Available online at www.sciencedirect.com
ScienceDirect
journal homepage: www.elsevier.com/locate/cosrev

Current status and key issues in image steganography: A survey

Mansi S. Subhedar[a,*], *Vijay H. Mankar*[b]

[a] *Research Scholar, Department of Electronics & Telecommunication, Bapurao Deshmukh College of Engineering, Sevagram, Wardha, 442102, Maharashtra, India*
[b] *Department of Electronics & Telecommunication, Government Polytechnic, Nagpur, 440001, Maharashtra, India*

ARTICLE INFO

Article history:
Received 5 October 2013
Accepted 11 September 2014

Keywords:
Information hiding
Image steganography
Steganalysis
Image quality measures

ABSTRACT

Steganography and steganalysis are the prominent research fields in information hiding paradigm. Steganography is the science of invisible communication while steganalysis is the detection of steganography. Steganography means "covered writing" that hides the existence of the message itself. Digital steganography provides potential for private and secure communication that has become the necessity of most of the applications in today's world. Various multimedia carriers such as audio, text, video, image can act as cover media to carry secret information. In this paper, we have focused only on image steganography. This article provides a review of fundamental concepts, evaluation measures and security aspects of steganography system, various spatial and transform domain embedding schemes. In addition, image quality metrics that can be used for evaluation of stego images and cover selection measures that provide additional security to embedding scheme are also highlighted. Current research trends and directions to improve on existing methods are suggested.

1. Introduction

The word steganography is obtained from the Greek words "stegos" means "cover" and "grafia" means "writing", defining it as "covered writing". Usually secure communication is achieved by the method of encryption. But nowadays, demand for security is increasing day by day that leads to the use of steganography for information security. The idea of data hiding or steganography was first introduced with the example of prisoner's secret message by Simmons in 1983 [1–3]. Fig. 1 shows various disciplines of information hiding.

Steganography and cryptography are closely related concepts. Though both the terms share a common goal, the way and the usage of both differ significantly. Steganography is hidden writing where as cryptography is secret writing i.e. cryptography provides security with respect to content of the message whereas steganography will hide the existence of the message itself. Digital watermarking is another branch of information hiding. Both steganography and watermarking are the methods of data embedding, but there are several differences among them. A detailed comparison can be found in [4–7]. A variety of multimedia carriers that includes

[*] *Corresponding author.* Tel.: +91 9867967304.
E-mail addresses: mansi_subhedar@rediffmail.com, msubhedar@mes.ac.in (M.S. Subhedar), vhmankar@gmail.com (V.H. Mankar).

http://dx.doi.org/10.1016/j.cosrev.2014.09.001
1574-0137/© 2014 Elsevier Inc. All rights reserved.

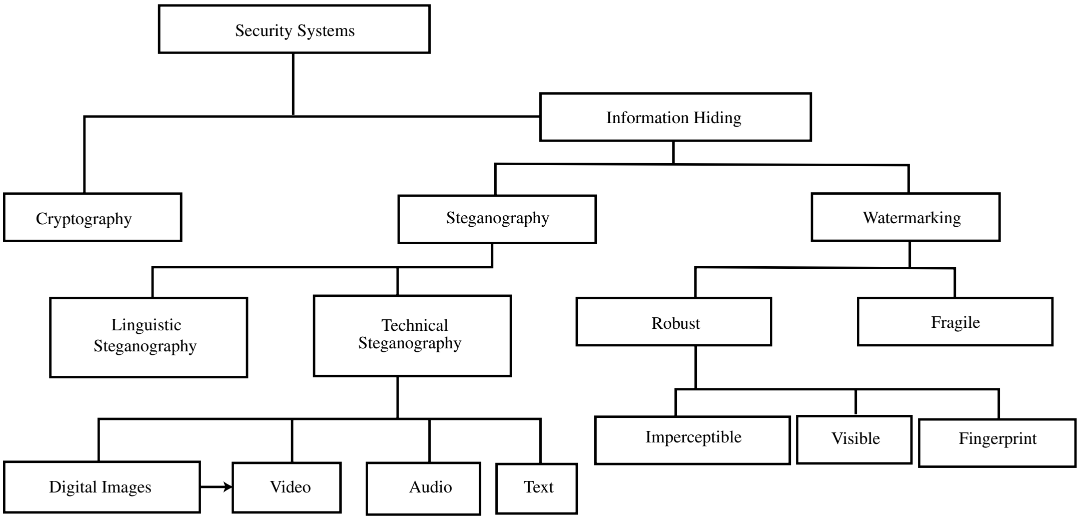


Fig. 1 – Disciplines of information hiding [4].

text, audio, video, image can be used for steganography. Some of the ways to achieve text steganography involve modification of text layout, use of *n*th character from text or alteration of some of the rules such as spaces etc. Another approach includes usage of a code consisting of combination of character, line and page numbers. However, this technique lacks in security. Hiding information in audio files can be done by using frequencies that are inaudible to human ear. Similarly, video files can also be thought of to embed secret information. Since it is a moving stream of images and sounds, any minor distortions may be unseen because of continuous flow of information. The advantage in this case will be high payload capacity. Image is the most popular file format used for steganography as they possesses high degree of redundancy. With image steganography, better imperceptibility and payload capacity can be achieved. Steganalysis is an art of detecting covert communication [8]. In this paper, we focus only on image steganography with little more emphasis on transform domain steganography.

1.1. *Fundamental concepts*

Cover image refers to the image used for carrying the embedded bits, embedded data is known as *payload* and the image with embedded data is called as *stego image*. *Steganalysis* refers to the attack on steganography. The distortion induced on the host signal by the data embedding process is called the *embedding distortion*.

Imperceptibility is innocuousness of the stego image. Stego image should not have severe visual artifacts. Some of the major requirements of steganography include capacity, robustness and security. *Robustness* indicates the amount of modification that the stego medium can withstand before an adversary can destroy hidden information. *Capacity* refers to the amount of information that can be hidden in cover medium without deteriorating the integrity of the cover image. It is represented in terms of bits per pixel (bpp). Embedding operation needs to preserve the statistical properties of the cover image in addition to the perceptual quality.

Security means eavesdropper's inability to detect hidden information. *Perceptual transparency* ensures the retention of the visual quality of the cover after data embedding. *Tamper resistance* means to remain intact in the face of malicious attacks. The *embedding rate* is measured as the number of embedded bits per carrier bit. The *embedding efficiency* is given by the expected number of embedded message bits per modified carrier bit. The *change rate* gives the average percentage of modified carrier bits.

1.2. *General model of steganography*

The concept of steganography is usually modeled by prisoner's problem. Fig. 2 exhibits the overall structure for the steganography system. Let 'C' denotes the cover medium i.e. image *A* and C' be the stego image obtained by data embedding. Let 'K' represents an optional key and 'M' is the message we want to communicate. E_m suggests the embedding process and E_x is for the process of extraction. Compression and encryption eliminate the redundancy in secret message and result in enhanced security. Thus, data embedding process can be represented as follows:

$$E_m : C \oplus K \oplus M \rightarrow C'$$
$$E_x\left(E_m\left(c, k, m\right)\right) \approx m, \quad \forall c \in C, k \in K, m \in M. \tag{1}$$

Image is the most often used file format for steganography and is only discussed here where the secret message is embedded in cover image. Applications of steganography include copyright control of materials, enhancing robustness of image search engines and smart id's, feature tagging, secret communication, video-audio synchronization, TV broadcasting, TCP/IP packets etc. [10,11]. Image quality measures are used for the evaluation of stego image quality obtained after embedding. Different methods exist for attacking the steganographic algorithm. The number of steganography tools are available that includes Ezstego, F5, Hide and Seek, Hide4PGP, Mp3Stego, OutGuess, StegHide, Stegnos, S-tools etc. Various forms of steganalysis include identifying the existence of secret message and finding its

Please cite this article in press as: M.S. Subhedar, V.H. Mankar, Current status and key issues in image steganography: A survey, Computer Science Review (2014), http://dx.doi.org/10.1016/j.cosrev.2014.09.001

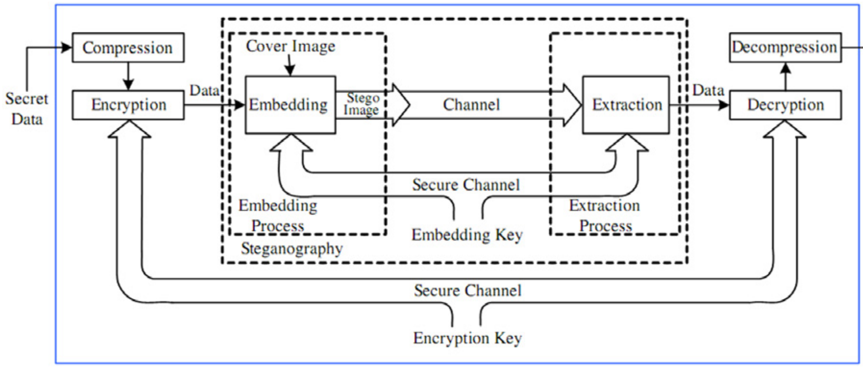


Fig. 2 – General model of steganography [9].

approximate length or even trying to retrieve it. Various stego attacks include image resizing attack, image tampering attack, AWGN attack, JPEG compression attack, RS attack, filter attack, chi square attack, J. Fridrich's RS steganalysis, Jeremiah J. Harmsena's Histogram attack etc. The algorithm used for data embedding should withstand against all these types of attacks making eavesdropper unable to retain the hidden message.

