International Journal of Security and Its Applications
Vol. 10, No. 4 (2016), pp.179-196
http://dx.doi.org/10.14257/ijsia.2016.10.4.18

Quality Evaluation of Image Steganography Techniques: A Heuristics based Approach

Ratnakirti Roy[1*] and Suvamoy Changder[2]

[1,2]*Department of Computer Applications, National Institute of Technology, Durgapur, India*
[1]*rroy.nitdgp@gmail.com*, [2]*suvamoy.nitdgp@gmail.com*

Abstract

Steganography refers to techniques that hide information inside innocuous looking objects known as "Cover Objects" such that its very existence remains concealed to any unintended recipient. Images are pervasive in day to day applications and have high redundancy in representation. Thus, they are appealing contenders to be used as cover objects. There are a large number of image steganography techniques proposed till date but negligible research has been done on the development of a standard quality evaluation model for judging their performance. Existence of such a model is important for fueling the development of superior techniques and also paves the way for the improvement of the existing ones. However, the common quality parameters often considered for performance evaluation of an image steganography technique are insufficient for overall quantitative evaluation. This paper proposes a rating scale based quality evaluation model for image steganography algorithms that utilizes both quantitative parameters and observation heuristics. Different image steganography techniques have been evaluated using proposed model and quantitative performance scores for each of the techniques have been derived. The scores have been observed to be in accordance with actual literature and the system is simple, efficient and flexible.

Keywords: *Image Steganography, Cover objects, Quality Evalutation, Heuristics, Rating Scale Method*

1. Motivation

The need for digital communication has increased dramatically in the recent times and as a result the Internet has essentially become the most effective and fastest medium for digital communication. At the same time, data over the internet has become susceptible to threats like copyright infringement, eavesdropping, hacking and thereby necessitating secret communication. As a result a new domain dealing with security of data has evolved and is known as information hiding. Steganography is a comparatively new inclusion in the field of digital information hiding but it traces its origin to long back in history.

The word "Steganography" is derived from Greek 'Steganos" meaning hidden or concealed. Thus, "Steganography" stands for "concealed writing". The primary goal of a steganography system is all about creating a form of covert communication between two parties. Steganography uses a medium like an image, video, audio or text file to hide some information inside it in such a way that it does not attract any attention and looks like an innocent medium [1]. The media with and without hidden information are called stego-media and cover media, respectively [2]. Steganography is complementary to cryptography where it aims at hiding the existence of a message rather than making the message illegible through encryption. Thus Steganography might be useful for secret communication in countries and regions where public use of cryptography is prohibited or restricted.

* Corresponding Author

ISSN: 1738-9976 IJSIA

Mathematically, steganography can be defined as a quintuple $\partial =< C, M, K, D_k, E_k >$ where, C is the set of all possible covers, M the set of secret messages with $|C| \geq |M|$, K is the set of keys, $E_K: C \times M \times K \rightarrow C$ and $D_K: C \times K \rightarrow M$. E_K and D_K are the embedding and the extraction functions respectively, such that, $D_K(E_K(C, M, K), K) = M$. It is interesting that the embedding function E_k has been shown to map the cover image C, the secret message M and the stego-key K to the same image C. This is because, theoretically it is expected that the stego-image and the cover image should be indistinguishable.

A typical steganography system is portrayed using the Prisoner's Problem [3] where two inmates Alice and Bob are hatching out an escape plan and Wendy, the warden observes communication between them. Wendy would put them to solitary confinement if she finds them communicating secretly. Thus, Alice and Bob must communicate in such that Wendy does not get to perceive their secret communication. In order to achieve this, they need to hide messages inside innocuous objects such that its very existence remains concealed to Wendy [4].In this context, steganalysis is the set of techniques (visual or statistical) by which it is possible to check for the existence of steganographic content in a cover object. Thus, it is through steganalysis that Wendy can test for the existence of any hidden message concealed in the medium of communication of Alice and Bob.

Recently, images have been a very popular choice as a cover medium primarily because of its redundancy in representation and pervasiveness in applications in daily life [5]. Over the years, many algorithms for hiding data in images have been proposed and developing newer algorithms are a topic of current research. However, negligible amount of research has been done in the development of a model that would evaluate the overall performance of an image steganography algorithm quantitatively. The necessity of such a model arises out of the fact that steganography algorithms span over a wide range of image formats, computational complexity and platforms of implementation. Thus, it is evident that there are a wide number of factors that might affect the overall performance of the algorithm. In general, a limited number of factors are considered individually for performance of an algorithm. However, these parameters have different units of measurement and are thus difficult to integrate to form a definitive quantitative system. As a result, there are many steganography algorithms available but hardly any model for their evaluation in a quantitative manner is proposed. A possible approach in resolving this issue may be the development of a measurement scale that will be able to bring most qualitative and quantitative measures adopted to evaluate image steganography techniques under one umbrella.

However, such an approach, though seems quite lucrative has hurdles to overcome. One of the big challenges in this context will be to fix the ranges of the parameters involved. As many parameters are qualitative measures but nevertheless important for consideration, hence it is obvious that such parameters cannot be omitted. Thus, in order to adapt these to a quantitative scale, observation heuristics may be useful. Some initial investigation in to the matter has been done in [6] where observation heuristics and available quantitative data from literature was thoroughly surveyed and merged to give an idea of their performance. The experimental data obtained from the literatures and also through implementation wherever possible was used to grade the algorithms in the scale *Low-Medium-High*. Interestingly, these gradations were more or less accurate with the claims made in the original literatures. Thus it was evident that such heuristics based approach may be applied to form an evaluation model for the image steganography techniques as well. This paper aims to propose a quality evaluation framework that uses performance observation heuristics to develop a rating scale that will be able to generate cumulative scores for any image steganography technique under consideration and thus evaluate its overall performance in accordance with the scores.

2. Relevant Terminology

Throughout the remainder of this text, the following terms are repeatedly used and thus need to be properly defined for better readability.

(i) ***Image****:* An image C is a discrete function assigning a colour vector *c(x, y)* to every pixel *(x, y)* [7].

(ii) ***Cover Image****:* The cover image is the carrier of the hidden message. A cover is generally chosen in a manner that it appears most ordinary and innocuous and does not arouse suspicion as such.

(iii) ***Stego Image****:* The cover image with a secret message concealed within it is known as the *Stego* image. It is used at the recipient site for extracting the hidden message.

(iv) ***Stego Key****:* It is a key to embed data in a cover and extract data from the same. It may be a number generated via a pseudo-random number generator [8] or can just be a password for decoding the embedding location.

