8	0.8447	53.02%
Gao *et. al.* (2015) [43]	6.0	34.6	0.9079	58.93%
Rabie FB-GAR (2016) [21]	**20.83**	27.24	0.9766	64.88%
Rabie QTAR (2016) [1]	**21.01**	27.21	0.9767	64.95%
Rabie CF-FB-GAR (2017) [15]	**21.71**	29.20	0.9875	66.62%
Rabie CF-QTAR (2017) [15]	**22.52**	28.16	0.9515	64.87%
Al-Dhamari *et. al.* (2017) [44]	11.0	33.84	**0.9908**	64.40%
Kocak & Cemal (2017) [45]	5.72	**33.37**	**0.994**	62.13%
CF-LPAR [3-point] (2017) [16]	**18.1**	**44.6**	0.989	**72.12%**
CF-LPAR [5-point] (2017) [16]	**19.5**	32.0	**0.9960**	67.34%
DWT-LPAR (2017) [17]	**20.57**	**42.4**	**0.9980**	**72.56%**

teresting result, is the CCQRE result obtained by the embedding scheme Lin *et. al.* (2010) [35] and Ghebleh & Kanso (2014) [38] using equation (23). Although the embedding capacity reached by the scheme is much less than other embedding schemes, Lin's scheme was able to compete other high embedding schemes, and even pass many others. That is because the CCQRE equation (23) is well-defined for comparing watermarking schemes where achieving high capacities is not a critical issue. Instead, imperceptibility (stego quality) is a much important issue for watermarking systems. So Let's assume that a researcher wants to use a watermarking system in his work. Without CCQRE, he might not choose the most suitable scheme for his use.

Case 3: Incorporating Robustness

Next, some additional tests are made adding the robustness efficiency rate. For such experiments, the PSNR/SSIM of the secret image must be known for both the