Survey reports presented till now [7,10–12] explored various fundamental issues in steganography, spatial domain and transform domain approaches for data hiding, steganalysis techniques etc. However, there are many unattended areas that considerably influence image steganography. This paper focuses mainly on such areas e.g. security aspects of steganography system, cover selection measures and IQM analysis.

The outline of the paper is as follows: Section 2 discusses performance evaluation measures and security aspects. Section 3 presents overview of various image steganography techniques. Image quality measures and cover selection criteria are illustrated in Sections 4 and 5 respectively. Section 6 concludes the paper.

2. Performance evaluation measures

In literature, many steganography schemes are presented based on variety of parameters. Some of them work in spatial domain and other in transform domain. Irrespective of the approach used for data embedding, some common attributes need to be defined to achieve uniqueness in performance rating. Some of them can be defined as follow:

Security against attack: The steganographic system may suffer from different types of stego attacks, allowing eavesdropper to retrieve secret message bits embedded in cover media. The system is said to be γ—secure if $TP\ Rate - FP\ Rate \leq \gamma$, where $0 \leq \gamma \leq 1$. And is said to be perfectly secure if $\gamma = 0$.

$$TP\ Rate = \frac{TP_S}{TP_S + FN_S}, \qquad FP\ Rate = \frac{FP_S}{TN_S + FP_S} \tag{2}$$

where, TP (True positive): a stego medium is correctly classified as stego, FN (False Negative): a stego medium is wrongly classified as cover, TN (True Negative): a cover medium is correctly classified as cover, FP (False Positive): a cover medium is wrongly classified as stego.

Payload capacity: It is defined in terms of number of secret bits that can be embedded per pixel. Ideally it should be as high as possible while maintaining the acceptable quality of the stego image. It is also known as hiding capacity or embedding capacity and is measured in terms of bits per pixel or bits per transform coefficient (for spatial and transform domain approach respectively).

Imperceptibility: Steganography system should have high embedding capacity and capability to withstand against stego attacks. The stego image should not have severe visual artifacts. Higher the fidelity of the stego image, the better.

2.1. *Steganographic security*

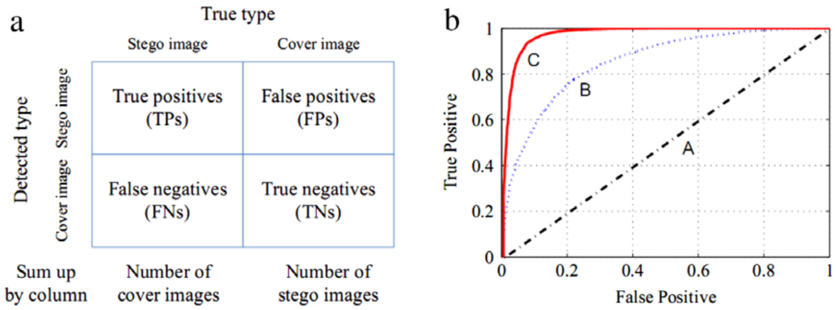
Security is always the important criterion while designing any application. There are numerous ways to define security of steganography system e.g.

Maximum mean discrepancy (MMD) security: With advances in steganography algorithms and methods to detect them, issue of comparing them with a fair benchmark is a critical task. The task of identifying the differences between cover and stego image is a two sample problem that can be solved using MMD. It finds the discrepancy between pdf of cover and stego objects. It is given by,

$$MMD\,(F, X, Y) \triangleq \sup_{f \in F} \left(\frac{1}{D} \sum_{i=1}^{D} f(x_i) - \frac{1}{D} \sum_{i=1}^{D} f(y_i) \right) \tag{3}$$

where $X = x_1, x_2, \ldots, x_D$ and $Y = y_1, y_2, \ldots, y_D$ are the samples from probability distributions P_x and P_y respectively. f is a class of function which is built from symmetric, positive definite function.
Advantages of MMD include numerical stability, well scaled with data dimensionality and converge independently on data dimension d with error $\frac{1}{\sqrt{D}}$,

Please cite this article in press as: M.S. Subhedar, V.H. Mankar, Current status and key issues in image steganography: A survey, Computer Science Review (2014), http://dx.doi.org/10.1016/j.cosrev.2014.09.001



		True type	
		Stego image	Cover image
Detected type	Stego image	True positives (TPs)	False positives (FPs)
	Cover image	False negatives (FNs)	True negatives (TNs)
Sum up by column		Number of cover images	Number of stego images

Fig. 3 – (a) Confusion matrix (b) ROC curve.

where D is the number of samples [13]. Also, MMD's computational complexity is $O\left(D^2\right)$, that is faster than support vector machines (SVM).

ROC based security: Another way to quantify security is with reference to ROC. As shown in Fig. 3, it is the plot of false positive rate versus true positive rate [6,14]. The true positive rate is plotted on Y axis and false positive rate on X axis. Larger the area under the curve, better the performance of the steganalytic system e.g. performance of curve C is better than B, and that of B is better than A. Eq. (2) describes one of the conditions to be satisfied for the secure system.

Correlation coefficient: The correlation coefficient between two adjacent elements C_i and C_{i+1} is ρ and the correlation coefficient between two arbitrary elements C_i and C_j is $\rho^{|j-i|}$. The bigger the ρ, the stronger the correlation. Security will be improved if selected cover image is with smaller ρ [15–17]. In statistics, Bhattacharya distance measures the similarity between two discrete or continuous probability distributions and is denoted by $DB(P_c, P_s)$. Smaller the ρ, smaller the $DB(P_c, P_s)$ when $\rho \in [0, 1]$. BD between P_c and P_s is defined as,

$$BD\left(P_c, P_s\right) = \frac{1}{2}\ln\left(\frac{\det(R)}{\sqrt{\det(R_c)\det(R_s)}}\right) \tag{4}$$

where P_c is probability distribution of cover image, R_c is covariance matrix, σ_c^2 is the variance of marginal distribution and ρ is the parameter representing the degree of cover data dependency.

Kullback–Leibler (K–L) divergence: KL divergence is also one of popular security measures to analyze the steganography system. It has been proposed by Cachin in 1998 [17]. Let X and Y represent cover and stego image and p_x and q_y denote the probability distribution function of X and Y respectively. KL divergence between two probability distribution functions is given by,

$$D\left(p_x \parallel q_y\right) = \sum_{g\in G} p_x(g)\log\frac{p_x(g)}{q_y(g)} \tag{5}$$

where $g \in G = \{0, 1, 2, \ldots, 255\}$ is the pixel value in gray scale images. The embedding algorithm should be designed so as to get minimum value of KL divergence which justifies the security. The bigger the correlation parameter ρ, KL divergence is larger.

3. Image steganography

Image steganography can be broadly classified into spatial domain, transform domain, spread spectrum and model based steganography as depicted in Fig. 4. In spatial domain, secret message is embedded in pixel value directly whereas transform domain methods achieve embedding by first transforming the image from spatial to frequency domain using any one of the transforms such as discrete cosine transform (DCT), discrete wavelet transform (DWT), Hadamard transform, Dual tree DWT, double density dual tree DWT (DD DT DWT), ridgelet transform, curvelet transform etc. and then embedding is done in suitable transform coefficients.

