International Journal of the Physical Sciences Vol. 5(7), pp. 1054-1062, August, 2010
Available online at http://www.academicjournals.org/IJPS
ISSN 1992 - 1950 ©2010 Academic Journals

*Full Length Research Paper*

# On the accuracy of hiding information metrics: Counterfeit protection for education and important certificates

**Ali K. Hmood[1], Z. M. Kasirun[1], Hamid A. Jalab[1], Gazi Mahabubul Alam[3]*
A. A. Zaidan[2] and B. B. Zaidan[2]**

[1]Faculty of Computer Science and Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia.
[2]Faculty of Engineering, Multimedia University, 63100 Cyberjaya, Selangor Darul Ehsan, Malaysia.
[3]Faculty of Education, University of Malaya, Kuala Lumpur, Malaysia.

Accepted 13 July, 2010

**There are two techniques used to hide information - one is steganography while the other is digital watermarking. The objective of this paper is to investigate the functionality and reliability of using the current metrics, which are used to measure the distortion caused by secret data embedding. These metrics are used to measure the quality of the steganographic or watermarked objects. The signal-to-noise ratio, peak signal-to-noise ratio, mean square error, root mean square error, histogram and human vision test are the current measurements for the steganographic object. The paper will also discuss the widely used metrics and their limitations. Apart from this, it will also look at how researchers have criticized the metrics and how these metrics are used to measure the quality of steganographic or watermarked objects.**

**Key words:** Steganography, digital watermarking, SNR, PSNR, MSE, RMSE, histogram, human vision, quality metrics.

## INTRODUCTION

Everyday thousands of multimedia files being uploaded and multi-thousands downloaded, all this make the use of the copyrights sign important to protect the intellectual property for the authors of these files. The high speed internet backbone has become ever-present and high speed modems have become the standard entry-level internet connection. Powerful images compression algorithms such as JPEG, and internet browser that are able to upload, download and view high-resolution images are currently in general use on the internet. Since that, more and more images appear in the physical and digital world around us (Alattar, 2000). With all this powerful technologies, unauthorised copies of digital images are very easy to make and store. Hence, early research efforts in digital watermark technique focused on water marking as a technique to communicate and enforce copyrights, detect counterfeit copies and deter improper use of digital media, in general and digital images, in particular.

During the past few years, the United States economy has performed beyond most expectations. A shrinking budget deficit, low interest rates, a stable macroeconomic environment, expanding international trade with fewer barriers and effective private sector management are all credited with playing a role in this healthy economic performance.

One of the strategies of the record companies to counter the decline of revenues was to fight unauthorized music copies. The actions taken against unauthorized music copying as well as their outcome during the years 2000 - 2004 are described. The multimedia files copyrights and copyright infringement can be one of the following forms:

i. Text: The unauthorized use of text content can be a form of copyright infringement. It is common on the World Wide Web for text to be copied from one site to another without consent of the author.

*Corresponding author. E-mail: gazi.alam@um.edu.my, gazimalamb@yahoo.com. Tel: + 603-7967 5077. Fax: + 603-7967 5010.

ii. Music or Videos: Duplication of a CD or other recorded media containing copyright material without permission of the copyright holder may be a form of copyright infringement, dependent on local laws. Unauthorized downloading of copyrighted material and sharing of recorded music or videos over the Internet, often in the form of MP3 files or RMVB files, is another form of infringement (Putter, 2006; Edström-Frejman, 2007; Becker and Buhse, 2009).
iii. Image: The unauthorized distribution, use, altering or transferring of images is one form of copyrights infringement for the images. The images consider as the most widely used form of multimedia files on the internet for every purpose the image is the best way to describe it (Caronni, 1995; Jensen, 2003).

Since the privacy, copyright and security are very important issues (Hashim et al., 2010). It is important to develop systems for copyright protection, protection against duplication and authentication of content. Watermarking seems to be the alternative solution for reinforcing the security of multimedia documents. The aim of watermarking is to include subliminal information (that is, imperceptible) in a multimedia document to ensure a security service or simply a labelling application. It would be then possible to recover the embedded message at any time, even if the document was altered by one or more non-destructive attacks, whether malicious or not. It is a well-known saying that an image is worth a thousand words. Images tend to have more impact on people than text, as it is easier to disregard the content of textual information than to question the origin and authenticity of a photograph. It used to be stated that the camera could not lie. However, it is now possible to edit pictures easily and at very little cost. The resulting images can have such a high quality that they appear to be genuine.

The hiding of information technique, which aims to transfer information secretly and to establish a hidden relationship between the message and its counterpart, has long been of a great interest to researchers. Methods of hiding information are mostly applied to images (Hmood et al., 2010), audio (Zaidan et al., 2010), video (Al-Frajat et al., 2010) and text (Zaidan et al., 2010) files. The steganography techniques use code fields of unimportant bits in digital multimedia files as potential areas to hide encoded messages or images (Cheddad et al., 2009). While such manipulation might slightly alter the quality of the original image, it generally goes unnoticed by the naked eye. The main goal of steganography is to hide a message μ in multimedia (cover) data β, to obtain new data α, in such a way that an attacker cannot detect the presence of μ in α. The main goal of watermarking is to hide the message μ in some multimedia (cover) data β, to obtain new data α, in such a way that an attacker cannot remove or replace μ in α. It is also often said that the goal of steganography is to hide a message in one-to-one communication and the goal of watermarking is to hide a message in one-to-many communications. Meanwhile, there is no standard or automated tools to measure the the quality of steganographic object after embedding the secret message. Due to the large number of steganography and watermarking approaches being developed, the most commonly used tools in ensuring the quality of steganography approaches are peak signal-to-noise ratio (PSNR) (Seng et al., 2009), signal-to-noise ratio (SNR) (Fridrich et al., 2005), histogram (Zaidan et al., 2009), mean square error (MSE) (Abraham et al., 2004), root mean square error (RMSE) (Wu and Tsai, 2003) and human vision T (Zaidan et al., 2009). Nevertheless, there is no standard metric for measuring the quality of steganographic objects.