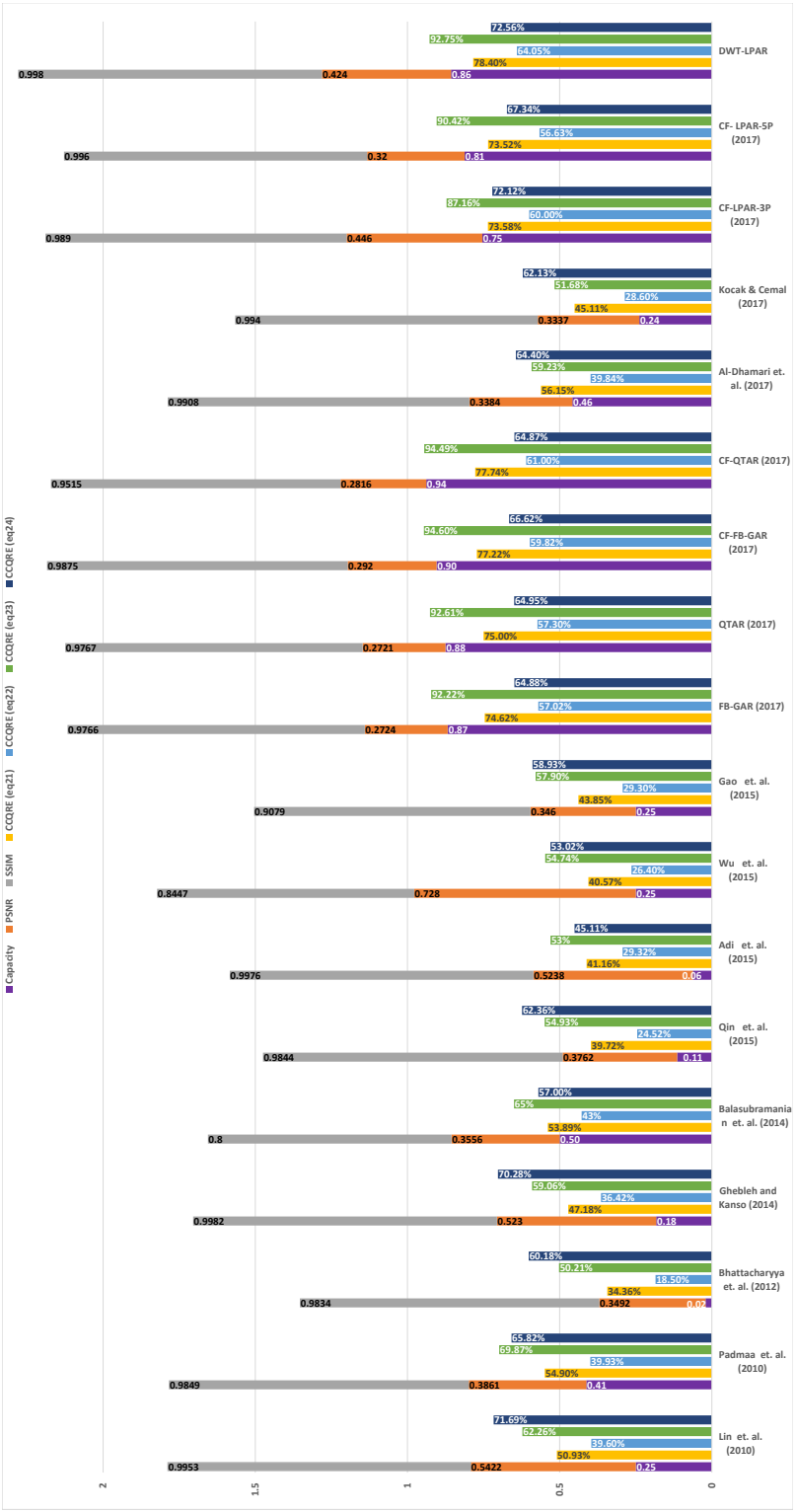

Fig. 7. Summarizing tables 2, 3, 4, and 5 in a bar graph. This graph shows how different CCQRE calculations can vary based on the researcher's interest in capacity, PSNR, or SSIM

ideal secret image and the degraded secret image (noisy extraction). These data are available in the DWT-LPAR and CF-LPAR methods. Adding the robustness measure, the CCQRE equation becomes:

$$CCQRE^{1}_{\frac{1}{3},\frac{1}{3},\frac{1}{3}} = \frac{1}{3}C + \frac{1}{3}Q + \frac{1}{3}R, \tag{25}$$

Since ω is 1, PSNR will be used, in this case, the CCQRE (equation (16)) will be:

$$CCQRE^{1}_{\frac{1}{3},\frac{1}{3},\frac{1}{3}} = (\frac{1}{3} \times \frac{E_c}{24}) + (\frac{1}{3} \times \frac{PSNR_s}{100}) + (\frac{1}{3} \times \frac{PSNR_d}{PSNR_i}), \tag{26}$$

where $PSNR_s$ is the PSNR value of the stego image, $PSNR_d$ is the PSNR value of the secret image after noisy extraction (degraded secret image), $PSNR_i$ is the PSNR value of the secret image after clear extraction (ideal secret image).

Tables 6 and 7 show the new CCQRE calculations for the DWT-LPAR [17] and CF-LPAR [16] methods respectively based on equation (26). Figure 8 illustrates comparative results expressed as maximum Capacity, $PSNR_s$, $PSNR_i$,$PSNR_d$, and CCQRE values for the various methods. CCQRE is calculated using equation (26).

Table 6. Comparative results expressed as maximum Capacity (bpp), $PSNR_s$ (dB), $PSNR_i$ (dB), $PSNR_d$(dB) and CCQRE values for the DWT-LPAR [17] method. $CCQRE^{1}_{\frac{1}{3},\frac{1}{3},\frac{1}{3}}$ is calculated using equation (26).