This section deals in detail with each of these methods. Various techniques can be employed to optimally choose the transform coefficients to hide data in. Soft computing tools can be considered for this purpose. As transform domain methods are more immune to image processing operations and are less susceptible to stego attacks, they are usually preferred over spatial domain methods.

Spread spectrum steganography involves embedding in noise inherent to image acquisition process. Image restoration and error control techniques can be used while extracting the data at the decoder side. It is a blind scheme as original image is not required while extraction. This method outperforms in terms of payload capacity and invisibility. Model based steganography is based on statistical model of the cover image. It is also known as statistics aware embedding. Before selecting the locations for data hiding in cover image, statistical global features of image are taken into account and then actual data embedding process is carried out accordingly. Thus, it provides additional layer of security to steganography. All these methods are discussed in detail in forthcoming subsections.

3.1. *Spatial domain steganography*

In this method, the pixel value is directly modified for data hiding. The various approaches to achieve embedding in spatial domain are shown in the Fig. 5.

Please cite this article in press as: M.S. Subhedar, V.H. Mankar, Current status and key issues in image steganography: A survey, Computer Science Review (2014), http://dx.doi.org/10.1016/j.cosrev.2014.09.001

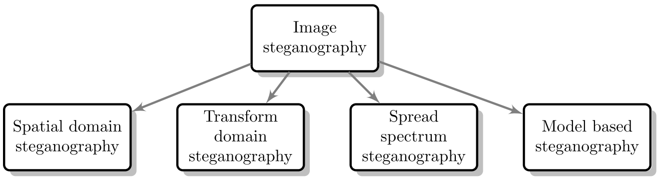


Image steganography
Spatial domain steganography
Transform domain steganography
Spread spectrum steganography
Model based steganography

Fig. 4 – Image steganography techniques.

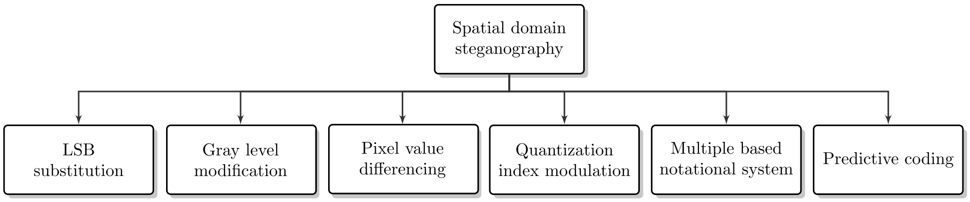

Spatial domain steganography
LSB substitution
Gray level modification
Pixel value differencing
Quantization index modulation
Multiple based notational system
Predictive coding

Fig. 5 – Spatial domain steganography techniques.

3.1.1. *Least significant bit (LSB) substitution*

Embedding can be achieved by simply replacing LSB of the randomly selected pixel in the cover image with the secret message bit. Let P_i is the pixel value of an image. It can be expressed in binary form as follows:

$$P_i = (b_7b_6b_5b_4b_3b_2b_1b_0)^2 = \sum_{n=0}^{7} b_n \, X \, 2^n \qquad (6)$$

where b_7 is MSB and b_0 is LSB. LSB substitution method usually does not lead to increase in the file size, but depending on the size of the information that is to be hidden, the file can become noticeably distorted. Many steganographic tools based on LSB substitution data hiding are available e.g. StegHide, S tool, Stegnos etc. [18]. In literature, a variety of LSB based steganography approaches are discussed. Some of them include Adaptive LSB substitution based on brightness, edges and texture masking of the host image to estimate the number k of LSBs for data hiding [19], loss less generalized LSB data embedding [20], optimized LSB substitution using cat swarm strategy and genetic algorithm [21,22], data hiding based on histogram modification [23,24] etc. Ramaiya et al. developed a spatial domain steganography scheme based on DES using S box mapping and secret key. The scheme is more secure as unintended recipient will not be able to extract secret message as information about mapping functions and secret key will not be available [25]. Simplicity and high perceptual efficiency are the advantages of this method. Though it achieves high capacity, LSB insertion is vulnerable to slight image manipulations such as scaling, rotation, cropping and addition of noise or lossy compression. Also, it is easily detectable by any of the stego attacks.

Multi bit plane steganography: This method was investigated in 2006 [26] presenting an extension to the simple LSB replacement technique. Secret message bits are hidden in multiple bit planes. Generally it is followed for uncompressed images and provides security against classical stego attacks like RS attack. Several adaptive versions of traditional LSB substitution method are also presented e.g. in [27], Kawaguchi presented bit plane complexity segmentation (BPCS) method where canonical gray coding (CGC) concept is used. This scheme achieves payload of 4 bits per pixel and good visual quality.

But one major defect with multi bit plane steganography is that non adaptive embedding manner may reduce the perceptual quality of the stego image if some of the high bit planes are involved in embedding arbitrarily without considering the local properties.

3.1.2. *Gray level modification*

It was put forward by Potdar et al. in 2004 [28]. This technique is used to map data by modifying the gray levels of pixels (not embed or hide it). Based on some mathematical function, a set of pixels is selected for mapping. This technique uses the concept of odd and even numbers to map data within a cover image e.g. 1 is mapped with odd value and 0 is mapped with even values. Advantages of this method include low computational complexity and high information hiding capacity.

3.1.3. *Pixel value differencing (PVD)*

Wu and Tsai demonstrated a novel embedding concept based on difference between pixel values [29]. Cover image is divided into non overlapping blocks containing two connecting pixels and the difference in each block is modified. A larger difference in original pixel value allows a greater modification. Number of secret bits that can be embedded depends on whether the pixel is in edge area or smooth area. In edge area, the difference between the adjacent pixels is more whereas in smooth area it is less. So, more data is embedded into pixels in the edge area than in the smooth area. As this scheme embeds data by modifying the difference value between two adjacent pixels rather than modifications in pixel values directly, it provides better results in terms of imperceptibility and stego image quality as compared to LSB replacement method of data hiding.

In order to provide secure communication and defeat statistical attacks, several approaches based on PVD are proposed e.g. PVD method vulnerable to histogram analysis [30], combination of PVD and modulus function to achieve data

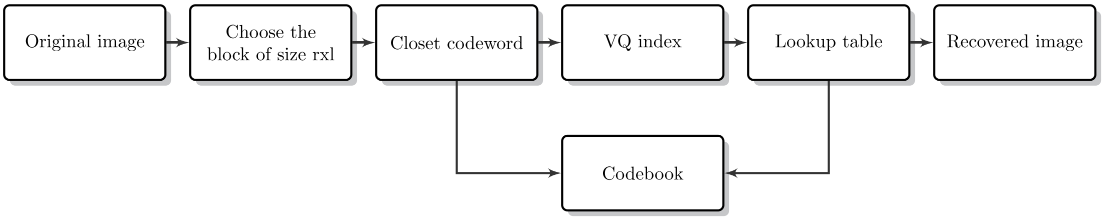


Fig. 6 – Vector quantization process.

hiding [31], varieties of PVD such as tri way PVD, four pixel PVD etc. [32–34]. Recently Liu et al. presented a novel idea in which embedding is carried out in adaptive manner depending on complexity of the pixel blocks. This complexity is computed by neighboring block difference [35]. Swain et al. demonstrates a scheme where two, three and four neighboring pixels are exploited for embedding decision. The author addresses full off boundary problem and fall in problem as well. For the payload of 20 480 bytes, PSNR of 45.3117 dB is achieved for four sided side match scheme [36].

Each tries to improve stego image quality and achieve high embedding capacity by making some modifications to original PVD method.

3.1.4. *Quantization index modulation (QIM)*

Quantization index modulation (QIM) [37] is one of the promising data embedding technique in digital watermarking and it can also be employed for steganography. QIM refers to embedding the information in cover medium by first modulating an index or sequence of indices with the embedded information and then quantizing the host signal with the associated quantizer or sequence of quantizers. QIM has high embedding capacity and it allows the embedder to control the robustness and the distortion induced while embedding. This technique is classified as a host interference rejection technique as it does not require the host signal at the decoder. Also, it is more robust than low bit(s) modulation (LBM) against various classes of attacks. It quantizes the input signal X to the output Y with a set of quantizers $Q_m(\cdot)$. Fig. 6 depicts the process of vector quantization. Vector quantization is popular compression standard which involves two important phases i.e. codebook generation and encoding–decoding process. Embedding techniques based on vector quantization are published in literature. Chung et al. presented a novel data embedding technique based on singular value decomposition (SVD) and vector quantization. It results in good compression ratio and better image quality [38]. A lossless data hiding algorithm that uses side match vector quantization (SMVQ) and search order coding (SOC) is presented in [39] that achieves a compression rate of 0.325 bpp with codebook size of 256. A reversible data hiding scheme for VQ indices is explained in [40] that outperforms many schemes such as Lin and Chang, Tsai and Yang and Lin's method giving the compression rate of 0.49 bpp.