(v) ***Embedding Domain****:* The embedding domain refers to the cover image characteristics that are exploited in order to embed messages. It may be spatial domain when the constituent elements of the cover (e.g. pixels in an image) is modified directly or it can be the frequency domain or transform domain if mathematical transformations are carried on the medium before embedding.

3. Preliminary Observations and Literature Review

In the recent times there have been quite a large number of research activities in the field of image steganography. Many algorithms have been developed over the existing LSB methods and also in the transform techniques. Several algorithms are available in literature. The techniques are primarily classified into two major classes based on whether the pixels of the image are modified directly or some mathematical transform is applied on the images before embedding. The former techniques are called spatial domain techniques while the latter are the transform domain techniques. After initial investigation it appears that the security level of the transform domain techniques are higher than that of the spatial domain algorithms. This is because transform domain techniques abstain from modifying the pixels of an image directly and hence the statistical signatures left behind these algorithms are less evident. But at the same time spatial techniques do offer larger capacity of embedding. Algorithm such as F5 has a very low rate of bit-flipping which makes it immune to most steganalysis attacks. Spatial domain schemes are generally of low complexity in terms of their time and resource requirements.

Techniques that use transforms and other statistics preserving mechanisms are inherently more complex. Spatial domain techniques work well with lossless images such as TIFF, BMP *etc*. but are less applicable to images supporting lossy compression such as JPEG/JPEG2000. Transform domain techniques however are suitable for application to both lossless and lossy images. This makes them comparatively more versatile withrespect to the choice of the cover image. As a result, initially the transform domain algorithms seem to have an upper hand in comparison to the spatial domain steganography techniques. However in order to completely evaluate the performance of the image steganography techniques, the common evaluation parameters may not be enough. Thus it is necessary that the existing evaluation parameters be explored in depth in order to find their dependency on various other factors which can be more accurately quantified. In an effort to find such parameters, different popular steganography techniques were carefully surveyed and a list of their weaknesses (mostly deviated image statistics) was prepared. The description of the methods has been derived from [6] which provide an initial

foundation for the image steganography evaluation model to be proposed later in the current text.

3.1. Spatial Domain Techniques

(i) Direct Least Significant Bit Replacement: LSB replacement or LSBR forms one of the most conventional techniques of hiding considerably large secret messages without introducing many visible distortions [9]. It replaces the LSBs of randomly selected or sequential pixels in an image. The following operation describes the embedding of the LSB substitution

$$Y_i = 2\left\lfloor \frac{X_i}{2} \right\rfloor + m_i$$

where m_i, X_i and Y_i are the i^{th} message bit, value of the selected pixel before embedding and value of the modified pixel after embedding respectively [5]. The biggest advantage of the LSB substitution method is its simplicity. LSB substitution affects pixels by *±1*, if it can be assumed in general sense that the distortion produced by the mechanism is perceptually transparent in the passive warden [10] context. However, LSB substitution is extremely susceptible to statistical attacks and image processing activities like compression, cropping *etc*. In fact, embedding in LSB causes PoVs (Pair of Value) in the image to flatten out with respect to each other which makes LSB embedding more susceptible to steganalysis [4].

(ii) Optimal Pixel Adjustment Procedure (OPAP): Originally proposed by Chi-Kwon Chan and L.M Cheng [11, 12], the OPAP scheme was developed as an improvement over the LSB based algorithm and described in [13]. The OPAP scheme modifies the embedded bits in order to improve the overall visibility of the stego image. The adjustment is done on the basis of the pixel differences between original pixel p_i and the pixel p_i' of the stego-image. If the difference is δ_i then depending on it pixel modification is done on the pixels before the embedded pixel so as to minimize the difference between the original pixel and the embedded stego pixel. The algorithm is tested for grey scale images and provides good overall imperceptibility. OPAP has been tested to provide high visual fidelity of the stego image for standard test images Baboon and Lena [14].

(iii) Pixel Indicator Technique (PIT) [15]*:* Pixel Indicator Technique is basically a modification over the conventional LSB insertion method of embedding and is primarily devoted to enhancing the security of the existing LSB scheme. PIT was designed to work on 24-bit/pixel RGB images. The algorithm uses two LSB of one colour channel to mark the existence of data in the other two. The size of the secret data serves as the key for choosing the selection channel. The indicator channel and the embedding channel are ordered in the following way: RGB, RBG, GBR, GRB, BRG, and BGR. The algorithm produces extremely low visual distortion when the embedding rate is less than 3 bits and has low susceptibility to histogram and visual attacks at this rate. Thus the maximum recommendable embedding rate for the PIT is less than 3 bits/ colour channel.

(iv) Pixel Value Differencing: In Pixel Value Differencing or PVD scheme [16], the number of insertion bits depends on whether the pixel is an edge or a smooth area [14]. Human Visual System is sensitive to subtle changes in the smooth areas as compared to the edges. This is because the difference between the pixels in the smooth areas is much less as compared to that between the edge pixels and embedding in edge pixels causes less visual perceptible distortion. Some implementations of the PVD scheme may be found in [17, 18]. PVD does not cause much visual distortion and neither it is directly susceptible to the histogram attack as the LSB substitution. It is however susceptible to histogram analysis of the differences of the pixel pairs and χ^2*-attack* [19].

(v) SLSB: The Selected LSB algorithm (SLSB) proposed in [20] embeds into single colour components of the pixels. It does not necessarily embed into the LSBs only but chooses the

colour plane and the modifiable bits of the colour plane in such a manner that will produce the minimum distortion. It can be classified under filtering algorithms as it applies a sample pair analysis filter before embedding to ensure that only the best candidate pixels are selected for embedding. It can embed at a rate of more than 1 bit per pixels. This however might lead to alteration of the degree of randomness of the pixels of the image and thereby makes it susceptible to statistical attacks when used for high degree of embedding.

3.2. Transform Domain Techniques

(i) JSteg: The JSteg algorithm is acclaimed as the first commercially available steganography tool for JPEG images [21]. The algorithm applies Discrete Cosine Transform to the image blocks and embeds the data in to LSBs of the DCT coefficients sequentially. The sequential embedding and absence of any secret key makes the algorithm susceptible to eavesdropping as only knowledge of the embedding procedure is sufficient to decode the hidden message. Moreover, JSteg is easily steg-analyzed using the χ^2*-attack*. Also, as the algorithm uses the DCT, it is extremely necessary to treat the DCT coefficients with sensitive care and intelligence in order to prevent the algorithm from leaving significant statistical signatures [22]. However, JSteg provided an embedding capacity of 12% [23].