Noise (density)	Capacity	$PSNR_s$	$PSNR_i$	$PSNR_d$	R	$CCQRE$
Salt & pepper (0.0001)	20.34	36.72	77.24	20.34	0.26	49.27%
Salt & pepper (0.0005)	20.34	36.72	77.24	20.33	0.26	49.26%
Salt & pepper (0.001)	20.34	36.72	77.24	14.28	0.39	46.65%
Speckle (0.0001)	20.34	36.72	77.24	22.67	0.62	50.27%
Speckle (0.0005)	20.34	36.72	77.24	17.09	0.47	47.87%
Speckle (0.001)	20.34	36.72	77.24	15.27	0.42	47.08%

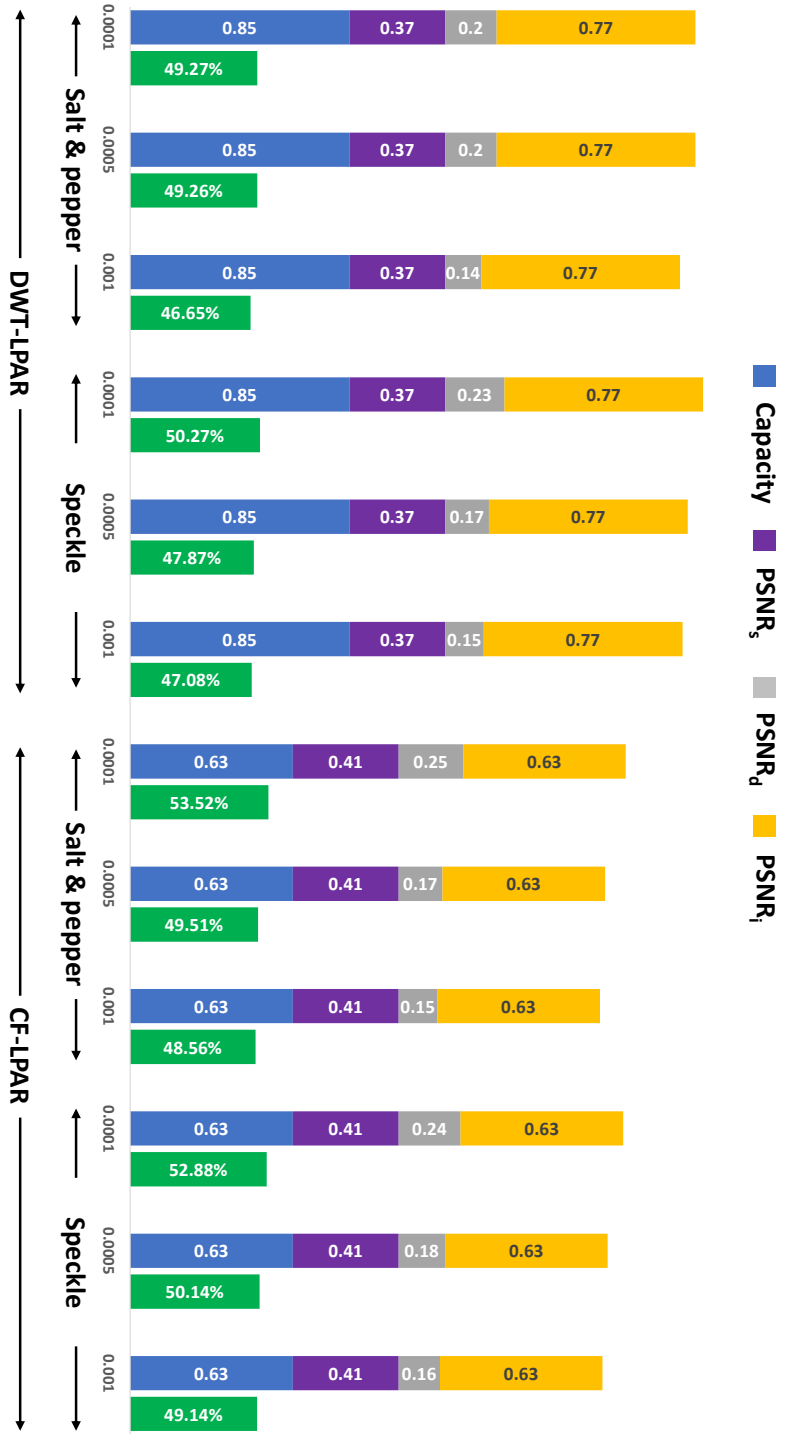

Fig. 8. Comparative results expressed as maximum Capacity, $PSNR_s$, $PSNR_i$,$PSNR_d$, and CCQRE values for the various methods. CCQRE is calculated using equation (26).