3.1.5. *Multiple base notational system (MBNS)*

A system can be represented as a notational system with multiple bases to reexpress a secret message to be hidden. As the computer world is based on binary number system with base 2, in most of the cases the secret message is a binary stream and the amount of information contained in each symbol is exactly one bit. In order to embed more data in busy areas, the message can be expressed as an integer number using a variable base system. In other words, the message is converted into a series of symbols with different information carrying capabilities due to different bases used. The greater the base, the more information is contained in the corresponding symbol.

In MBNS steganography, secret data is converted into symbols in a notational system with multiple bases. The pixels of a host image are then modified such that when the pixel values are divided by the bases, their remainders are equal to the symbols. Xinpeng Zhang et al. proposed such kind of steganography method. The specific bases used are determined by the degree of local variation of the pixel magnitudes in the host image so that pixels in busy areas can potentially carry more hidden data. High payload capacity is achieved with this method. The results obtained by MBNS were compared with BPCS and PVD method and found to be superior in terms of PSNR, quality factor and Watson's metric [41].

Varying radix numeral system is proposed by Geetha et al. based on statistical model of host image. The developed system is resistant to RS steganalysis and provides high visual quality [42]. Kieu et al. proposed $2n + 1$ base system by EMD (exploiting modification direction) method [43]. This technique outperforms the methods proposed by Mielikainen, Zhang and Wang and Yang et al. etc. PVD based base selection is employed by Hong et al. along with diamond encoding to achieve better results in terms of payload capacity and image quality [44]. Another approach proposed by Chang et al. uses combination of MBNS and VQ and compared the results with SMVQ [39].

3.1.6. *Prediction based steganography*

Embedding by altering the pixel values directly leads to significant distortion in stego image resulting in less hiding capacity and poor visual quality. To overcome this issue, predictive coding approach is suggested where pixel values are predicted using predictor and instead of altering the pixel values, prediction error values (EV) are modified to embed secret data. According to international standards for lossless and near lossless image compression, the compression procedure is often composed of two separate steps: prediction and entropy coding of prediction EVs. Predictive rule can be stated as,

$$X' = \begin{cases} \min(a, b), & \text{if } c \geq \max(a, b); \\ \max(a, b), & \text{if } c \leq \min(a, b); \\ a + b - c, & \text{otherwise.} \end{cases}$$

Please cite this article in press as: M.S. Subhedar, V.H. Mankar, Current status and key issues in image steganography: A survey, Computer Science Review (2014), http://dx.doi.org/10.1016/j.cosrev.2014.09.001

Table 1 – Comparison of different reversible data hiding schemes.

Reversible data hiding scheme	Embedding capacity of 512 × 512 gray scale image	Percentage of embedding capacity
Wu et al. [45]	250k–256k	97.68–99.85
Honsinger et al. [46]	<1024	<0.39
Macq and Deweyand [47]	<2046	<0.78
Fridrich et al. [48]	1024	0.39
Goljan et al. [49]	3k–4k	1.17–1.56
Vleeschouwer et al. [50]	<4096	<1.56
Xuan et al. [51]	5k–49k	5.86–36.72
Celik et al. [52]	15k–143k	0.005–55.86
Ni et al. [53]	5k–80k	1.95–31.25

The prediction step usually employs a predictor to estimate the pixel values of an input image. Then the prediction EV is compressed by an entropy coder. The gradient adjusted prediction (GAP) and the median edge detector (MED) are the state of-the-art predictors used in prediction based image coding schemes. Various reversible prediction based data hiding methods are presented in literature. Each tries to improve on existing techniques. Reversible data hiding methods are able to have lossless data recovery that cannot be obtained in irreversible methods. So user prefers to employ reversible schemes. Table 1 shows a review of nine reversible data hiding schemes in terms of payload capacity. A scheme proposed by Wu et al. [45] based on hiding tree proved superior by achieving almost 99.85% embedding capacity.

Though, spatial domain steganography schemes achieve high embedding capacities they are vulnerable to any small modifications that may result due to image processing operations such as cropping, rotation, scaling etc. Also, these methods compensate the statistical properties of image indicating poor robustness against lossy compression and image filters. So, we can prefer transform domain steganography. Subsection below gives an overview of transform domain steganography.

3.2. *Transform domain steganography*

Any digital image is combination of low and high frequency components. The smooth and plane areas represent low frequency content whereas the edges and sharp transitions contribute significantly to the high frequency components. Low frequency regions are more sensitive as any change in them will be transparent to human visual system (HVS). Hence, it is not feasible to hide an equal amount of information in both high and low frequency regions. Also, pixel in low frequency region is strongly correlated with its neighbors whereas in high frequency region it greatly deviates from its neighbors. With this, we can conclude that obtaining and analyzing the image in frequency domain will greatly help to achieve efficient data embedding. It has been observed that transform domain schemes are less prone to attacks.

To obtain the frequency domain representation, image transforms are used and are designed to possess two main properties: (a) Reduce image redundancy (b) Identify less important parts of image by isolating various frequencies in image. Frequency domain representation depicts that low frequencies correspond to significant image features and high frequencies represent less important image details. Usually linear transforms are used for faster operations and easy implementations. In general, the structure for transform domain steganography can be illustrated as shown in Fig. 7. Image that can be used to carry secret information i.e. cover image is taken as an input. Cover image decomposition can be obtained by forward (choose appropriate type of transform as per the nature of application) transform to obtain transform coefficients. These transform coefficients can be altered to hide secret data. With the help of desired embedding algorithm, secret data can be embedded in suitable transform coefficients. Now, apply inverse transform to derive stego image. For extraction, similar steps can be performed to recover cover image and secret data.

Various image transforms that can be employed for data embedding include DCT, DWT, Haar transform, Hadamard transform, integer transform, contour let transform, DD DT DWT, Ridgelet transform, Ripplet transform etc. Not only the choice of transform but also the optimal data embedding locations affect the performance of the steganography system. Soft computing tools such as optimization algorithms, neural networks, fuzzy logic, hybrid networks etc. can be applied to improve embedding efficiency and perceptual quality.

3.2.1. *DCT based steganography*

JPEG is of great interest nowadays and widely used file format on internet. JPEG uses DCT for spatial to transform domain conversion. Significance of DCT is that it takes correlated input data and concentrates its energy in first few transform coefficients. Image compression is based on two dimensional correlation of pixels (a pixel tends to resemble all its near neighbors not just those in its row), so we use 2D DCT. Given a two dimensional $N \times N$ image $f(x, y)$, it's discrete cosine transform $C(u, v)$ is defined as,

$$C(u,v) = \alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cos\left[\frac{(2x+1)u\pi}{2N}\right] \times \cos\left[\frac{(2y+1)v\pi}{2N}\right] \quad (7)$$

where

$$\alpha(u) = \begin{cases} \frac{\sqrt{1}}{N}, & \text{for } u = 0; \\ \frac{\sqrt{2}}{N}, & \text{for } u = 1, 2, \ldots, N-1. \end{cases}$$

Fig. 8 shows the JPEG based steganography. Cover image is divided into a set of 8 × 8 non overlapping blocks. 2D DCT

Please cite this article in press as: M.S. Subhedar, V.H. Mankar, Current status and key issues in image steganography: A survey, Computer Science Review (2014), http://dx.doi.org/10.1016/j.cosrev.2014.09.001

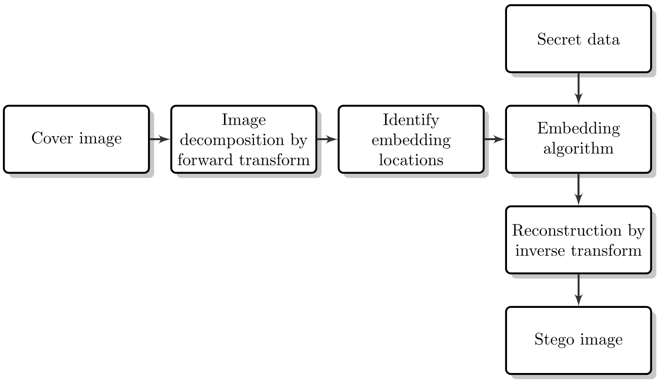

Secret data
Cover image
Image decomposition by forward transform
Identify embedding locations
Embedding algorithm
Reconstruction by inverse transform
Stego image

Fig. 7 – General model of transform domain image steganography.