## RESEARCH QUESTIONS

In the area of copy right, steganography, and digital watermarking; there are hundreds if not thousands research papers developed new approaches; most of these papers have used SNR, PSNR, MSE or RMSE as a metrics to measure the acceptance of these approaches. Regarding to them, the success factor of the algorithm depend on the result of these metrics, however, non of these research's reported, these metrics are not suitable for data hidden applications. Unlike the literatures, this research has been created to provide the answers for the following questions:

i. Is the hiding information technique important?
ii. What are the SNR, PSNR, MSE and RMSE?
iii. Are the current metrics for hiding information technique reliable?
iv. How accurate are the results of these metrics?
v. Are the SNR, PSNR, MSE and RMSE the only metrics used for hiding information technique?

### State of the art

The metrics used for the quality of the steganographic object are the main metric to measure the distortion level in the steganographic object. The metric should show the possibility of any alteration to the perceptual layout of the image or the video, while the used metrics in the literature have a number of limitations, such as, the most commonly used full-reference objective image and video distortion/ quality metrics which are the mean squared error (MSE) and the peak signal-to-noise ratio (PSNR). MSE and PSNR are widely used because they are simple to calculate, have clear physical meanings, and are mathematically easy to deal with for optimization purposes. Regardless of (Kanvel and Monie, 2009) where the author mentioned that the peak signal-to-noise ratio (PSNR) and root mean square error (RMSE) offer a more objective way to compare various algorithms' performance. However, the metrics have been widely criticised as well for not correlating well with perceived quality measurement (Girod, 1993; Teo and Heeger, 1994; Eskicioglu and Fisher, 1995; Wang, 2001; Wang and Bovik, 2002; Bovik et al., 2002; Wang et al., 2002; Wang et al., 2003; Wang et al., 2004; Lee et al., 2006). MSE is not a good measure to evaluate the quality of a given image, this conclusion appeared in (Hellier et al., 2001; Van der Weken et al., 2004). Additionally, (Wang et al., 2002) mentioned that the MSE is extremely poor in the sense that images with nearly identical MSE are sometimes drastically different in perceived quality.

The SNR has been found in the literature to be considered, as it is not the sole factor determining overall image quality in (Kaufman et al., 1989; Rubin and Kneeland, 1994), while SNR is not an effective measure of coding quality appeared in (Lengyel, 1999).

The most widely used metric is the PSNR received many criticism such as, PSNR is not always a good indication of the visual quality argued by (Zlokolica et al., 2003; Kimmel, 1998; Kimmel, 1999; Muresan and Parks, 2002; Yuan et al., 2003) and the PSNR is not a perfect measure of image quality by (Hamzaoui et al. 2000; Ebrahimi et al., 2004), additionally, the PSNR is not a suitable metric for video quality mentioned by (Nemethova et al., 2004), while (Wang et al., 2002) reported that the PSNR is not an appropriate approach and (Wang et al., 2002) mentioned PSNR is not well correlated with perceived noise.

The Root Mean Square Error (RMSE) is not a true or reliable for measuring the image quality as mentioned by (Armstrong and Collopy, 1992; Willmott and Matsuura, 2005) and the RMSE is not an adequate measure of image quality appeared in (Christopoulos et al., 1998) while the use of RMSE is not sufficient for measuring the quality of the image appeared in (Rushmeier et al., 1995; Gaddipatti et al., 1997; McNamara et al., 2001).

Before starting the literature survey, the authors would like to first present how the quality of steganographic object has been measured, the name of each metric used for measurement and the way the metric would measure the quality of steganographic objects.

Firstly, a sample image will be presented in order to understand the way the metrics are used to measure the quality of steganographic objects, where the two images are represented in Figure 1.

The most widely used measurements are comprised of two main types - one is the subjective measurement while the other is the objective measurement. These metrics use the original object as a reference to compare it with the steganographic object.

### Subjective measures

Subjective evaluation by viewers is still a method commonly used in measuring image quality. The subjective test emphatically examines fidelity, while at the same time considers image intelligibility. When taking a subjective test, a viewer focuses on the difference between the reconstructed image and the original image, he or she can notice such details where information loss cannot be accepted. The representative subjective method is mean opinion score (MOS) (Lee et al., 1992; Cosman et al., 1994; Eskicioglu and Fisher, 1995; Ghrare et al., 2008).

The human vision test is the first type of measurement that has been found to measure the quality of steganographic objects after embedding the hidden data. This type of measurement is based on a survey, usually of 10 - 15 persons who have examined the image or the video before and after the embedding of the hidden data. They are then asked if they had found any alterations in the perceptual vision of the image or video. This, however, is not a reliable measurement.

### Objective measures

A widely used measurement for reconstructed images for an *n x m* size image is the histogram. The histogram can tell you whether or not your image has been properly exposed, whether the lighting is harsh or flat, what adjustments will work best and whether or not there are any changes to the colours. The histogram works by examining the repetition of each colour in the image, where each pixel in an image has a colour, which has been produced by the combination of the primary colours red, green and blue (RGB). Each of these colours can have a brightness value, ranging from 0 to 255, for a digital image with a bit depth of 8 bits. An RGB histogram demonstrates results when the computer scans through each of these RGB brightness values and counts how many are bins/colours at each level, from 0 through 255.