Table 7. Comparative results expressed as maximum Capacity (bpp), $PSNR_s$ (dB), $PSNR_i$ (dB), $PSNR_d$ (dB) and CCQRE values for the CF-LPAR [16]. $CCQRE^{1}_{\frac{1}{3},\frac{1}{3},\frac{1}{3}}$ is calculated using equation (26).

Noise (density)	Capacity	$PSNR_s$	$PSNR_i$	$PSNR_d$	R	$CCQRE$
Salt & pepper (0.0001)	15.1	41.4	63.2	24.7	0.39	53.52%
Salt & pepper (0.0005)	15.1	41.4	63.2	17.1	0.27	49.51%
Salt & pepper (0.001)	15.1	41.4	63.2	15.3	0.24	48.56%
Speckle (0.0001)	15.1	41.4	63.2	23.5	0.37	52.88%
Speckle (0.0005)	15.1	41.4	63.2	18.3	0.29	50.14%
Speckle (0.001)	15.1	41.4	63.2	16.4	0.26	49.14%

4.2. *Using Euclidean CCQRE*

Tables 8 and 9 show the new CCQRE calculations for the DWT-LPAR [17] and CF-LPAR [16] methods respectively based on equation (17).

4.3. *Using CCQRE Slope*

Figures 9-(a,b,c,d) visualize the data of table 10 in graphical form, and demonstrate the $CCQRE_{slope,8.2}$ metric for the CF-LPAR steganography scheme.

When considering robustness in calculations (for example equation (25)), $PSNR_s$, $PSNR_i$, and $PSNR_d$ values are needed. Table 11 shows these values, and a graphical representation is provided in figure 9-e. The CCQRE slopes were obtained using the following formulas:

for figure 9-a:

$$CCQRE_{slope,8.2} = \frac{70.38 - 55.2}{18.8 - 10.6} = 1.85, \tag{27}$$

for figure 9-b:

$$CCQRE_{slope,8.2} = \frac{52.56 - 38.38}{18.8 - 10.6} = 1.73, \tag{28}$$

Table 8. Comparative results expressed as maximum Capacity (bpp), $PSNR_s$ (dB), $PSNR_i$ (dB), $PSNR_d$ (dB), and CCQRE values for the DWT-LPAR [17] method. $CCQRE_{euc}$ is calculated using equation (17).

Noise (density)	Capacity	$PSNR_s$	$PSNR_i$	$PSNR_d$	R	$CCQRE$
Salt & pepper (0.0001)	20.34	36.72	77.24	20.34	0.26	55.45%
Salt & pepper (0.0005)	20.34	36.72	77.24	20.33	0.26	55.45%
Salt & pepper (0.001)	20.34	36.72	77.24	14.28	0.39	54.38%
Speckle (0.0001)	20.34	36.72	77.24	22.67	0.62	55.95%
Speckle (0.0005)	20.34	36.72	77.24	17.09	0.47	54.83%
Speckle (0.001)	20.34	36.72	77.24	15.27	0.42	54.53%

for figure 9-c:

$$CCQRE_{slope,8.2} = \frac{88.2 - 72.0}{18.8 - 10.6} = 1.97, \tag{29}$$

for figure 9-d:

$$CCQRE_{slope,8.2} = \frac{64.02 - 64.03}{18.8 - 10.6} = 0, \tag{30}$$

and for figure 9-e:

$$CCQRE_{slope,8.2} = \frac{41.07 - 28.84}{18.8 - 10.6} = 1.49. \tag{31}$$

Thus, since the CCQRE slope is a positive value, the CF-LPAR scheme can be considered as a system that is dealing well with the capacity-imperceptibility trade-off; it is an indication that the increase in the capacity is much faster than the decrease in the stego quality.

4.4. *Testing CCQRE on a DCT-Based Method*

In this section, a new steganography method is designed in order to evaluate the effectiveness of the proposed CCQRE metric. The new technique is based on the Discrete Cosine Transform (DCT) where hiding the secret image takes place into

Table 9. Comparative results expressed as maximum Capacity (bpp), $PSNR_s$ (dB), $PSNR_i$ (dB), $PSNR_d$ (dB), and CCQRE values for the CF-LPAR [16]. $CCQRE_{euc}$ is calculated using equation (17).