(ii) Outguess: The algorithm was developed by N. Provos *et al.* [21] as an improvement of the existing JSteg method. Outguess uses a PRNG (Pseudo Random Number Generator) to randomize the pixels in which the embedding is supposed to be made. It skips embedding into DCT coefficients with values 0 and 1 as because they form a *Pair of Value* when their LSB changes and there are no ways of distinguishing between a zero DCT coefficient and a steganographic zero. The algorithm, after embedding, modifies the unchanged DCT coefficients to preserve the histogram of the original image. Thus, OutGuess is immune to attacks like the visual attack, histogram attack and the χ^2*-attack*. However, Fridrich *et al.* [24] have successfully steganalyzed OutGuess by calculating the *blockiness* of the image. The steganalyzing algorithm for OutGuess utilizes the fact that as OutGuess uses LSB embedding of the DCT coefficients and that it makes random changes to the quantized coefficients, the spatial discontinuity at the border of each *8X8* block will increase.

(iii) F5: The F5 algorithm was proposed as a steganography technique that allows higher capacity of embedding and better security at the same time [23]. The F5 differs from most other steganography techniques in the fact that it does not overwrite LSBs of DCT coefficients/pixels rather it increments/decrement the value of the DC coefficients depending on need. The algorithm takes into consideration that flipping the LSBs either at the pixel level or at the DC coefficient level alters the statistical properties of the image and can serve as a means to steg-analyze the algorithm. F5 uses permutative straddling and matrix encoding to scatter the embedding effect and to embed data respectively. F5 is the first implementation of the matrix encoding method proposed in [25]. F5 embeds at a rate of 3.8 bits per change and is secure against most statistical attacks like the histogram attack, the χ^2*-attack*, blockiness detection *etc*. Moreover it has a high embedding capacity. However, F5 remained a challenging algorithm to break until Fridrich *et al.* steganalyzed F5 by estimating the original histogram of the cover image from the stego image [26]. It is done by decompressing the stego-image to spatial domain, cropping it by 4 pixels in both directions and recompressing using the same quality factor as the stego image.

(iv) Singular Value Decomposition (SVD) transform based method (RHISSVD): The SVD based steganographic method proposed in [27] transforms the image into singular values and then embeds into them. Singular Values correspond to the luminance in the image and minor changes into them do not cause perceptible distortions in the image. The experimental results show that the method has a high PSNR value beyond the perceptible

range for RGB images with compression *quality* $\leqslant$ *60 %.* It has an average embedding capacity of 0.44 bits per singular value coefficient for an image with compression *quality 50%.*

4. Proposed Evaluation Model

In order to evaluate the performance of different techniques for image steganography, it is important to define some acceptable evaluation criteria based on the quality of the objectives. Moreover, setting up specific evaluation parameters helps in leading to development of newer algorithms and also to improve the performance of the existing algorithms. Three common requirements namely level of security, capacity and stego image fidelity may be used as the parameters to be considered for evaluating the image steganography algorithms [28]. Apart from these, there are factors such as the runtime complexity of the algorithm that influences the overall performance of the algorithm. These major factors however depend on various other sub parameters which actually determine the overall weights of the major factors. The model proposed here is a rating scale based system that will assign values to the parameters in accordance with a set of rules (to be proposed later) that will govern the awarding of the values to the parameters. This section is divided into three parts; the first describes the parameters to be used in the model whereas the second and third parts frame the rating scale system to be adopted for the proposed quality evaluation model.

4.1. Parameters to be Considered

To design the quality evaluation model, we consider four primary parameters namely, *Level of security, capacity, Imperceptibility or Fidelity* and *Runtime Performance* for judging the overall performance of any steganography algorithm under consideration. The parameters are elaborated as under.

a. Level of Security: There have been many approaches till date in defining the security of a steganographic system. Zollner et al. [29] provide an analysis to show secure steganography from the information theoretic point of view is possible if embedding operation has a random nature and the embedded message is independent from both the cover-object and stego-object. These conditions, however, ensure non-detectability against an attacker who knows the stego-object but has no information available about them in deterministic embedding operation. In [30], Cachin defined steganographic security from the information theoretic perspective. Let, P_c and P_s be probability distributions of the cover image and the stego-image respectively. Then the detectability *D (Pc||Ps)* is given by,

$$D(P_C \parallel P_S) = \sum P_C \log \frac{P_C}{P_S} \quad (1)$$

The expression above is also known as the *KL-Divergence* or the Relative Entropy between two probability distributions. Thus, for a completely secure stego system, D=0 and if D$\leq\epsilon$, then it is ϵ-secure. Perfectly secure stego systems may be shown to exist theoretically but they are impractical. In short, security of a stego system is defined in terms of undetectibility. A steganography system is said to be undetectable or secure if no statistical tests can distinguish between the cover and the stego-image [31]. The impracticality of the fact that perfectly secure stego-systems exist in the real world well establishes the reason behind using observational heuristics for fixing operational ranges for the different parameters under consideration. Hence, using Equation 1, the relative entropy between the cover and the stego image can be calculated. But, level of security cannot be ascertained wholly by using relative entropy alone. Other factors like

embedding efficiency, degree of resistance to statistical steganalysis are equally important in determining the level of security offered by any steganography technique.

b. *Capacity*: Capacity of a steganography system implies the amount of data that can be effectively hidden within a selected cover medium by a steganography algorithm without causing visual impairment to the image. The embedding rate is mostly expressed in absolute measurement (such as the size of the secret message) or in relative measurement called the data embedding rate (given mostly in *bits per pixel* or *bpp*, *bits per non-zero DCT coefficients* or *bpnc*, *etc*.).

c. *Imperceptibility or Fidelity*: Stego images are expected not to have any significant visual artifacts. Under the same level of security and capacity, higher fidelity of the stego image implies better imperceptibility. There are numerous quantities that can be used for measuring the stego-image quality but for convenience we use two commonly used measures or stego image fidelity namely, Mean Square Error and Peak Signal to Noise Ratio to estimate the stego-image fidelity. Other image quality metrics that can be used to estimate the visual fidelity of the stego image include *Structural Similarity Index Measure (SSIM), Absolute deviation etc*.

d. *Runtime Performance*: Steganography algorithms vary according to their domain of embedding. In simpler systems, the embedding job is less time consuming but may not be as secure as some other more complicated `systems offering better performance. Nevertheless, runtime performance of an algorithm is important for judging the applicability of the algorithm for embedding into large images and also their implementation in low resource systems such as mobile devices *etc*. Runtime performance depends on factors like *domain of embedding, embedding time, degree of pre-processing* involved and so on.