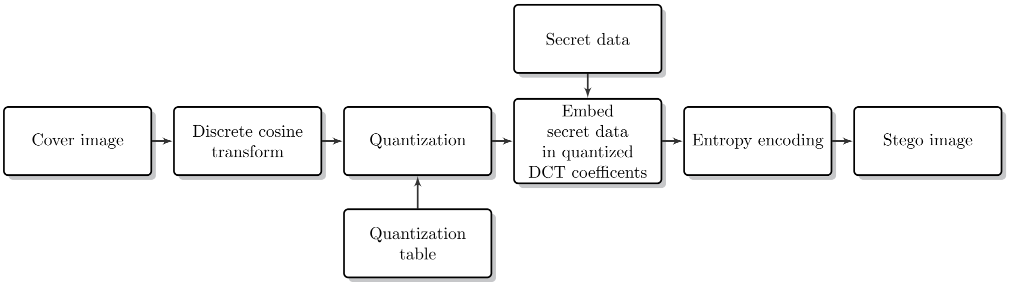


Fig. 8 – JPEG based steganograpy.

is applied on each block. The DCT coefficients are quantized according to default quantization table of JPEG. Secret message bits are embedded in quantized DCT coefficients which are then coded by using combination of run length coding and Huffman coding. The frequency distribution in DCT block reveals that high frequency components can be the better places for data hiding as they often become zero after quantization and hence there is no need to alter the coefficient value if the data to be embedded is zero. High frequency components are more visually resistant to noise than low frequency components. Here, we review some major steganography tools based on DCT:

Jsteg/JPHide:

1. Steganographic tool based on LSB embedding.
2. Embedding is done by replacing LSBs of non-zero quantized DCT coefficients by secret message bits.
3. In JPHide, these quantized coefficients are selected at random with the help of any pseudorandom number generator that can be controlled by a key.
4. Second LSB can also be modified in JPHide.
5. Capacity of Jsteg is equal to number of DCT coefficients whose values are not equal to 0, 1, −1 (this condition is selected so as to avoid ambiguity in secret bit extraction) [54,55].

YASS (Yet another steganographic scheme):

1. Input image in spatial domain is divided into the blocks of fixed size known as big blocks (B blocks). Within each big block, 8 × 8 sub block called host block (H blocks) is selected randomly.
2. Secret message bits are embedded in DCT coefficients of H block by QIM.
3. With the help of IDCT of H block, JPEG image can be obtained.
4. Advantages include survival of message bits in active warden scenario, performs well against steganalysis tool called self calibration [56].

F5:

1. Introduced by Westfield and LSB replacement is not used for embedding.
2. Depending on secret message bit to be embedded, the absolute value of the coefficient is decreased by 1 if it needs to be modified.
3. Selection of DCT coefficients is made randomly and matrix encoding (syndrome coding) is employed.
4. Number of non-zero DCT coefficients and length of secret message to be embedded are used to employ matrix embedding.
5. Successfully defends chi square and extended chi square attacks due to random selection of DCT coefficients [57].

Outguess:

1. Embedding is performed by LSB replacement technique.
2. DCT coefficients except with value 0 and 1 are selected.
3. Only half of workable coefficients are selected to avoid detection against chi square attack [58].

Sachnev et al. discussed BCH based scheme in [59] where two consecutive blocks can be overlapped to form a combined block. Data embedding in intersected area results in increase

Table 2 – Review of major DCT based steganography schemes.

Algorithm	Embedding location	Key features
Behbahani et al. [63]	Eigenvalues of quantized DCT matrices	Higher embedding Resistance against Subtractive Pixel Adjacency Matrix (SPAM) and Merged Markov and DCT features steganalyzers. Embedding rates of 5%, 10% and 20%.
Mali et al. [64]	DCT coefficients, Interleaving and randomization spreads the embedded information all over the cover image	Uses Image Adaptive Energy Thresholding (AET) Coding framework with Class Dependent Coding Scheme (CDCS), Robust against image compression, tampering, resizing, filtering and AWGN, Achieves minimum IQM variations, Achieves PSNR of 40 dB for 6190 bits of information
Chu et al. [65]	Based on similarities of DCT coefficients between the adjacent image blocks	Preserve good image quality as embedding distortion is spread within the image blocks Resist some typical statistical attacks and achieves PSNR of 45.89 dB for 4 KB of information
Chang et al. [39]	Middle-frequency components of the quantized DCT coefficients	Same security as that of Jpeg–Jsteg. Uses modified quantization table, hiding capacity of 53 248 bits and max PSNR of 39.14 dB
Solanki et al. [66]	Uses coefficients that lie in a low frequency band of 21 coefficients for data embedding	Secure system as achieves zero Kullback–Leibler divergence between the cover and the stego image distributions with 20%–40% of hiding rates and error rates of less than 2%
Almohammad et al. [67]	2LSB of middle frequency coefficients	Larger hiding capacity as compared to Jpeg–Jsteg and Chang et al. scheme, 16 × 16 block size approach instead of traditional 8 × 8 method, gives PSNR of 48 dB for payload of 24 200 Kb with computational time as 1.56 s
Tseng et al. [68]	Employs a capacity table derived from the JPEG default quantization table and HVS to estimate the number of bits that can be hidden in each DCT coefficient	Embedding capacity of around 20% of the compressed image size with little noticeable degradation in image quality, employs modified quantization table
Liu et al. [69]	Embedding by subtracting one from or adding one to the non-zero DCT coefficient	Capacity is larger than J-Steg, F5 and outguess. Excellent performance against the chi-square family attack, S family attack, PSNR of 38.26 dB at an embedding rate of 20%
Chang et al. [70]	Two successive zero coefficients of the medium-frequency components in each block	Employs modified quantization table and PSNR of 2.2 times higher than that offered by a standard quantization table without affecting hiding capacity
Mandal et al. [71]	Three bits of hidden image are embedded per byte of the source image onto the rightmost 3 bits of each pixel excluding the first byte of each mask	GA is used to enhance the security level, better results as compared to Hashad A. I. et al. scheme in terms of hiding capacity and PSNR of 41.13 dB
Li et al. [72]	Derives an optimal substitution matrix by PSO to transform the secret message and then achieves data hiding in DCT coefficients	High security level because one cannot recover the secret messages correctly without knowing the substitution matrix Uses modified JPEG quantization table, results in PSNR of 38.02 dB for max payload of 73 728 bits
Yu et al. [73]	GA is used to optimize the performance e.g. Minimizes blockiness	Preserves the first order statistical properties of histogram
Yanqing et al. [74]	DCT coefficients based on GA	K–L divergence between cover and stego distribution used as the objective function defined by Cachin System security and excellent visual quality are achieved.
Fard et al. [75]	DCT coefficients selected by Genetic algorithm	Use of GA optimizes the message embedding locations and converge to optimal fitness after 50 generations, defeat all known steganalysis methods

in embedding rate. Also, Thiyagarajan et al. presented a reversible scheme for embedding patient information in medical image using a dynamic key generated by using graphs coloring problem. The algorithm is proved to be better in terms of robustness of stego image against affine transformation embedding rate and reversibility [60]. Hu et al. presented a lossless data hiding scheme which makes use of unused variable length codes to enhance the embedding capacity [61]. A steganography scheme is developed in [62] where quantization table elements and quantized DCT coefficients are varied together to control the increase in file size and hiding capacity. The results show that image quality is superior and capacity is enhanced.

Table 2 exhibits the relative comparison for some of the major DCT based steganography schemes discussed in literature.