Noise (density)	Capacity	$PSNR_s$	$PSNR_i$	$PSNR_d$	R	$CCQRE$
Salt & pepper (0.0001)	15.1	41.4	63.2	24.7	0.39	48.99%
Salt & pepper (0.0005)	15.1	41.4	63.2	17.1	0.27	46.20%
Salt & pepper (0.001)	15.1	41.4	63.2	15.3	0.24	45.67%
Speckle (0.0001)	15.1	41.4	63.2	23.5	0.37	48.49%
Speckle (0.0005) (0.0005)	15.1	41.4	63.2	18.3	0.29	46.59%
Speckle (0.001) (0.001)	15.1	41.4	63.2	16.4	0.26	45.99%

Table 10. set of data obtained using CF-LPAR scheme [16]. CCQRE is calculated at different capacity levels.

Capacity	PSNR	SSIM	eq. (21)	eq. (22)	eq. (23)	eq. (24)
10.6	32.6	0.9987	55.2%	38.38%	72.0%	64.03%
12	32	0.9976	57.94%	41.0%	74.88%	64.29%
15.1	31.1	0.9854	63.87%	47.01%	80.73%	64.63%%
18.8	26.8	0.9806	70.38%	52.56%	88.2%	64.02%
CCQRE slope			1.85	1.73	1.97	0

the high-frequency region of the DCT. Table 12 shows the CCQRE calculations after testing with various capacity ratios and with using different cover images. It is clear from the table that the PSNR values decrease when increasing the hiding capacity ratios. However, the obtained CCQRE values were similar between high and low capacity tests. That is logical since the increase in the capacity ratios compensates the decrease in the PSNR values.

Table 11. set of data obtained after salt and pepper attack (density of 0.0001) for CF-LPAR scheme [16]. CCQRE is calculated using equation (25) at different capacity levels.

Capacity	$PSNR_s$	$PSNR_i$	$PSNR_d$	CCQRE equation (25)
10.6 bpp	32.6	65.1	6.4	28.84%
12 bpp	32	60.0	5.81	30.53%
15.1 bpp	31.1	37.4	5.9	36.56% %
18.8 bpp	26.8	31.4	5.7	41.07%

Table 12. Implementing the proposed CCQRE metric on a new steganography method. The $CCQRE^{1}_{0.5,0.5,0}$ equation used was the equation (22).

Secret image size	Cover image	Capacity	PSNR	CCQRE
64 x 64	F15Large	0.38	74.85	38.21%
	TigerFace	0.38	62.44	32%
	TigerPounce	0.38	80.28	40.92%
	Balloons	0.38	71.76	36.66%
	Zebras	0.38	59.27	30.42%
	Peppers	0.38	44.73	23.14%
128 x 128	F15Large	1.5	69.35	37.8%
	TigerFace	1.5	54.42	30.34%
	TigerPounce	1.5	71.25	38.75%
	Balloons	1.5	63.67	34.96%
	Zebras	1.5	51.15	28.7%
	Peppers	1.5	42.23	24.24%
256 x 256	F15Large	6	61	43%
	TigerFace	6	38.45	31.72%
	TigerPounce	6	50.9	37.95%
	Balloons	6	50.64	37.82%
	Zebras	6	37.21	31.1%
	Peppers	6	35.82	30.41%

5. CONCLUSIONS

This work has introduced a new performance measurement metric that will allow researchers to compare various steganography schemes even if they have differ-