The above parameters, their sub-parameters along with the inter-dependencies can be pictorially expressed as in Figure 1 (Figures in bracket signify the symbolic representation for each of the parameters)

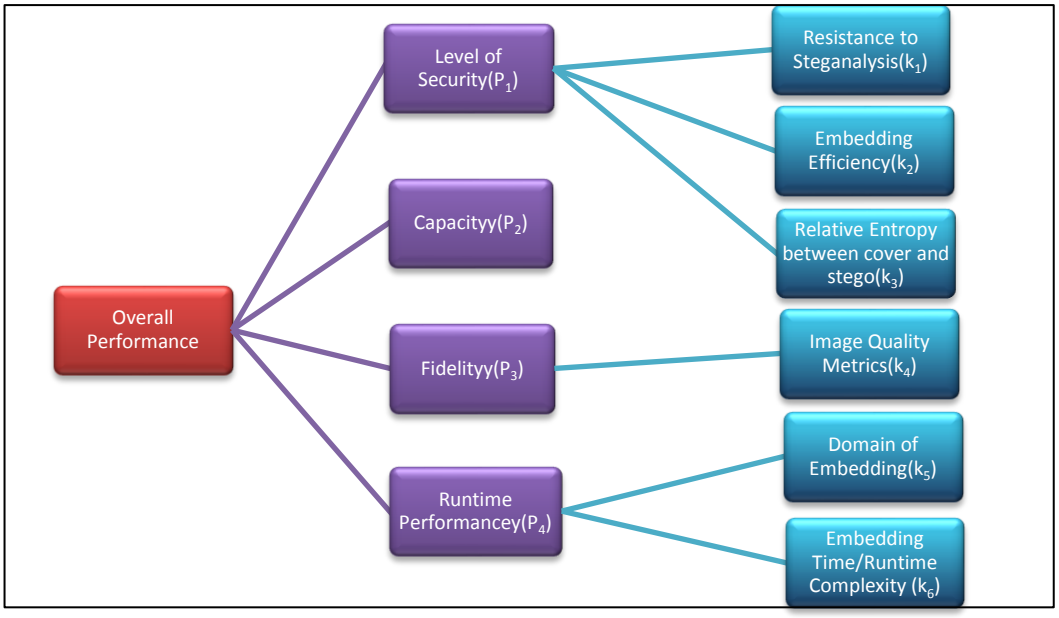

Figure 1. Steganography Parameters and their Dependencies

4.2. The Proposed Rating System

The proposed performance evaluation system aims to find a quantitative performance score resulting from the experimental data and interpretation of observational heuristics, for any image steganography technique under consideration. To achieve this, we adopt a rating scale based mechanism which rates parametric values obtained from each algorithm in a *low-medium-high* type scale. Each rating has an associated numeric weight which signifies the score of a particular parameter for the algorithm. It is mention worthy that the numeric weight associated with a rating depends strictly on the parameter under consideration. For example, in Figure 1, the relative entropy between the cover and the stego image is expected to be as low as possible. Thus, a steganography technique which gets a *low* rating for the relative entropy parameter is expected to be of higher level of security. Hence, here a low rating has the highest associated numerical weight. Such an adjustment easily adapts the system for both direct and inversely related parameters. Mathematically the proposed system can be expressed as follows:

Let there be *n* parameters which determine the performance of an image steganography technique *A*. If *p parameters* (say P_i) among these *n* parameters have *m* sub-parameters*(denoted by* k_j*)* and the respective numeric weight allotted to each k_j be w_j, then the score for each P_i, denoted by $Score_i$ is calculated as,

$$Score_i = \sum_{m} w_j \tag{2}$$

where, *m* is the number of sub-parameters k_i and $m \in \mathbb{Z}^+$with $\mathbb{Z}^+$signifying the set of all positive integers greater than *zero*. Thus, the overall performances score (OPS) of the image steganography technique *A* is given by,

$$OPS = \sum_{i=1}^{n} Score_i = \sum_{i=1}^{p} \sum_{j=1}^{m \epsilon \mathbb{Z}^+} w_j \tag{3}$$

Similarly, if there are *r* parameters which do not have sub parameters, then each of these parameters will have a direct score. The overall score comprising of parameters with sub-parameters and parameters without parameters is calculated as,

$$OPS = \sum_{i=1}^{n} Score_i = \sum_{k=1}^{r} rw_k + C \tag{4}$$

Where rw_k is the numeric weight allotted to parameter r_k and *C* is the score of the remaining parameters (with sub-parameters). *C* is calculated as in Equations (2) and (3).

Since, each of the parameters will have a maximum score they can attain, therefore is evident that the *overall performance score*, a numeric value, can be well be interpreted as a suitable performance measure with a higher value indicating a better performance. Once the final score generation expression has been finalized, it is now required to set criteria for awarding scores to the parameters. The parameters, their rating criteria and the basis for the criteria are explained next.

4.3. Rating Criteria

(i). Level of Security: The level of security offered by any steganography technique depends primarily on three factors, namely, resistance to *statistical Steganalysis*, *embedding efficiency* and the *Relative Entropy* between the cover and the stego images.

a. Resistance to Statistical Steganalysis: In order to determine the degree of resistance an image steganography technique is capable of offering against Steganalysis, the

steganalysis methods are further classified into three categories depending upon the statistical properties of the image they exploit. The categories are shown in Table 1. Based on the classification in the said table, any algorithm that is resistant to the attacks in the first category can be said to be of *low* resistance to statistical steganalysis, that is resistant to the attacks in both the first and second categories is assumed to have *medium* resistance and so on. Similarly, there can be instances where a steganography technique may show rather partial containment to a category rather than total. For example, a steganography algorithm may resist all attacks in category *A* but may not resist all in category *B*. In such a case, a score corresponding to the mean of the two categories may be considered. The scale is shown in Table 2.