The histogram is represented by a bar chart for each image (original image and the stego-image), where each bar represents the repetition of the colour in the image. The signal-to-noise ratio (SNR) is used to quantify how much a signal has been corrupted by noise. The SNR works by comparing the level of a desired signal to the level of background noise. The higher SNR ratio means the less obtrusive the background noise. After getting the level of the noise in each image (the original and the stego-image), the SNR compares the level of noise in both images and shows the differences between the two images in order to know the quality of the stego-image after embedding the hidden data.

The SNR is represented by the following equation:

$$SNR = 10 * Log_{10} \frac{\sum_{i=1}^{n}\sum_{j=1}^{m}\left(A_{ij}\right)^2}{\sum_{i=1}^{n}\sum_{j=1}^{m}\left(A_{ij} - B_{ij}\right)^2}$$

Where: $A_{ij}$ represent one pixel in the original image

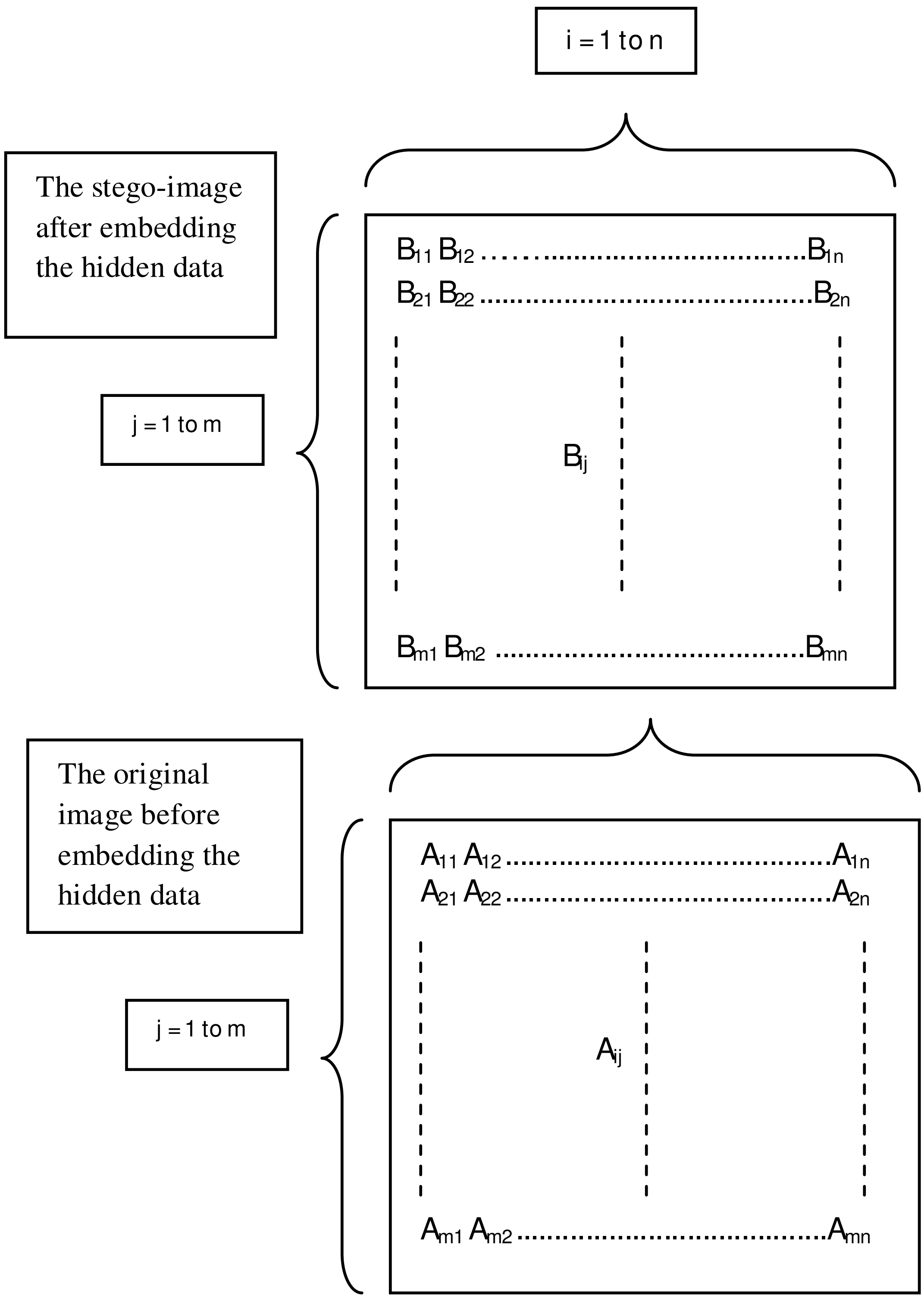


**Figure 1.** Image representation.

(before embedding the hidden data) and $B_{ij}$ represent one pixel in the stego-image (after embedding the hidden data). The final result will be presented by a constant and the measuring unit is decibel (dB). The mean square error (MSE) represents the cumulative squared error between the original image and the stego-image. A lower value of MSE means a lower error between the two images. The MSE measurement fo the steganographic objects is represented by the following equation:

$$MSE = \frac{1}{m*n}\sum_{i=0}^{m}\sum_{j=0}^{n}(A_{ij} - B_{ij})^2$$

Where: $A_{ij}$ represent one pixel in the original image (before embedding the hidden data), $B_{ij}$ represent one pixel in the stego-image (after embedding the hidden data) and M*N represent the height and width of the image. The result of the MSE is represented by a constant and the measuring unit is dB.