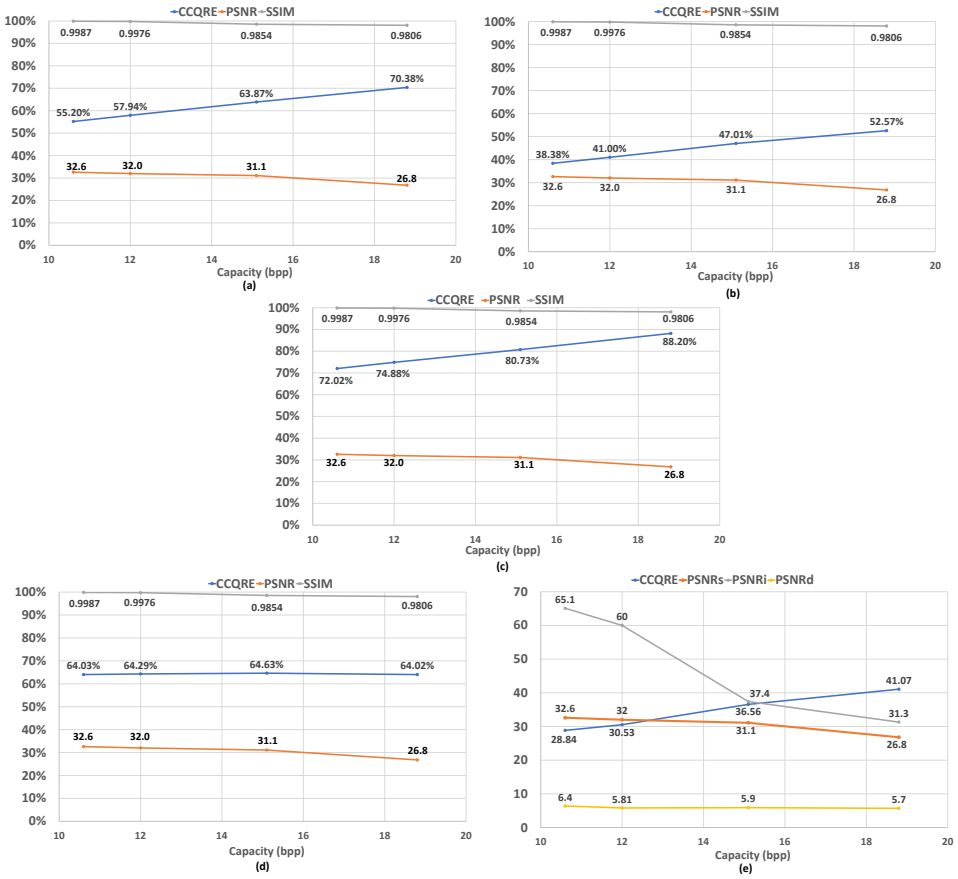

Fig. 9. The CCQRE slope is shown for the CF-LPAR scheme [16]. CCQRE was calculated using equation (21) in (a), equation (22) in (b), equation (23) in (c), equation (24) in (d) and equation (25) in (e). It is noticeable that the slope has a positive value in all cases. This is an indication that CF-LPAR hiding scheme is performing well with the capacity-imperceptibility trade-off.

ent range values for their attributes. The proposed "Combined Capacity-Quality-Robustness Effectiveness" (CCQRE) metric overcomes the tri-trade-off challenge formed by the three opposing steganography attributes; namely the capacity, imperceptibility, and robustness, by computing an efficiency percentage calculated by combining basis metric values of the three attributes using a parameter-controlled weighted average formulation. Comparative results have demonstrated the effectiveness of the proposed metric as a rational benchmarking tool for differing steganography schemes.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their valuable suggestions that contributed to the overall improvement of the original manuscript. This work was funded by the College of Graduate Studies & Research and by the Research Institute of Sciences & Engineering at the University of Sharjah.