Table 1. Categories of Steganalysis Methods

Category	***Type of Attack***	***Variants***
A	Visual Attacks	LSB Plane Extraction, Visual Quality Estimation
B	Common Histogram based Attacks	HCF-COM, HCF, RS-Steganalysis, χ^2-attack
C	Other Specialized Attacks	Blockiness Detection, Calibration Attack, Step Effect Detection

Table 2. Scale for Resistance to Steganalysis

Category	***Scale Value***	***Numeric Equivalent***	***Max. scale Value***
A	Low	1	3
A,B	Medium	2	
A,B,C	High	3	
A,B*	Low-Medium	1.5	
A,B,C*	Medium-High	2.5	
A,B*: Resistance to Cat A, Partial Resistance to Cat B. **A,B,C***: Resistance to Cat A, B, Partial Resistance to C			

b. Embedding Efficiency: Embedding efficiency is defined as the bits embedded per unit distortion in the cover image. Thus, it is evident that a high embedding efficiency scheme will produce less statistical artifacts in the cover image and hence it will add up to the level of security. If any embedding step changes n_1 bits in the cover image to embed n_2 bits, the embedding efficiency of the technique, η is defined as:

$$\eta = \frac{n_2}{n_1} \tag{5}$$

There are different image steganography techniques and each of them offers different levels of embedding efficiency. Several high embedding schemes such as matrix encoding

are also available in literature. However, it is evident that higher the embedding efficiency, lower will be the alteration in the statistical properties of the cover. It has been observed that the lowest embedding efficiency is seldom less than *1*, that is, a unit distortion will at least embed 1 bit of information in the cover image. Similarly, high embedding efficiency schemes can support embedding efficiency as high as 9.02. However, a high embedding efficiency such as 9.02 comes at a compromise of the capacity utilization and thus applicable for small messages. It is more common to find embedding schemes with acceptable capacity utilization along with high embedding efficiency in the range of 3-4 bits per unit distortion. A rating scale based on such observations can be framed as in Table 3.

Table 3. Scale for Embedding Efficiency

Scale Value	***Criteria***	***Numeric Equivalent***	***Max. scale Value***
Low	$\eta \leq 1.5$	1	3
Medium	$1.5 < \eta \leq 3$	2	
High	$\eta > 3$	3	

c. Relative Entropy between Cover and Stego Images: Embedding information in a cover image alters the average amount of information or the entropy of the cover image. Hence, the stego image is expected to have a different entropy value as compared to the cover image. Thus, one of the primary aims of any steganography system is to minimize the entropy difference between the cover and the stego objects. For images, the entropy difference can be measured using the *Relative Entropy* between the cover and the stego images as in Equation (1). For fixing the scale for rating the algorithms based on the relative entropy between the cover and the stego images, different algorithms have been implemented with identical cover and secret messages and the relative entropy between the cover and the stegoimages were measured.

The algorithms have been carefully selected so that both spatial and the transform domains are explored maximally. It is evident from Equation (1) that a steganography scheme that produces the least modification on the cover must have relative entropy between the cover and the stego images close to *zero*. However, achieving zero relative entropy between the cover and the stego image is only possible if no modification of the cover takes place at all, which is practically impossible if information embedding takes place. Machine implementation revealed that the relative entropy between cover and stego image peaked at 0.607 bits/pixel for OPAP scheme. Table 4 shows the rating scale based on the above observation. In Table 4, low relative entropy has been rated the highest, that is, lower the relative entropy between the stego and the cover image, larger will be its contribution towards high level of security.

Table 4. Scale for Embedding Efficiency

Scale Value	***Criteria***	***Numeric Equivalent***	***Max. scale Value***
Low	$0 < R.E \leq 0.1$	3	3
Medium	$0.1 < R.E \leq 0.5$	2	
High	$R.E > 0.5$	1	

(ii). Capacity: The capacity of an image steganography scheme is defined as the amount of data it can successfully embed into a cover image without leaving behind visible artifacts. However, measuring the embedding capacity of a steganography technique will vary according to the domain of implementation. Spatial domain steganography techniques, which directly alter pixel values to embed data, have their embedding capacity measured in terms of *bits per pixel(bpp)*. On the other hand, transform domain techniques mostly modify the non-zero post-transform coefficients instead and their embedding capacity is given in terms of *bits per non-zero coefficient (bpnc)*. Machine implementation reveals that spatial domain techniques have a varied rage of embedding capacities ranging from *1bpp-4bpp* for most of them while for the transform domain methods, the embedding rate varied from a low of less than 0.4 bpnc for YASS to a high of 0.8 bpnc for F5. On the basis of these observations, a probable scale that can well be used to rate the capacity parameter for steganography systems is as shown in Table 5 and Table 6 for transform domain and spatial domain respectively.

Table 5. Scale for Capacity (Transform Domain)

Scale Value	***Criteria (capacity in bpnc)***	***Numeric Equivalent***	***Max. scale Value***
Low	0.1<Capacity≤0.3	1	3
Medium	0.3<Capacity≤0.6	2	
High	Capacity>0.6	3	

Table 6. Scale for Capacity (Spatial Domain)

Scale Value	***Criteria (capacity in bpp)***	***Numeric Equivalent***	***Max. scale Value***
Low	0<Capacity≤1	1	3
Medium	1< Capacity ≤3	2	
High	Capacity >3	3	

(iii). Fidelity or Imperceptibility: Fidelity, from the image steganography point of view refers to the visual quality of the resultant stego image after an embedding operation has taken place. Nevertheless, high fidelity implies better visual quality of the stego image and thus, it is one of the primary requirements of any image steganography system. Fidelity of the stego image can be directly determined by the use of some standard image quality metrics. One common such metric is the *Peak Signal to Noise Ratio* or PSNR measured in decibels (*dB*). PSNR estimates the degree of distortion induced in the stego image as compared to the original cover image. In the calculation of *PSNR,* it is necessary to define Mean Square Error (MSE). MSE and PSNR are defined as follows:

$$MSE = \frac{1}{MXN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(x_{ij} - y_{ij}\right)^2 \quad (6)$$

$$PSNR = 10\,log_{10}\left(\frac{MAX^2}{MSE}\right)dB \quad (7)$$

where *M, N* are the horizontal and vertical pixel dimensions of the cover image, x_{ij} and y_{ij} are the pixel values in the cover and the stego image respectively. *MAX* signifies the maximum value a pixel may hold for a particular cover image. For binary images, *MAX=1* and for 8-bit grayscale/RGB images *MAX=255*. For an almost human eye imperceptible stego image, the threshold for PSNR is at least 40 dB [32]. For the same cover image and payload, some of the implemented algorithms produce PSNR values as high as 65.84*dB* whereas PSNR values as low as 37.17*dB* has been recorded. Based on these results, the corresponding rating scale for evaluating the degree of fidelity offered by a steganography technique is as shown in Table 7. The numeric equivalent for the low and medium scale values has been set in a range to adjust minor differences from the next higher scale. The range adjusts by 0.05 for each 1 dB change in PSNR from the next starting scale.