The peak signal-to-noise ratio (PSNR) is the metric which computes the peak signal-to-noise ratio, in decibels, between two images. This ratio is often used as a quality measurement between the original image and its compressed version. The higher PSNR is the better quality of the compressed or reconstructed image. It is normally used in steganography to measure the peak signal-to-noise ratio in the original image and the stego-image after embedding the hidden data.

The PSNR is represented by the following equation:

$$PSNR = 10*\log_{10}\frac{(Max)^2}{\frac{1}{m*n}\sum_{i=0}^{m}\sum_{j=0}^{n}(A_{ij} - B_{ij})^2}$$

Or in the other representation for the PSNR:

$$PSNR = 10*\log_{10}\frac{(Max)^2}{MSE}$$

Where: $A_{ij}$ represent one pixel in the original image (before embedding the hidden data), $B_{ij}$ represent one pixel in the stego-image (after embedding the hidden data), M*N represent the height and width of the image and MAX represent the maximum value of the colours which is 255. The result of the PSNR is represented by a number and the measuring unit is dB. Note that the image and video processing community has long been using the mean squared error (MSE) and the peak signal-to-noise ratio (PSNR) as fidelity metrics (mathematically, the PSNR is just a logarithmic representation of the MSE). There are a number of reasons for the popularity of these two metrics. The formulas for computing them are simple to understand and implement as they are easy and fast to compute. Minimizing the MSE is also very well understood from a mathematical point of view. Over the years, video researchers have developed familiarity with the PSNR which allows them to interpret the values immediately. However, the usage of these two metrics is still not considered the best measurement types to determine the quality of steganographic objects.

The root mean square error (RMSE) is the square root of the average squared difference between every pixel in the distorted image and its counterpart in the original image. A low value of RMSE means a lower distortion.

The RMSE is represented by the following equation:

$$RMSE = \sqrt{\frac{1}{m*n}\sum_{i=0}^{m}\sum_{j=0}^{n}(A_{ij} - B_{ij})^2}$$

Where: $A_{ij}$ represent one pixel in the original image (before embedding the hidden data), $B_{ij}$ represent one pixel in the stego-image (after embedding the hidden data), M*N represent the height and width of the image. The result of the RMSE is represented by a number and the measuring unit is dB. After this brief introduction, we shall examine these metrics now. In the following part, as shown in Table 1, the authors show the different papers that used (mostly) one, two or maximum three metrics and the quality of the stego-object for the proposed method in each paper.

### The current measurements' drawback

Objective measurement plays an important role in the development, optimization, and assessment of image, video and audio coding systems. It is also very useful for the design and evaluation of the post-processing algorithms at the decoding side. In the literature, most of the papers have simply used the MSE, RMSE, SNR and PSNR in the objective tests of Steganography. The mean squared error (MSE) is used as the distortion measure. Since the MSE is not good for image quality assessment (Girod, 1993; Wang et al., 2000), the assessment of an image can be carried out by comparing it with a reference image, which is assumed to be perfect for a particular application. Usually, such comparison is implemented on pixel-based operations, like the mean square error (MSE) or root mean square error (RMSE).

However, such operations' performance is questionable because the same MSE or RMSE value does not always assure a comparable image similarity under different distortion to perceptually significant features. The RMSE and PSNR are also known to not always faithfully represent visual quality (Liu and Laganière, 2007). One potential limitation in the use of the RMSE and/or image discrimination/ perceptual differences models in the current context is that it is unclear how predicting an observer's ability to discriminate between an original image and its degraded version relates to performance detecting a low contrast signal within the image (Eckstein et al., 1981). The MSE is not a good measure to evaluate quality measurements (Hellier et al., 2001), as it is extremely poor, in the sense that images with nearly identical MSEs are drastically different in perceived quality (Wang et al., 2002). Currently, the most commonly used full-reference (FR) objective image and video distortion / quality metrics are the MSE and PSNR

**Table 1.** The use of steganography metrics.

| Number | Paper | Human vision test | Histogram | SNR | PSNR | MSE | RMSE |
|---|---|---|---|---|---|---|---|
| 1 | Hossain et al., 2010 | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ |
| 2 | Seng et al., 2009 | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ |
| 3 | Eltahir et al., 2009 | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| 4 | Zaidan et al., 2009 | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| 5 | Zaidan et al., 2009 | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ |
| 6 | Naji et al., 2009 | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| 7 | Wang et al., 2008 | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ |
| 8 | Lee et al., 2008 | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ |
| 9 | Kim et al., 2007 | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| 10 | Aabed et al., 2007 | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| 11 | Gutub and Fattani, 2007 | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| 12 | Ker, 2007 | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| 13 | Solanki et al., 2006 | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| 14 | Kumar and Rajpal, 2006 | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ |
| 15 | Zhang and Wang, 2006 | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| 16 | Noda et al., 2006 | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ |
| 17 | Wang, 2005 | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ |
| 18 | Holotyak et al., 2005 | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ |
| 19 | Potdar et al., 2005 | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| 20 | Fridrich et al., 2005 | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| 21 | Brisbane et al., 2005 | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ |
| 22 | Kharrazi et al., 2004 | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| 23 | Venkatraman et al., 2004 | ✗ | ✗ | ✓ | ✓ | ✓ | ✗ |
| 24 | Noda et al., 2004 | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ |
| 25 | Franz and Schneidewind, 2004 | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| 26 | Lin and Tsai, 2004 | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ |
| 27 | Wang and Wang, 2004 | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| 28 | Chang and Tseng, 2004 | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ |
| 29 | Wu and Tsai, 2003 | ✗ | ✗ | ✗ | ✓ | ✗ | ✓ |
| 30 | Su and Kuo, 2003 | ✗ | ✗ | ✗ | ✓ | ✓ | ✗ |
| 31 | Fu and Au, 2003 | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ |
| 32 | Chang et al., 2002 | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ |
| 33 | Aspert et al., 2002 | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ |
| 34 | Niimi et al., 2002 | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ |
| 35 | Robie and Mersereau, 2002 | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ |
| 36 | Noda et al., 2002 | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ |
| 37 | Noda et al., 2002 | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ |
| 38 | Retter, 2000 | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ |
| 39 | Moskowitz et al., 2000 | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| 40 | Areepongsa et al., 2000 | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ |
| 41 | Marvel et al., 1999 | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ |
| 42 | Hrytskiv et al., 1998 | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Frequency | | 2/42 | 12/42 | 3/42 | 20/42 | 3/42 | 2/42 |