References

1. T. Rabie and I. Kamel, Toward optimal embedding capacity for transform domain steganography: a quad-tree adaptive-region approach, *Multimedia Tools and Applications* **76**(6) (2017) 8627–8650.
2. L. Li, P. Cong, K. Cao, J. Zhou, T. Wei, M. Chen, S. Hu and X. S. Hu, Game theoretic feedback control for reliability enhancement of ethercat-based networked systems, *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* (2018).
3. J. Yang, J. Shen, P. Guo, B. Payne and T. Wei, A machine learning based forwarding algorithm over cognitive radios in wireless mesh networks, in *International Conference on Machine Learning and Intelligent Communications*, Springer2016, pp. 228–234.
4. C. K. Chan and L. Cheng, Hiding data in images by simple LSB substitution, *Pattern Recognition* **37** (2004) 469–474.
5. K. Solanki, N. Jacobsen, U. Madhow, B. S. Manjunath and S. Chandrasekaran, Robust image-adaptive data hiding using erasure and error correction, *IEEE Trans. Image Processing* **13**(December 2004) 1627–1639.
6. A. Jain, U. Uludag and R. Hsu, Hiding a face in a fingerprint image, in *Proc. of the International Conference on Pattern Recognition (ICPR)*, (Quebec City, Canada, 2002).
7. L. M. Marvel, J. Charles G. Boncelet and C. T. Retter, Spread spectrum image steganography, *IEEE Trans. Image Processing* **8**(August 1999) 1075–1083.
8. K. Nozaki, M. Niimi, R. O. Eason and E. Kawaguchi, A large capacity steganography using color bmp images, in *ACCV '98: Proceedings of the Third Asian Conference on Computer Vision-Volume I*, (Springer-Verlag, London, UK, 1998), pp. 112–119.
9. B. J. Mohd, T. Hayajneh, S. Abed and A. Itradat, Analysis and modeling of fpga implementations of spatial steganography methods, *Journal of Circuits, Systems, and Computers* **23**(02) (2014) p. 1450018.
10. B. Zaidan and A. Zaidan, Software and hardware fpga-based digital watermarking and steganography approaches: Toward new methodology for evaluation and benchmarking using multi-criteria decision-making techniques, *Journal of Circuits, Systems and Computers* **26**(07) (2017) p. 1750116.
11. G. Kasana, K. Singh and S. S. Bhatia, Block-based high capacity multilevel image steganography, *Journal of Circuits, Systems and Computers* **25**(08) (2016) p. 1650091.
12. T. Bonny and K. N. Salama, Abs: Sequence alignment by scanning, in *2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, Aug 2011, pp. 928–931.
13. T. Bonny and J. Henkel, Lict: Left-uncompressed instructions compression technique to improve the decoding performance of vliw processors, in *2009 46th ACM IEEE Design Automation Conference*, July 2009, pp. 903–906.
14. T. Bonny, M. A. Zidan and K. N. Salama, An adaptive hybrid multiprocessor technique for bioinformatics sequence alignment, in *2010 5th Cairo International Biomedical Engineering Conference*, Dec 2010, pp. 112–115.

15. T. Rabie, I. Kamel and M. Baziyad, Maximizing embedding capacity *and* stego quality: Curve-fitting in the transform domain, *Multimedia Tools and Applications* **77**(7) (2018) 8295–8326.
16. T. Rabie and M. Baziyad, Visual fidelity without sacrificing capacity: An adaptive laplacian pyramid approach to information hiding, *Journal of Electronic Imaging* **26**(6) (2017) p. doi: 10.1117/1.JEI.26.6.063001.
17. T. Rabie, M. Baziyad and I. Kamel, Enhanced high capacity image steganography using discrete wavelet transform and the laplacian pyramid, *Multimedia Tools and Applications* **77**(18) (2018) 23673–23698.
18. T. Rabie and I. Kamel, On the embedding limits of the discrete cosine transform, *Multimedia Tools and Applications* **75**(10) (2016) 5939–5957.
19. S.-C. Chu, H.-C. Huang, Y. Shi, S.-Y. Wu and C.-S. Shieh, Genetic watermarking for zerotree-based applications, *Circuits, Systems & Signal Processing* **27**(2) (2008) 171–182.
20. F. A. Petitcolas, R. J. Anderson and M. G. Kuhn, Information hiding-A survey, *Proceedings of the IEEE* **87**(7) (1999) 1062–1078.
21. T. Rabie and I. Kamel, High-capacity steganography: A global-adaptive-region discrete cosine transform approach, *Multimedia Tools and Applications* **76**(5) (2017) 6473–6493.
22. K. Cao, J. Zhou, T. Wei, M. Chen, S. Hu and K. Li, A survey of optimization techniques for thermal-aware 3D processors, *Journal of Systems Architecture* **https://doi.org/10.1016/j.sysarc.2019.01.003** (2019).
23. M. S. Subhedar and V. H. Mankar, Current status and key issues in image steganography: A survey, *Computer science review* **13** (2014) 95–113.
24. K. Sayood *et al.*, Statistical evaluation of image quality measures, *Journal of Electronic imaging* **11**(2) (2002) 206–223.
25. Z. Wang and A. C. Bovik, Mean squared error: love it or leave it? a new look at signal fidelity measures, *Signal Processing Magazine, IEEE* **26**(1) (2009) 98–117.
26. T. Chai and R. R. Draxler, Root mean square error (rmse) or mean absolute error (mae)?–arguments against avoiding rmse in the literature, *Geoscientific Model Development* **7**(3) (2014) 1247–1250.
27. C.-C. Chang, T.-S. Chen and L.-Z. Chung, A steganographic method based upon jpeg and quantization table modification, *Information Sciences* **141**(1) (2002) 123–138.
28. G. Pavlidis, A. Tsompanopoulos, N. Papamarkos and C. Chamzas, Jpeg2000 over noisy communication channels thorough evaluation and cost analysis, *Signal Processing: Image Communication* **18**(6) (2003) 497–514.
29. Z. Wang, A. C. Bovik, H. R. Sheikh and E. P. Simoncelli, Image quality assessment: from error visibility to structural similarity, *Image Processing, IEEE Transactions on* **13**(4) (2004) 600–612.
30. I. Avcibas, N. Memon and B. Sankur, Steganalysis using image quality metrics, *IEEE transactions on Image Processing* **12**(2) (2003) 221–229.
31. R. Román-Roldán, J. F. Gómez-Lopera, C. Atae-Allah, J. Martınez-Aroza and P. L. Luque-Escamilla, A measure of quality for evaluating methods of segmentation and edge detection, *Pattern recognition* **34**(5) (2001) 969–980.
32. W. K. Pratt, Digital image processing, *Wiley-Interscience* (1991).
33. T. Rabie, Frequency-domain data hiding based on the matryoshka principle, *Special Issue on Advances in Video Processing and Security Analysis for Multimedia Communications, International Journal of Advanced Media and Communication* **1**(3) (2007) 298–312.
34. T. Rabie, High-capacity steganography, in *6th International Congress on Image and*