Table 7. Scale for Visual Fidelity

Scale Value	***Criteria (PSNR in dB)***	***Numeric Equivalent***	***Max. scale Value***
Low	PSNR<40	0.5-1.95	3
Medium	40≤PSNR<60	2-2.95	
High	PSNR≥60	3-4	

(iv). Runtime Performance: Runtime performance of any steganography algorithm depends primarily on two factors, namely, *domain of implementation* and *embedding time.*

a. Domain of Implementation: Image steganography algorithms are generally classified according to the type of alteration they carry out on the cover image. This can be either by directly modifying the pixel values or modifying transformed coefficients of the cover image. Spatial domain algorithms (direct pixel modifications) are inherently simple to implement and use less of computer resources. Thus they are expected to have a better runtime performance as compared to their transform domain counterparts which apply mathematical transforms on the cover image before embedding and subsequent inverse transforms after embedding. They are more resource consuming and have more complex implementation. Based on such observations, a rating system as in Table 8 may be considered.

Table 8. Scale for Domain of implementation

Scale Value	***Criteria***	***Numeric Equivalent***	***Max. scale Value***
Low	Spatial Domain	2	2
Medium	Spatio-Transform	1.5	
Medium/High	Transform Domain	1	

b. Embedding Time and Pre-embedding steps: Embedding time is a useful metric in determining the runtime performance of any image steganography technique. Experimental verification of the embedding time for different algorithms reveal that for a standard image payload of size 100X100, embedding time ranges from around 1.4

seconds to 2.79 seconds for steganography methods such as LSBR and PVD. Similarly, in a separate experiment with similar setup for transform domain methods, the embedding time clocked in a range of 3-5 seconds. However, setting up a rating scale based on time of embedding alone is difficult as because embedding time has a dependence on the underlying hardware used for testing. If a graphical plot of the embedding time against varying payload sizes is performed, it reveals how the embedding time changes with respect to the varying payload.

This trend is however likely to remain same even if the processing power of the underlying hardware changes. It is observed that techniques which perform more pre-embedding steps require more time to execute as compared to those are simpler. Often the computational complexity of the pre-embedding influences the overall runtime performance of the steganography scheme. For example, JSteg and F5 both use DCT based embedding schemes but F5 uses a further permutative straddling step before actual embedding takes place. As a result F5, though claimed to be more secure than JSteg, has a higher runtime. Table 9 depicts a rating scale developed from such knowledge.

In Table 9, Simple Pre-Embedding Processing signifies *single step* pre-processing such as only applying a mathematical transform (as in JSteg) after which the next step is embedding. Complex Pre-Embedding Processing will then refer to algorithms which perform *more than one* distinct pre-embedding calculation before the actual embedding takes place.

Table 9. Scale based on Embedding Time and Pre-Embedding Steps

Scale Value	***Criteria (PSNR in dB)***	***Numeric Equivalent***	***Max. scale Value***
Low	No Pre-Embedding Processing	3	3
Medium	Simple Pre-Embedding Processing	2	
High	Complex Pre-Embedding Processing	1	

5. Evaluating the Algorithms and Result Analysis

In the previous section, the parameters to be considered for evaluating image steganography techniques are described and the rating scale to be adopted for quantitative evaluation of the same are explained in details. In addition to this, the parametric ratings are combined together mathematically to form an expression for deriving the quantitative overall performance score. Once the parameters under consideration have been adjusted to fit a rating scale and a method for calculating an overall performance score has been devised, the next step is to validate the performance of the proposed rating scale based evaluation system. For this purpose, a set of six well known algorithms, three each from the spatial domain and the transform domains respectively have been selected. These algorithms are then evaluated using the proposed rating scale to verify whether the scale produces acceptable scores for the techniques under consideration or not. The techniques chosen for testing the proposed rating scales are *Randomized Least Significant Bit Replacement (LSBR), Optimal Pixel Adjustment Process (OPAP)* at 3 bits/pixel and *Pixel Value Differencing (PVD)* at 3 and 4 bits/pixel variants for spatial domain techniques and *JSteg, Outguess (OG) and F5* for transform domain techniques respectively. Every parameter defined in Section 4 has a maximum obtainable score as in Table 10.

Thus, all steganography techniques that will be evaluated using the proposed model will have a cumulative score less than or equal to *21*. So, a score more near to *20* will indicate overall higher quality for any steganography technique under consideration. Experiment was performed on an AMD 2.4 GHz machine with 2 GB primary memory and without any additional graphics accelerators. The cover used was *Nadal* image of 480*480 with a secret image of size 100*100. The experimental results are shown in Table 11. The scores obtained for different steganography techniques using the proposed rating scale based evaluation model are listed in table 12. The sub-parameters are labeled as in Figure 1.

Next, the steganography techniques under consideration in Table 11 are evaluated for their scores according to the rating scale proposed in the previous section. The detailed score sheet is given in Table 12.

The scores obtained in Table 12 can now be used to interpret the performance of the steganography techniques under consideration. The score sheet reveals that the F5 steganography technique shows the best performance with a score of 16.5 out of 20. This result thus conforms that F5 outperforms most other existing steganography techniques as available in the literature. Similarly, for the spatial domain techniques, the Pixel Value Differencing (PVD) with high capacity *4 bpp* embedding is the best performer with an overall score of 13.35. This is also in accordance with the information in the literature. Thus, the rating scale system adopted for quantitative evaluation of the steganography techniques provides satisfactory results. Again, Randomized LSBR and the Optimal Pixel Adjustment Procedure both are scored at *nearly equal values*. OPAP inherently involves more bits flipping in order for pixel adjustment and hence produces a larger stego-cover relative entropy value as compared to be LSBR or the randomized LSBR, resulting in a lower score in the relative entropy sub-parameter. Another important observation from the scores obtained in Table 12 is the performance of the transform domain steganography technique F5. It is the only technique among those considered here which has an *embedding efficiency* greater than 1. This significantly increases their performances in the level of security parameter giving it an overall higher score (16.95). Employing high efficiency embedding schemes can significantly improve visual fidelity and also the embedding capacity.

The performance scores can also be used for segregated analysis of the techniques and can form the basis for requirement based selection of the steganography techniques. For example, consider a situation where the requirement is more focused on high fidelity of the stego-image as well as good runtime performance. In such a case, both LSBR and JSteg will serve the purpose well. Similarly, if high embedding capacity, high security as well as high fidelity of the stego-image is expected, then F5 will serve the best. Thus, the scores generated by the rating system acts well as a guideline for the choice of image steganography technique to be used under different requirement situations.