It has been found that DCT used in JPEG though provides good results, rests on the unrealistic assumption of the independence of the blocks. The alternative to this blocked transform is discrete wavelet transform (DWT). Due to its

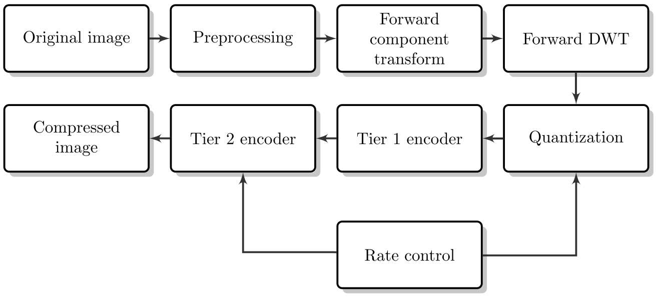


Fig. 9 – JPEG2000 encoder.

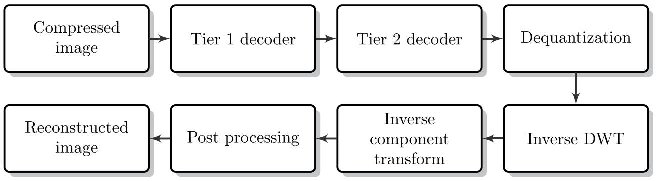


Fig. 10 – JPEG2000 decoder.

Table 3 – Various embedding locations in JPEG2000.

Locations for hiding data	Advantages	Limitations
Embedding after DWT	Larger word size of coefficients leading to high capacity, all the components are easily available	Steganalysis is easier since there is high probability of unusual coefficient values, embedding must be robust enough to resist ensuing steps of quantization and T1 coding
After quantization	Embedding can be done in clipped coefficients	Reduced capacity
Embed in T1 coded symbols	Partitioned code blocks are coded independently using the bit plane coder generating sequence of symbols that can be entropy coded	Smaller embedding capacity and higher rate of distortion
Embed in T2 coded symbols	Simplicity	Low capacity and high degradation

multiresolution nature, it results in sub bands containing same level of detail, derived from the whole image. Sub subsection below gives an overview of DWT based steganography schemes.

3.2.2. *DWT based steganography*

DWT decomposition of image results in four sub bands. Lowest sub band has the most important and relevant information and the higher sub band has finer details. Most of the energy is compacted into few transform coefficients-an entropy coder locates them and encodes. A generalized scheme of the JPEG2000 can be explained with the help of encoder and decoder as shown in Figs. 9 and 10.

It must be noted that in JPEG2000 coding pipeline, there are two primary sources of data loss. One is obviously quantization and the other is the stage in tier-1 coding when a decision is made that which coding passes must be excluded from the final JPEG2000 file. There are various possibilities for data hiding locations in JPEG2000 structure flow. However, each approach has its own advantages and limitations which can be summarized as shown in Table 3. Advantages of DWT include: DWT offers better energy compaction than DCT without any blocking artifact after coding, DWT decomposes the image as L level dyadic wavelet pyramid and resultant wavelet coefficient can be easily scaled in resolution as one can discard the wavelet coefficients at levels finer to a given threshold and thus reconstructs the image with less details, multiresolution nature of DWT makes it suitable for scalable image coding.

Dual transform based steganography is developed in [76] that uses a combination of integer wavelet transform and DWT to embed secret image in cover. This method results in high imperceptibility and PSNR in range of 35–54 dB. Also, Nadiya et al. discussed embedding technique which is a combination of cryptography and steganography and is based on concept of double stegging. Here, encrypted secret data is embedded to one area of detail coefficient. Then again that detail coefficient is embedded to another area of detail coefficient of image. This yields better PSNR values with minimum distortions [77].

Along with DWT, several other transforms can also be employed for steganography e.g. Curvelet transform, Slantlet transform, Integer transform, Contourlet transform, Dual Tree DWT, DD DT DWT etc. Each of them offers certain advantages over others e.g. contourlet transform possesses main features of wavelet and decomposes the sub bands at each scale into different directions. It resolves the wavelet sub band mixing problem and is more powerful in characterizing

Please cite this article in press as: M.S. Subhedar, V.H. Mankar, Current status and key issues in image steganography: A survey, Computer Science Review (2014), http://dx.doi.org/10.1016/j.cosrev.2014.09.001

Table 4 – Review of major transform domain techniques (except DCT based schemes).

Reference	Embedding location	Key features
Huang et al. [78]	Successive zero coefficients of the medium–high frequency components in each reconstructed block for 3-level 2-D DWT of a cover image	Employs 9/7 wavelet filter in DWT. Offer PSNR of 31.41 dB for 36 710 bits of hiding capacity and preserve the good quality of stego-image
Phadikar et al. [79]	Embedding in lifting based discrete wavelet transform (DWT) coefficients instead of conventional DWT	Better robustness, results in low loss in image quality due to QIM Better watermark decoding reliability, improvement in PSNR, MSSIM and watson metric by 30%, 12% and 77% resp.
Liu et al. [80]	A whole JPEG 2000 bit stream is divided into multiple layers, every 0.5 bpp and perform backward embedding in each layer	High embedding capacity, progressive extractability and better image quality. Due to visual masking measurement and CSF weighting, visual distortion is very slight even though a large amount of data is embedded
Youssef et al. [81]	Using significant wavelet coefficients and their texture and sensitivity to gray value variations, the positions and the magnitudes are opted to adaptively embed the secret message	Resistant to various statistical attacks. High visual quality with minimum degradation
Sarreshtedari, S. [82]	Wavelet transforms coefficients of the original image	Using BPCS, data hiding capacity of each block is computed and then embedding is done over whole block and not in any bit planes
Xu et al. [83]	Invertible 2D wavelet transform is used that maps integer to integer instead of the traditional lossy DWT to eliminate the errors	Good imperceptibility (PSNR greater than 39 db). For absolutely error-free recovery, the payload signal should be preprocessed by a convolution encoder before embedding
Ghasemi et al. [84]	GA based mapping function is used to embed data in 4 × 4 block of DWT coefficients and OPAP is applied after embedding the message Embeds data in integer wavelet transform coefficients by using a mapping function based on genetic algorithm	Outperforms adaptive steganography technique based on wavelet transform in terms of PSNR and capacity, 39.94 db and 50% respectively Uses GA and OPAP to obtain an optimal mapping function to improve stego image quality and improve embedding rate
Kumar et al. [85]	Embedding in the high frequency sub-bands viz. HH, HL and LH obtained by applying Slantlet transform	Better data recovery. Use of T-Code to encode the original message Employs LSB and thresholding algorithm for embedding data in the image
Al-Ataby et al. [86]	Based on FDCT–FW (fast discrete curvelet transform–frequency wrapping)	Encrypt the 1D bit stream of the message with RC4, thus provides more security, High robustness against attacks
Muttoo et al. [87]	Encodes the message using best T-codes. Encoded message is embedded in high frequency sub bands HH, HL and LH obtained by Slantlet transform	T-codes are used for better embedding capacity and decoding efficiency, Image quality metrics evaluated are PSNR and MSSIM, good imperceptibility and better run time than the known Haar–Wavelet based technique
Keshari et al. [88]	Useof Weighted fractional Fourier transformation (WFRFT) Data embedding in LSB positions of real part of the transformed image	Transform order which determines the intermediate domain between spatial and frequency is considered as a secret key
Peng et al. [89]	According to the image block type determined by the pre-estimated distortion, embedding can be performed adaptively in selected block	Embedding as high as 2.17 bits per pixel into Lena image with a reasonable PSNR of 20.71 db
Sajedi et al. [105]	Coefficients with large magnitudes (edges) as human eyes are less sensitive in edgy and non-smooth regions of images	Average embedding capacity of 0.05 bits per pixel

(continued on next page)

images rich in directional details and smooth contours. Also, it is easily adjustable for detecting fine details in any orientation at various scale levels. The Slantlet transform is wavelet-like transform that provides better time localization and signal compression than the conventional discrete cosine transform (DCT) and discrete Haar–wavelet transform. Choice of transform to be used for embedding depends on user requirements and the need of application.

Table 4 summarizes image steganography schemes based on DWT and some of the other types of transforms excluding DCT.