because they are simple to calculate, have clear physical meanings and are mathematically easy to deal with for optimization purposes. However, they have also been widely criticised for not correlating well with perceived quality measurement (Girod, 1993; Teo and Heeger, 1994; Eskicioglu and Fisher, 1995; Wang, 2001; Wang and Bovik, 2002; Wang et al., 2002; Wang et al., 2002; Wang et al., 2003; Wang et al., 2004; Lee et al., 2006). The SNR is not the sole factor in determining the overall image quality (Kaufman et al., 1989; Rubin and Kneeland, 1994), and it is not an effective measure of coding quality (Lengyel, 1999). However, we realize that

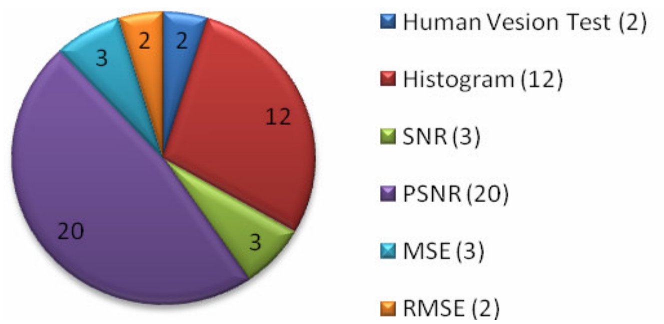


**Figure 2.** Frequency of use.

the PSNR is not always a good indication of the visual quality, so we also judge the visual quality (Zlokolica et al., 2003). Thus, an increase of the PSNR may not necessarily be accompanied by an improvement in perceived image quality (Hamzaoui et al., 2000). The PSNR is not a good image quality indicator for high compression ratios (Ebrahimi et al., 2004), it can be concluded once again that the PSNR is not a suitable metric for video quality (Nemethova et al., 2004) and the PSNR is not an appropriate approach (Wang et al., 2002). It is also not well correlated with perceived noise (Winkler et al., 2003).

Although it is well known that PSNR is not a good measure of perceptual quality (Yuan et al., 2003), we know that the PSNR is popularly used as a metric in video or image processing. However, in order to allow the video object to move smoothly instead of precisely predicting the object location in non-coded frames of the original sequence. The PSNR is not a good metric to determine the visual performance of frame interpolation (Kuo et al., 1999). The Root Mean Square Error (RMSE) is not a true or reliable measure (Armstrong and Collopy, 1992; Willmott and Matsuura, 2005) as it does not measure the image quality adequately (Christopoulos et al., 1998) and the use of RMSE is not sufficient (Rushmeier, 1995; Gaddipatti et al., 1997; McNamara et al., 2001).

Figure 2 depicted the frequency of use the metrics. Within the papers, which have been shown above, the measurement for the quality of steganographic objects after embedding the hidden data is insufficient to satisfy the aim of the steganography (Zlokolica et al., 2003). Nevertheless, the current metrics are still used in measuring the steganographic and watermarked objects (Zaidan et al., 2009).

The metrics used for the quality of the steganographic object in the literature survey are the main metrics to measure the distortion level of the steganographic object. The metric should show the possibility of any altering to the perceptual layout of the image or the video after embedding the secret message. The researchers reported in the survey have relied on these metrics in order to approve their methods, or compared the PSNR, SNR MSE, RMSE of their new methods' to approve that their methods is much better than others (Wang et al., 2008) while as we have shown these metrics are not reliable for such kind of application. However, these metrics need enhancement to be reliable for steganography and digital watermark systems.

## CONCLUSION

Since the main aim of the steganography is to send secure messages within an insecure channel, the steganographic object should use a reliable measurement to ensure that the steganography approach is functional. In this paper, we have discussed the ways that the steganographic metrics are used to measure the quality of steganographic or watermarked objects. In addition, the steganographic metrics are unable to give the exact result on the amount of distortion being added to the steganographic objects as approved by a number of researchers. In the review, we have shown the papers, which had proposed or criticized the limitations of the steganographic metrics. A further extension to this work can be done by enhancing the steganography and digital watermark measurements. The measurement should be accurate in showing the amount of distortion being added to the steganographic objects after embedding the secure message in order to enhance the security level against any suspicion to the steganographic image.