Table 10. Scale based on Embedding Time and Pre-embedding Steps

Parameter	***Sub-Parameters***	***Maximum Score/Parameter***
Level of Security	Resistance to steganalysis (3)* Embedding efficiency (3) Relative Entropy (3)	9
Capacity	NA	3

Fidelity	Image Quality Metrics (4)	4
Runtime Performance	Domain of Implementation (2) Embedding Time (3)	5
Overall Maximum Score		**21**
*Figures in the brackets signify maximum score for each sub-parameter, NA: Not Applicable		

Table 11. Experimental Data sheet

Technique	***Level of Security(P_1)***			***Capacity(P_2)***	***Fidelity(P_3)***	***Runtime Performance(P_4)***	
	k_1	***k_2***	***k_3***		***k_4***	***k_5***	***k_6***
LSBR(randomized)	A	1	0.0022	1 *bpp*	52.67	Spatial	2
OPAP(3 bit)	A,B	1	0.6071	3 *bpp*	37		1
PVD (t=3)†	A,B,C*	1	0.5011	3 *bpp*	38.18		2
PVD (t=4)	A,B,C*	1	0.6075	4 *bpp*	36.17		2
JSteg	A,B*	1	0.0022	0.5 *bpnc*	60	Transform	1
OutGuess	A,B	1	0.003	0.4 *bpnc*	50		2
F5	A,B,C*	3.8	0.0047	0.8 *bpnc*	49.1		2
† : *k* is the number of bits per pixel embedded							

Table 12. Evaluation Score Sheet

Technique	***Level of Security(P_1)***			***Capacity(P_2)***	***Fidelity(P_3)***	***Runtime Performance(P_4)***		***Overall Score (out of 20)***
	k_1	*k_2*	*k_3*		*k_4*	*k_5*	*k_6*	
LSBR(randomized)	1	1	3	1	2.63	2	2	12.63
OPAP(3 bit)	2	1	1	2	1.6	2	3	12.6
PVD (*t*=3)†	2.5	1	1	2	1.94	2	2	12.44
PVD (*t*=4)	2.	1	1	3	1.85	2	2	**13.35***

	5							
JSteg	1.5	1	3	2	3	1	3	14.5
OutGuess	2	1	3	2	2.5	1	3	14.5
F5	2.5	3	3	3	2.45	1	2	**16.95***
ℸ: t is the number of bits per pixel embedded. *: Figures in bold indicate the highest scores per domain								

6. Features of the Proposed System

The chief features of the proposed quality evaluation system are as follows:

a. Simplicity: The proposed evaluation system uses rating scales for each of the parameters under consideration to assign numeric weights for score calculation. The rating criteria are clearly defined and hence it is easy to use and simple.

b. Efficiency: The scores evaluated using the proposed system has been shown in Table 12. The performance scores generated by the system to mostly conform to the actual performance of the image steganography techniques in the literatures. Thus, the system is efficient in generating scores which can be well used for almost accurate performance analysis of image steganography techniques.

c. Flexibility: One of the important features of the proposed system is that new parameters can be incorporated into the existing system without much difficulty. The process is simple and needs no modification of the score calculation procedure for the inclusion of any new parameter. The parameter inclusion procedure is as follows:

Let $\boldsymbol{X}$ be a new parameter to be included in the system which already has other parameters and the maximum obtainable score is *K*. Also, suppose $\boldsymbol{X}$ has *n* sub-parameters $\boldsymbol{S_i}$ where $n \in \mathbb{Z}^+$. The rating scale for each $\boldsymbol{S_i}$ is prepared following the discussion in section 4.3. If the maximum scale value attained by each $\boldsymbol{S_i}$ be x_i then the maximum score obtainable for *X* is given by $\sum x_i$. Thus, the new maximum score is as follows:

$$Score_{max} = K + \sum_{n} x_i \tag{8}$$

where *K* is the previous maximum obtainable scores (Table 12). If *X* does not have sub-parameters, an appropriate rating scale is assigned to it directly and if *M* is the maximum score according to the scale, then

$$Score_{max} = K + M \tag{9}$$

The score generation for any image steganography technique can be now done as usual. Hence, the proposed system is flexible in the sense that extending the existing system to incorporate new parameters and its subsequent use for the evaluation of image steganography techniques is simple and easy to perform.

7. Conclusion

This chapter proposes a quality evaluation model for the quantitative evaluation of image steganography techniques. The need of such a model arises from the fact that there are numerous image steganography techniques available in literature and they are equally

varied in implementation thus, it is necessary to have a way to grading them according to some quantitative performance measure. The model proposed here is a rating scale based evaluation system whose ratings are derived from experimental data and observational heuristics.

The proposed model has been tested on various popular steganography techniques and their respective calculated overall scores have been observed to conform to performance characteristics of the techniques as available in the literature. The scores can also be used for segmented analysis of the techniques based on different parameters. It can also serve as a basis of choosing a particular steganography technique based on situational requirements.

The proposed evaluation system is simple, yet effective. The simplicity of the system lies in the fact that it is a rating scale based system which also makes it easily usable. It is effective as the performance analysis made on the basis of the scores generated by the system is seen to be at par with the actual literature. The performance evaluation system is flexible as new parameters may be added as required without affecting the score calculation technique. However, as the proposed quality evaluation model has a large heuristics contribution, hence it is important that inclusion of any new parameter into the existing system be dealt with care. Thus, any parameter which needs to be integrated into the system must be well experimented and studied prior to its inclusion so that the rating scales arising out of the observational heuristics of the parameter and the scores generated by the resulting system are optimally accurate.