3.3. *Spread spectrum steganography*

Spread spectrum technique is well known concept in digital communication. It involves spreading the bandwidth of

Table 4 (*continued*)

Reference	Embedding location	Key features
Sajedi et al. [90]	Secret data is embedded by increasing or decreasing the value of coefficient in a block of a contourlet sub band	Average embedding capacity of 0.02 bits per pixel and with cover selection procedure it is up to 0.06 bits per pixel
Muttoo et al. [91]	Embedding in the high frequency bands of 1-level decomposition of Double Density Dual Tree Discrete Wavelet Transform (DD DT DWT)	Three layer of security—one layer at each level of compression, encryption and embedding. Better in terms of imperceptibility, robustness and embedding capacity than DWT

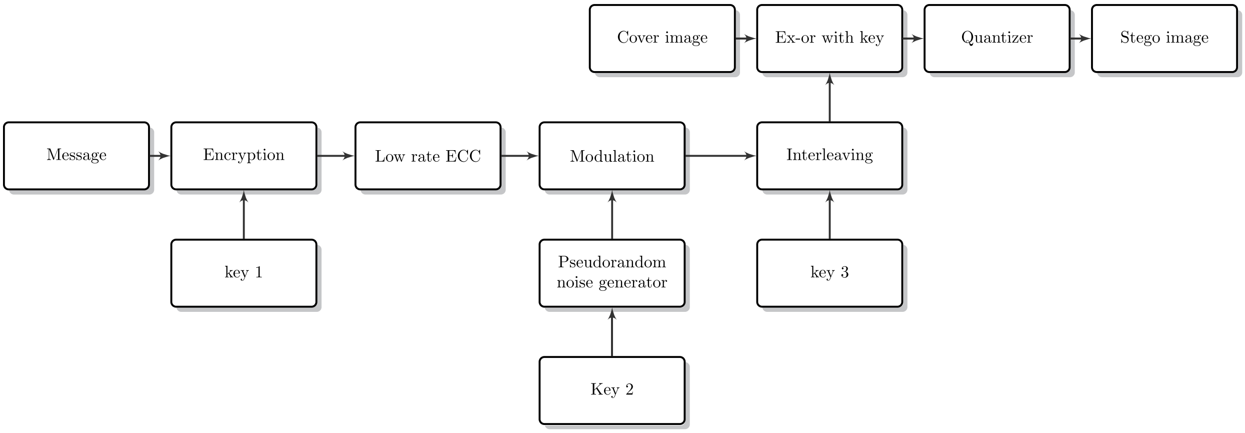


Fig. 11 – Spread spectrum image steganography encoder.

a narrowband signal across a wide band of frequencies. Spread spectrum steganography technique was proposed by Marvel et al. in [92]. Error control coding, encrypted message and property of pseudo randomness help to form blind steganography system where original message is not required for information extraction. Figs. 11 and 12 demonstrate the concept of spread spectrum communication.

The narrow band signal is modulated with a wide band signal such as white noise. After spreading, energy of the narrow band signal in any one frequency band is low and therefore difficult to detect. The resulting signal is combined with the cover image to form the stego image. Since the power of the embedded signal is much lower than the power of the cover image, the SNR is low indicating low perceptibility and low probability of detection by an observer. However, the pseudo random noise generator at the transmitter and receiver needs to be synchronized well else desired results will not be obtained.

Symmetric key system is used that needs both transmitter and receiver to have same keys for communication. This system proves better not only in imperceptibility but also withstand against additional noise and compression. A spread spectrum steganography approach is presented in where secret information is embedded in Galois Field, $GF(2^m)$ [93]. Amir Valizadeh et al. introduced correlation and bit aware concept in traditional spread spectrum steganography. Superior robustness and increased payload capacity are the significant benefits obtained with this method [94]. Use of advanced error correcting codes can be considered for further improvements. In order to enhance the performance of the system, bit error rate (BER) must be lowered while increasing the embedding capacity. One of the major advantages of spread spectrum technique is to maintain the robustness against statistical attacks. As the secret message is spread throughout the cover image while preserving the statistical properties, it results in good stego image quality. Encoding is done using low rate error correcting code. The few secret message bits are spread among many output bits with the help of parity bits. The quality of the stego image can be assessed using performance measures such as PSNR and MSE. It is very much difficult for the eavesdropper to detect or extract the hidden information because though the technique is known, without the possession of keys information extraction is quiet impossible.

3.4. *Model based steganography*

The solution to the drawbacks of spatial domain steganography can be found with frequency domain approach. However, simplicity of spatial domain method certainly matters in design and cannot be ignored. Steganography system should be designed in such a way that it should not reveal the presence of hidden information. Distortions in stego image and modifications occurred in statistical properties of image while hiding data allow an observer to suspect stego image.

To overcome these factors, model based steganography is developed. P. Sallee [95] proposed the idea of model based steganography in 2003 based on some statistical properties of the cover medium. It is also known as adaptive steganography or statistics aware steganography. This novel technique helps to embed the secret message without altering any of these properties. The theme of model based steganography can be

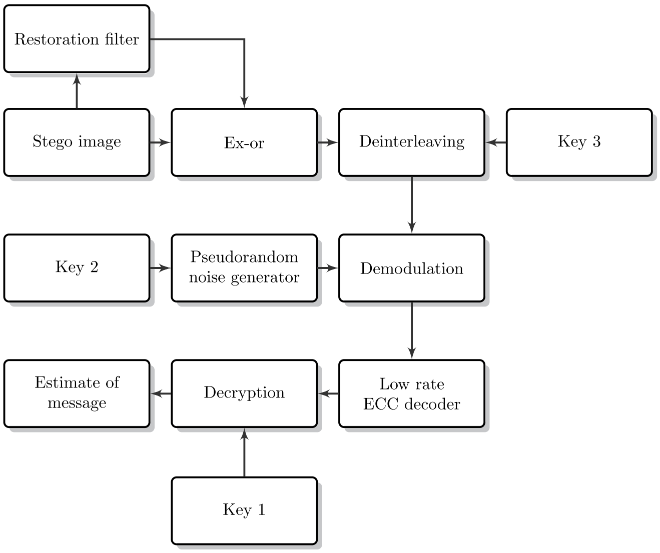


Fig. 12 – Spread spectrum image steganography decoder.

explained as below. Cover image is represented as a random variable X, and is divided in two parts, X_a that will not be modified during embedding and X_b, which is used to carry the secret message without altering the statistical properties of the cover. The embedded message is assumed to be a uniform random stream of bits. The embedded message is processed by an entropy decoder according to the conditional probability distribution $P_{X_b|X_a}(x_b|x_a)$. Its output is denoted by x'_b and forms together with X_a the stego message x'. At the decoder side, entropy encoder is used. The stego message x' is separated in x_a and x_b. Probability distribution $P_{X_b|X_a}(x'_b|x_a)$ is calculated to obtain x_b according to the model distribution and the encoder outputs the embedded message. In [96], a survey on adaptive steganography is presented.

A popular adaptive method presented by Hioki [97] is known as "A block complexity based data embedding (ABCDE)". By replacing pixels of noisy blocks in image with the block obtained by embedding data, data embedding is achieved. Larger embedding capacity is one of the key advantages. Since modifications in image are done by first analyzing the statistical parameters of image, there will not be much issues with stego image generated and will result in good quality. With the help of two measures, run length irregularity and border noisiness, image blocks are categorized as simple and complex and their suitability is decided for data embedding. The threshold values for the two complexity measures can be mentioned independently for each bit-plane that results into high quality image and larger embedding capacity simultaneously.

Despite of large embedding capacity, certain parameters need to be controlled manually e.g. finding an appropriate section length for sectioning a stream of resource blocks and finding the threshold value. Authors did not pay much attention towards the issues like, if cover image dimensions are not suitable to form image blocks for embedding then how to carry out data hiding and whether this method is prone to various types of stego attacks. These requirements lead to unsuitability of the method for the automatic process. However, ABCDE method provides an improvement over BPCS method.

Though model based method works better by providing additional security layer as it is statistics aware, no steganography system is 100% secure. Therefore some additional means need to be employed such as modifications to less number of pixels or transform coefficients, use of encrypted version of secret message to be embedded etc. Still lot of work in this field is required so as to choose proper trade off between the performance evaluation measures such as security, imperceptibility and payload capacity.

4. Image quality measure (IQM)

Due to thousands of new arrivals in Internet and multimedia technology, quality of transmission and retrieval of data has become critical issues. There should be uniqueness in the measures used for performance analysis. Image quality metric is the figure of merit to provide quantitative data on the fidelity of rendered images. Typically, the quality of an image synthesis method is evaluated using numerical techniques which attempt to quantify fidelity using image to image comparisons. Several image quality metrics have been developed to predict the visible differences between a pair of images.