## ACKNOWLEDGMENTS

This research has been funded by the University of Malaya, under the grant number (P0033/2010A). The author would like to express his heartfelt thanks to Dr.Abbas Chedad and Prof. David Ngo for their invaluable comments on this paper.

### REFERENCES

Aabed MA, Awaideh SM, Elshafei ARM, Gutub AA (2007). Arabic Diacritics Based Steganography. IEEE International Conference on

Signal Processing and Communications (ICSPC 2007). Dubai, UAE: pp. 24-27.
Al-Frajat AK, Jalab HA, Kasirun ZM, Zaidan AA, Zaidan BB (2010). "Hiding Data in Video File: An Overview." J. Appl. Sci., 10(15): 1644-1649.
Alattar A (2000). Smart Images' using Digimarc's watermarking technology.
Ali KH, Hamid AJ, Kasirun ZM, Zaidan AA, Zaidan BB (2010). "On the Capacity and Security of Steganography Approaches: An Overview." J. Appl. Sci., 10(16): 1825-1833.
Areepongsa S, Syed YF, Kaewkamnerd N, Rao KR (2000). Steganography for a low bit-rate wavelet based image coder. International Conference on Image Processing 2000. Vancouver, BC, Canada, IEEE Computer Society, 1: 597-600.
Armstrong J, Collopy F (1992). "Error measures for generalizing about forecasting methods: Empirical comparisons." Int. J. Forecasting, 8(1): 69-80.
Aspert N, Drelie E, Maret Y, Ebrahimi T (2002). Steganography for Three-Dimensional Polygonal Meshes. Proceedings of the SPIE 47th annual meeting, Seattle, Applications of Digital Image Processing.
BECKER E, BUHSE W (2009). "Digital rights management: technological, economic, legal and political aspects (lecture notes in computer science vol. 2770)." européen des systèmes automatisés 43.
Brisbane G, Safavi-Naini R, Ogunbona P (2005). "High-capacity steganography using a shared colour palette." IEE proceedings. Vision, Image And Signal Processing, 152: 787-792.
Caronni G (1995). Assuring ownership rights for digital images, Citeseer.
Chang CC, Chen TS, Chung LZ (2002). "A steganographic method based upon JPEG and quantization table modification." Information Sci., 141(1-2): 123-138.
Chang CC, Tseng HW (2004). "steganographic method for digital images using side match." Pattern Recognition Lett., 25(12): 1431-1437.
Cheddad A, Condell J, Curran K, Mc Kevitt P (2009). "A skin tone detection algorithm for an adaptive approach to steganography." Signal Processing, 89(12): 2465-2478.
Christopoulos C, Philips W, Skodras A, Cornelis J (1998). "Segmented image coding: Techniques and experimental results." Signal Processing-Image Commun., 11(1): 63-80.
Cosman P, Gray R, Olshen R (1994). "Evaluating quality of compressed medical images: SNR, subjective rating, and diagnostic accuracy." Proceedings IEEE, 82(6): 919-932.
Ebrahimi F, Chamik M, Winkler S (2004). JPEG vs. JPEG2000: An objective comparison of image encoding quality, Citeseer.
Eckstein M, Bartroff J, Abbey C, Whiting J, Bochud F (2003). "Automated computer evaluation and optimization of image compression of x-ray coronary angiograms for signal known exactly detection tasks." Optics Express, 11(5): 460-475.
Edström-Frejman A (2007). "eCommerce rhetoric and reality in the music industry: estimating the real impact of file-sharing activities on CD-sales."
Eltahir ME, Kiah MLM, Zaidan BB, Zaidan AA (2009). High Rate Video Streaming Steganography. Proceedings of the 2009 International Conference on Future Computer and Communication, Kuala Lumpur, Malaysia, IEEE Computer Society.
Eskicioglu A, Fisher P (1995). "Image quality measures and their performance." IEEE Trans. Commun., 43(12): 2959-2965.
Franz E, Schneidewind A (2004). Adaptive Steganography Based on Dithering. Proceedings of the 2004 workshop on Multimedia and security, Magdeburg, Germany ACM.
Fridrich J, Goljan M, Soukal D (2005). "Perturbed quantization steganography." Multimedia Syst., 11(2): 98-107.
Fu MS, Au OC (2003). "Steganography in halftone images: conjugate error diffusion." Signal Processing, 83(10): 2171-2178.
Gaddipatti A, Machiraju R, Yagel R (1997). Steering image generation with wavelet based perceptual metric, Blackwell Publishing.
Ghrare S, Ali M, Ismail M, Jumari K (2008). Diagnostic Quality of Compressed Medical Images: Objective and Subjective Evaluation, IEEE Computer Society.