Signal Processing (CISP), **2**2013, pp. 858–863.
35. P.-Y. Lin and C.-S. Chan, Invertible secret image sharing with steganography, *Pattern Recognition Letters* **31**(13) (2010) 1887–1893.
36. M. Padmaa and Y. Venkataramani, Zig-zag pvd–a nontraditional approach, *International Journal of Computer Applications* **5**(7) (2010) 5–10.
37. S. Bhattacharyya and G. Sanyal, A robust image steganography using dwt difference modulation (dwtdm), *International Journal of Computer Network and Information Security* **4**(7) (2012) p. 27.
38. M. Ghebleh and A. Kanso, A robust chaotic algorithm for digital image steganography, *Communications in Nonlinear Science and Numerical Simulation* **19**(6) (2014) 1898–1907.
39. C. Balasubramanian, S. Selvakumar and S. Geetha, High payload image steganography with reduced distortion using octonary pixel pairing scheme, *Multimedia tools and applications* **73**(3) (2014) 2223–2245.
40. C. Qin, C.-C. Chang and C.-C. Lin, An adaptive reversible steganographic scheme based on the just noticeable distortion, *Multimedia Tools and Applications* **74**(6) (2015) 1983–1995.
41. P. W. Adi, F. Z. Rahmanti and N. A. Abu, High quality image steganography on integer haar wavelet transform using modulus function, in *Science in Information Technology (ICSITech), 2015 International Conference on*, IEEE2015, pp. 79–84.
42. H.-T. Wu, J.-L. Dugelay and Y.-Q. Shi, Reversible image data hiding with contrast enhancement, *IEEE signal processing letters* **22**(1) (2015) 81–85.
43. G. Gao and Y.-Q. Shi, Reversible data hiding using controlled contrast enhancement and integer wavelet transform, *IEEE Signal Processing Letters* **22**(11) (2015) 2078–2082.
44. A. K. Al-Dhamari and K. A. Darabkh, Block-based steganographic algorithm using modulus function and pixel-value differencing, *Journal of Software Engineering and Applications* **10**(01) (2017) p. 56.
45. C. Kocak, Clsm: Couple layered security model a high-capacity data hiding scheme using with steganography, *Image Analysis & Stereology* **36**(1) (2017) 15–23.