References

[1] T. Morkel, J.H.P Eloff, M.S Olivier, "An Overview of Image Stenography", Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), **(2005)**. Source: http://mo.co.za/open/stegoverview.pdf. Last Access: January 2014.
[2] B. Pitzmann, "Information hiding terminology-results of an informal plenary meeting and additional proposals", Proc. of the First International Workshop on Information Hiding, Springer, **(1996)**, vol. 1174, pp.347-350.
[3] G. Simmons, "The prisoners problem and the subliminal channel", CRYPTO, (**1983)**, pp. 51-67,
[4] Mehdi Kharrazi, Husrev T. Sencar, Nasir Memon, "Image Steganography: Concepts and Practice", WPSC/Lecture Note Series, **(2004)**. Source: www2.ims.nus.edu.sg/preprints/ab2004-25.pdf. Last Access: May 2013.
[5] Bin Li, Junhui He, Jiwu Huang, Yun Qing Shi, "A Survey on Image Steganography and Steganalysis", Journal of Information Hiding and Multimedia Signal Processing, Vol.2, Issue 2, **(2011),** pp. 142-172,.
[6] Ratnakirti Roy, Suvamoy Changder, Anirban Sarkar, Narayan C Debnath, "Evaluating Image Steganography Techniques: Future Research Challenges", International Conference on Computing, Management and Telecommunications (COMMANTEL 2013), Ho Chi Minh City, Vietnam, pp. 309-314, (**2013)**.
[7] Neil F. Johnson, Stefan C. Katzenbeisser, "A Survey of Steganographic Techniques", Information Hiding Techniques for Steganography and Watermarking, edited by Stefan Katzenbeisser and Fabien A.P. Petitcolas, pp. 45, Artech House Inc, (**2000)**.
[8] Mehdi Kharrazi, Husrev T. Sencar, Nasir Memon, "Image Steganography: Concepts and Practice", WPSC/Lecture Note Series, pp. 3, April, (**2004)**. Source: www2.ims.nus.edu.sg/preprints/ab2004-25.pdf.Last Access: May 2013.
[9] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding", IBM System Journal, vol. 35, no. 3, **(1996)**, pp. 313-336.
[10] R. Chandramouli, Nasir Memon, "Analysis of LSB based Image Steganography Techniques", Proc. International Conference on Image Processing, 2001, Vol. 3, **(2001)**, pp. 1019-1022.
[11] Chi-Kwong Chan, L.M. Cheng, "Improved hiding data in images by optimal moderately signifcant-bit replacement", IEE ElectronLett. Vol. 37, No. 16, **(2001)** ,pp. 1017–1018.
[12] Chi-Kwong Chan, L.M. Cheng, "Hiding data in images by simple LSB substitution", Pattern Recognition, Vol.37, **(2010)**, pp. 469-474.
[13] R.-Z. Wang, C.-F. Lin and J.-C. Lin, "Hiding data in images by optiinal moderately-significant-bit replacement", IEEElectron. Lett., vol. 36, no. 25, **(2000)**, pp. 2069-2070.
[14] R. Amritharajan, R. Akila, P. Deepikachowdavarapu, "A Comparative Analysis of Image Steganography", International Journal of Computer Applications, vol. 2, no.3, **(2010)**, pp. 41-47.
[15] Adnan Abdul-Aziz Gutub, "Pixel Indicator Technique for RGB Image Steganography", Journal of Emerging Technologies in Web Intelligence, vol 2, no. 1, **(2010)**, pp. 56-64.

[16] D. C. Wu and W. H. Tsai, "A steganographic method for images by pixel-value differencing," Pattern Recognition Letters, vol. 24, no. 9-10, **(2003)**, pp. 1613–1626.
[17] C.M. Wang, N.I. Wu, C.S. Tsai, M.S. Hwang, "A high quality steganography method with pixel-value differencing and modulus function", J. Syst. Software Vol. 81, No. 1, **(2008)**, pp. 150-158.
[18] Young-Ran Park, Hyun-Ho Kang, Sang-Uk Shin, and Ki-Ryong Kwon, "An Image Steganography Using Pixel Characteristics", Y.Hao *et al.*(Eds.): CIS 2005, Part II, Springer-Verlag Berlin Heidelberg LNAI 3802, **(2005)**, pp. 581– 588.
[19] V. Sabeti, S. Samavi, M. Mahdavi, S. Shirani, "Steganalysis of Pixel-Value Differencing Steganographic Method", Proc. IEEE PacificRim Conference on Communications, Computers and Signal Processing, **(2007)**, pp. 292-295.
[20] J. J. Roque, J. M. Minguet, "SLSB: Improving theSteganographic Algorithm LSB", Universidad Nacional de Educación a Distancia (Spain). Source:http://www.fing.edu.uy/inco/eventos/cibsi09/docs/Papers/CIBSI-Dia3-Sesion9(1).pdf.Last Access: January 2013.
[21] N.Provos, P.Honeyman, "Hide and seek:an introduction to steganography", IEEE Security and Privacy, vol. 1, no. 3, **(2003)**, pp. 32–44.
[22] A. Cheddad, J. Condell, K. Curran and P. Mc Kevitt, "Digital Image Steganography: Survey and Analyses of Current Methods", Signal Processing, vol. 90, no. 3, **(2010)**, pp. 727-752.
[23] A. Westfeld, "F5-A Steganographic Algorithm: High capacity despite better steganalysis," Proc. 4th International Workshop on Information Hiding, vol. 2137, **(2001)**, pp. 289-302.
[24] Jessica Fridrich, Miroslav Goljan, Dorin Hogea, "Attacking the OutGuess", Proc. of 2002 ACM Workshop on Multimedia and Security, ACM Press, **(2002)**, pp. 3-6.
[25] Ron Crandall, "Some Notes on Steganography", Posted on Steganography Mailing List, **(1998)**. Source: http://www.dia.unisa.it/~ads/corso-security/www/CORSO-0203/steganografia/LINKS%20LOCALI/matrix-encoding.pdf. Last Access: April 2013.
[26] Jessica Fridrich, Miroslav Goljan, Dorin Hogea, "Steganalysis of JPEG Images: Breaking the F5 Algorithm",Proc. of the 5th Information Hiding Workshop, Springer, vol. 2578, **(2002)**, pp. 310-323.
[27] K S. Babu, K B Raja, U. M. Rao, Rashmi K A, Venugopal K R, L M Patnaik, "Robust and High Capacity Image Steganography using SVD",IET-UK International Conference on Information and Communication Technology in Electrical Sciences, **(2007)**, pp. 718-723.
[28] Ingemar J. Cox *et al.*, Digital Watermarking and Steganography, pp.36-41, Second Edition, Morgan Kaufmann, Burlington, USA, 2008.
[29] J. Zollner, H. Federrath, H. Klimant, A. Pitzman, R. Piotraschke, A. Westfeld, G. Wicke, and G. Wolf, "Modeling the security of steganographic systems," 2nd Information Hiding Workshop, **(1998)**, pp. 345-355.
[30] C. Cachin, "An information-theoretic model for steganography," Proc. 2nd International Workshop Information Hiding LNCS 1525, **(1998)**, pp. 306–318.
[31] Jessica Fridrich, Tomáš Pevný, Jan Kodovský, "Statistically Undetectable JPEG Steganography: Dead Ends, Challenges and Opportunities", Proc. 9th Workshop on Multimedia and Security, **(2007)**; ACM, New York, USA.
[32] C.V. Serdean, M. Tomlinson, J. Wade, A.M. Ambroze, "Protecting Intellectual Rights: Digital Watermarking in the wavelet domain", IEEE Int. Workshop Trends and Recent Achievements in IT, **(2002)**, pp. 16-18.