Girod B (1993). What's wrong with mean-squared error?, MIT Press.
Girod B (1993). What's wrong with mean-squared error? Digital images and human vision, MIT Press: pp. 207-220.
Gutub AAA, Fattani MM (2007). "A Novel Arabic Text Steganography Method Using Letter Points and Extensions." World Acad. Sci. Eng. Technol., 27: 28-32.
Hamzaoui R, Hartenstein H, Saupe D (2000). "Local iterative improvement of fractal image codes." Image Vision Comput. 18(6-7): 565-568.
Hashim F, Alam GM, Siraj S (2010). "Information and communication technology for participatory based decision-making-E-management for administrative efficiency in Higher Education." Int. J. Phys. Sci., 5(4): 383-392.
Hellier P, Barillot C, Corouge I, Gibaud B, Le Goualher G, Collins L, Evans A, Malandain G, Ayache N (2001). Retrospective evaluation of inter-subject brain registration, Springer.
Holotyak T, Fridrich J, Soukal D (2005). Stochastic Approach to Secret Message Length Estimation in ±k Embedding Steganography. Security, Steganography, and Watermarking of Multimedia Contents VII. Delp, E. J. and Wong, P. W. San Jose, California, USA, SPIE, 5681: 673-684.
Hossain M, Al Haque S, Sharmin F (2010). "Variable Rate Steganography in Gray Scale Digital Images Using Neighborhood Pixel Information." The Int. Arab J. Info. Technol., 7(1): 34-38.
Hrytskiv Z, Voloshynovskiy S, Rytsar Y (1998). "cryptography and steganography of video information in modern communications." series: Electronics Energetics, 22(3): 115-125.
Jensen A (2003). "Copy Protection of CDs: The Recording Industry's Latest Attempt at Preventing the Unauthorized Digital Distribution of Music." J. Marshall J. Comput. Info. l. 21: 241-591.
Kanvel N, Monie EC (2009). "Adaptive lifting based image compression scheme for narrow band transmission system." Int. J. Phys. Sci., 4(4): 194-164.
Kaufman L, Kramer D, Crooks L, Ortendahl D (1989). "Measuring signal-to-noise ratios in MR imaging." Radiology, 173(1): 265.
Ker AD (2007). Batch Steganography and Pooled Steganalysis. Information Hiding. Berlin / Heidelberg, Springer. 4437/2007: 265-281.
Kharrazi M, Sencar HT, Memon N (2004). "Image Steganography: Concepts and Practice." WSPC/Lecture Notes Series , Institute for Mathematical Sciences, National University of Singapore, Singapore, Republic of Singapore.
Kim Y, Duric Z, Richards D (2007). Modified Matrix Encoding Technique for Minimal Distortion Steganography. VA, USA, Springer Berlin / Heidelberg, 4437: 314-327.
Kimmel R (1998). "Demosaicing: image reconstruction from color CCD samples." Computer Vision—ECCV'98: 610.
Kimmel R (1999). "Demosaicing: Image Reconstruction from Color CCD Samples." IEEE Trans. Image Processing, 8(9): 1221-1228.
Kumar A, Rajpal N (2006). "Application of T-Code, Turbo Codes and Pseudo-Random Sequence for Steganography." J. Comput. Sci., 2(2): 148-153.
Kuo T, Kim J, Kuo C (1999). Motion-compensated frame interpolation scheme for H. 263 codec, Citeseer.
Lee CC, Hsien-ChuWu TCS, Chu YP (2008). "Adaptive lossless steganographic scheme with centralized difference expansion." the j. Patt. Recognition Society, 41(6): 2097-2106.
Lee C, Cho S, Choe J, Jeong T, Ahn W, Lee E (2006). "Objective video quality assessment." Optical Eng., 45: 017004.
Lee H, Rowberg A, Frank M, Choi H, Kim Y (1992). Subjective evaluation of compressed image quality.
Lengyel, J. (1999). Compression of time-dependent geometry, ACM.
Lin CC, Tsai WH (2004). "Secret image sharing with steganography and authentication." J. Syst. Software, 73(3): 405-414.
Liu Z, Laganière R (2007). "Phase congruence measurement for image similarity assessment." Pattern Recognition Lett., 28(1): 166-172.
Marvel LM, Boncelet CG Jr., Retter CT (1999). "Spread spectrum image steganography." Image Processing, IEEE Trans., 8(8): 1075-1083.
McNamara A, Chalmers A, Trocianko T (2001). Visual perception in realistic image synthesis.
Moskowitz IS, Longdon GE, Chang L (2000). A new paradigm hidden in steganography. Proceedings of the 2000 workshop on New security paradigms, Ballycotton, County Cork, Ireland ACM New York, NY,

USA.
Muresan D, Parks T (2002). "Optimal recovery demosaicing." IASTED Signal and Image Processing.
Naji AW, Gunawan TS, Hameed SA, Zaidan BB, Zaidan AA (2009). "Stego-Analysis Chain, Session Two" Novel Approach of Stego-Analysis System for Image File. International Association of Computer Science and Information Technology - Spring Conference. Singapore: pp. 410-414.
Nemethova O, Ries M, Siffel E, Rupp M (2004). Quality assessment for H. 264 coded low-rate and low-resolution video sequences, Citeseer.
Niimi M, Noda H, Kawaguchi E, Eason RO (2002). High capacity and secure digital steganography to palette-based images. Proceedings. 2002 International Conference on Image Processing.
NODA H, FURUTA T, NIIMI M, KAWAGUCHI E (2004). Application of BPCS steganography to wavelet compressed video. 2004 International Conference on Image Processing: (ICIP, 2004) Singapore, IEEE, pp. 2147-2150.
Noda H, Niimi M, Kawaguchi E (2006). "High-performance JPEG steganography using quantization index modulation in DCT domain." Pattern Recognition Lett., 27(5): 455-461.
Noda H, Spaulding J, Shirazi MN, Kawaguchi E (2002). "Application of bit-plane decomposition steganography to JPEG2000 encoded images." IEEE Signal Processing Lett., 9(12): 410-413.
Potdar VM, Han S, Chang E (2005). Fingerpnnted Secret Sharing Steganography for Robustness against Image Cropping Attacks. 3rd IEEE International Conference on Industrial Informatics (INDIN). Perth, Australia, IEEE: 717-724.
Putter J (2006). "Copyright infringement v. academic freedom on the Internet: dealing with infringing use of peer-to-peer technology on campus networks." JL & Pol'y, 14: 419.
Retter LMM aCT (2000). The Use of Side Information in Image Steganography. Proceedings of the IEEE 2000 International Symposium on Information Theory and Its Applications (ISITA'2000), Honolulu, Hawaii, U.S.A.
Robie DL, Mersereau RM (2002). "Video error correction using steganography." EURASIP J. Appl. Signal Processing, 2002(2): 164-173.
Rubin D, Kneeland J (1994). "MR imaging of the musculoskeletal system: technical considerations for enhancing image quality and diagnostic yield." Am. J. Roentgenol. 163(5): 1155.
Rushmeier H, Ward G, Piatko C, Sanders P, Rust B (1995) Comparing real and synthetic images: Some ideas about metrics, Citeseer.
Seng WC, Du J, Pham B (2009). "Semi Fragile Watermark with Self Authentication and Self Recovery" Malaysian J. Comput. Sci., 22(1): 64-84.
Solanki K, Sullivan K, Madhow U, Manjunath BS, Chandrasekaran S (2006). Provably Secure Steganography: Achieving Zero k-l Divergence using Statistical Restoration. IEEE International Conference on Image Processing, USA.
Spaulding J, Noda H, Shirazi MN, Kawaguchi E (2002). "BPCS steganography using EZW lossy compressed images." Pattern Recognition Lett., 23(13): 1579-1587.
Su PC, Kuo CCJ (2003). "Steganography in JPEG2000 Compressed Images." IEEE Trans. Consumer Electronics, 49(4): 824-832.
Teo P, Heeger D (1994). Perceptual image distortion. Proceedings of the SPIE, Citeseer.
Van der Weken D, Nachtegael M, Kerre E (2004). "Using similarity measures and homogeneity for the comparison of images." Image Vision Comput., 22(9): 695-702.
Venkatraman S, Abraham A, Paprzycki M (2004). Significance of steganography on data security. International conference on information technology: (coding and computing). Las Vegas, Nevada, IEEE Comput. Society, 2: 347-351.
Wang CM, Wu NI, Tsai CS, Hwang MS (2008). "A high quality steganographic method with pixel-value differencing and modulus function." J. Syst. Software, 81(1): 150-158.
Wang H, Wang S (2004). "Cyber Warfare: Steganography vs. Steganalysis." Commun. ACM, 47(10): 76-82.
Wang SJ (2005). "Steganography of capacity required using modulo operator for embedding secret image." Appl. Math. Comput., 164(1): 99-116.
Wang Z (2001). Rate scalable foveated image and video communications, PhD thesis, Dept. of ECE, The University of Texas at Austin.
Wang Z, Bovik A (2002). "A universal image quality index." IEEE Signal Processing Lett., 9(3): 81-84.
Wang Z, Bovik A, Evans B (2000). Blind measurement of blocking artifacts in images. International Conference of Image Processing, IEEE, Vancouver, Canada, Citeseer.
Wang Z, Bovik A, Lu L (2002). Why is image quality assessment so difficult?, IEEE; 1999.
Wang Z, Lu L, Bovik A (2004). "Video quality assessment based on structural distortion measurement." Signal processing: Image Commun., 19(2): 121-132.
Wang Z, Sheikh H, Bovik A (2002). No-reference perceptual quality assessment of JPEG compressed images, Citeseer.
Wang Z, Sheikh H, Bovik A (2003). "Objective video quality assessment." The Handbook of Video Databases: Design and Applications, pp. 1041-1078.
Willmott C, Matsuura K (2005). "Advantages of the mean absolute error (MAE) over the root mean square error (RMSE) in assessing average model performance." Climate Res., 30(1): 79.
Winkler S, Gelasca E, Ebrahimi T (2003). "Toward perceptual metrics for video watermark evaluation." Applications Digital Image Processing 5203: 371-378.
Wu DC, Tsai WH (2003). "A steganographic method for images by pixel-value differencing." Pattern Recognition Lett., 24(9-10): 1613-1626.
Yuan C, Zhu B, Su M, Wang X, Li S, Zhong Y (2003). Layered access control for MPEG-4 FGS video, Citeseer.
Zaidan AA, Zaidan BB, Al-Frajat AK, Jalab HA (2010). "Investigate the Capability of Applying Hidden Data in Text File: An Overview." J. Appl. Sci., 10(17): 1916-1922.
Zaidan BB, Othman F, Kiah MLM, Taqa AY, Zaidan AA (2009). An Extensive Empirical Study for the Impact of Increasing Data Hidden on the Images Texture. Proceedings of the 2009 International Conference on Future Computer and Communication, Kuala Lumpur, Malysia, IEEE Computer Society.
Zaidan BB, Zaidan AA, Al-Frajat AK, Jalab HA (2010). "On the differences between Hiding Information and Cryptography Techniques: An Overview." J. Appl. Sci., 10(15): 1650-1655.
Zaidan BB, Zaidan AA, Othman F, Raji RZ, Mohammed SM, Abdulrazzaq MM (2009). Quality of Image vs. Quantity of Data Hidden in the Image. Proceedings of the 2009 International Conference on Image Processing, Computer Vision, and Pattern Recognition, IPCV 2009, Las Vegas Nevada, USA, CSREA Press.
Zhang X, Wang S (2006). "Dynamical running coding in digital steganography." IEEE Signal Processing Lett., 13(3): 165-168.
Zlokolica V, Pizurica A, Philips W (2003). Video denoising using multiple class averaging with multiresolution. Visual Content Processing and Representation. Berlin / Heidelberg, Springer, 2849: 172-179.