It is well accepted that only mean squared error (MSE) do not provide meaningful measure of image fidelity, so more sophisticated techniques are necessary. As image quality assessment should correspond to assessments made by humans. A better understanding of features of the human visual system should lead to more effective comparisons, which in turn will steer image synthesis algorithms to produce more realistic and reliable images. Image quality metrics are categorized into six groups according to the type of information they use to evaluate the quality of stego image. The categories used are as shown in Table 5.

Please cite this article in press as: M.S. Subhedar, V.H. Mankar, Current status and key issues in image steganography: A survey, Computer Science Review (2014), http://dx.doi.org/10.1016/j.cosrev.2014.09.001

Table 5 – Image quality measures.

Sr. no.	Criteria/parameter on which metric is based on	Examples of metric
1	Pixel difference-based measures (mean square distortion)	Mean Square Error, Mean Absolute Error, Modified Infinity Norm, $L * a * b*$ Perceptual Error, Neighborhood Error, Multiresolution Error, PSNR, SSIM (Structural Similarity), MSSIM (Multi scale SSIM), VIF (Visual Information Fidelity), VSNR (Visual Signal-to-Noise Ratio), UIQI (Universal Image Quality Index)
2	Correlation-based measures (correlation of pixels, or of the vector angular directions)	Normalized Cross-Correlation, Image Fidelity, Czenakowski Correlation, Mean Angle Similarity, Mean Angle–Magnitude Similarity
3	Edge-based measures (displacement of edge positions or their consistency across resolution levels)	Pratt Edge Measure, Edge Stability Measure
4	Spectral distance-based measures (Fourier magnitude and/or phase spectral discrepancy on a block basis)	Spectral Phase Error, Spectral Phase–Magnitude Error, Block Spectral Magnitude Error Block Spectral Phase Error, Block Spectral Phase–Magnitude Error
5	Context-based measures (penalties based on various functional of the multidimensional context probability)	Rate Distortion Measure, Hellinger distance, Generalized Matusita distance, Spearman Rank correlation
6	Human Visual System-based measures (measures either based on the HVS weighted spectral distortion measures or (dis) similarity criteria used in image database browsing functions)	HVS Absolute Norm, HVS L2 Norm, Browsing Similarity, DCTune

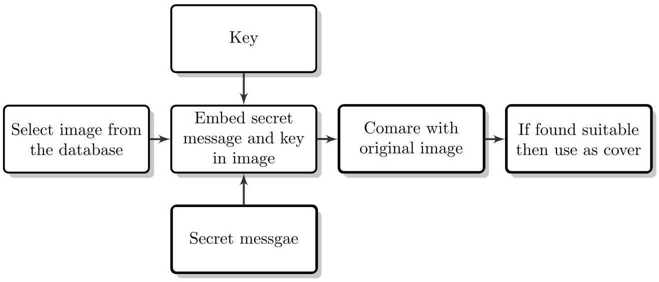

Key
Select image from the database
Embed secret message and key in image
Comare with original image
If found suitable then use as cover
Secret messgae

Fig. 13 – Cover selection process.

Each measure has its own advantages and disadvantages. According to the need of application, suitable metric should be chosen and computed so as to analyze and compare stego image with cover image. The detailed description and formulas can be found in [98–101].

5. Cover selection

Basically, steganography is the way to protect the confidentiality. The primary objective of steganography is to modify the carrier i.e. cover image in an imperceptible way so that it reveals nothing: neither the embedding of a message nor the embedded secret message i.e. image steganography basically aims at maximizing the payload capacity (embedding capacity) and minimizing the detectability of stego image. Many enhanced techniques are proposed in literature so as to achieve these two goals; however, the area of cover image selection which helps to obtain less noticeable changes in stego image is not exploited much till now.

Fig. 13 illustrates cover selection method in general. Alice has the choice for cover image. From the image database, suitable cover image can be selected with the help of any of the metrics available and then embedding should be carried out in selected cover image i.e. two approaches can be employed to optimize the performance. One is choice of cover image and the other is selection of appropriate embedding algorithm. By employing the cover image selection process, one can make steganalyzer to misclassify the stego image and thus helps to obtain imperceptibility. Different measures are discussed in literature for cover selection which can be broadly categorized into two types: Cover based and Cover-stego based. Some of them are discussed here. Table 6 gives a brief overview of various cover selection measures.

Sajedi et al. proposed cover selection method based on similarity of image blocks [102]. It uses statistical features of image blocks and their neighborhood to select the best host image. The performance is analyzed with wavelet and feature based steganalysis algorithms. Along with security, this algorithm provides high embedding capacity with less distortions in image. Another way of choosing the cover image is based on correlation coefficient. Relation between correlation parameter, KL divergence and ROC curve can be used to define the cover selection and security criteria for

Please cite this article in press as: M.S. Subhedar, V.H. Mankar, Current status and key issues in image steganography: A survey, Computer Science Review (2014), http://dx.doi.org/10.1016/j.cosrev.2014.09.001

Table 6 – Cover selection measures.

Criteria	Measure	Description
Cover based	Changeable coefficients	More the changeable coefficients, less are the number of modifications
	Correlation parameter	Smaller the correlation parameter, better is the security
	JPEG quality factor	Higher the quality factor, less the performance of steganalyzer
	Bhattacharya distance	If the Bhattacharya distance is zero, system is almost secure
	Depending on embedding capacity	Image with embedding capacity greater than secret message size will be a good cover image
	Quad tree based complexity measure	Low, middle and high complexity images are preferred to provide high embedding capacity
	Uniformity based complexity measure	
	Similarity of image blocks	Using block texture and neighborhood information, most similar blocks to those of secret image are found
	Contrast	Using co occurrence matrix, contrast value can be computed. Higher contrast shows better cover image
	Complexity of binary images, percentage of edges, DCT complexity	Complex images will be the more appropriate choice for the cover image
Cover stego based	MSE (Mean Square Error)	Lower the MSE, greater the PSNR, and the system is less detectable
	Watson's metric	Less detect ability if value is less for Watson's metric between cover and stego image
	Prediction error	Same as MSE i.e. less the error, less the detect ability
	Structural similarity measure (SSIM)	Larger the measure less is the detect ability

steganography system. Consider an image I which has $M \times N$ pixels. The correlation coefficient between two arbitrary pixels $I(x, y)$ and $I(x + \triangle x, y + \triangle y)$ is denoted by $r(\triangle x, \triangle y)$ and is given by,

$$r(\triangle x, \triangle y) = \rho^{\triangle r} = \rho^{[k_1(\triangle x)\,2+k_2(\triangle y)\,2]I/2} \tag{8}$$

where k_1 and k_2 denote the difference between horizontal and vertical correlation in image. Cover image with smallest value of correlation parameter ρ is suitable to design secure steganography system. ROC curves can also be used for this purpose. Lower the nature of ROC curve, detection of steganography becomes more difficult [103]. It indicates that cover image with smaller correlation parameter should be selected for better security. Smaller the correlation parameter, smaller is the Bhattacharya distance and KL divergence.

In [104], cover selection phenomenon is evaluated based on three scenarios in which embedder has no knowledge, partial knowledge or full knowledge about the steganalyzer. As per the results observed by Sajedi and Jamzad, cover selection can also be made depending on embedding capacity. They found that the images with embedding capacity greater than secret message to be embedded are proper for data hiding.

It was proved that, Quad tree based and Uniformity based complexity measures can be used to select image with high embedding capacity among low, middle and high complexity images in database. Also, Sajedi et al. [105] proposed a novel approach for classification of cover selection measures. They classified the measures into two types, fast measures and exact measures. Fast measures consist of image complexity measures (e.g. Complexity of binary images, Quad tree representation, homogeneity, Uniformity, Contrast, Correlation, Percentage of edges, DCT complexity etc.) and textureness. Exact measures include visual quality and amount of changes in stego image. Fig. 14 shows the performance of cover image under various selection measures. Using the secret data size of 5185 bits, results can be compared for visual quality of stego image and shows better performance for all measures except for the percentage of edges.

It has been observed that image complexity measures though fast, are not precise. On the other hand, exact measures are slow in nature however result in best cover image for the given amount of secret message bits.

Ultimately, if we choose the proper cover image to hide data in, embedding rate can be significantly improved. Using any of the measures discussed above we can make optimum choice of cover image for data embedding. As precise selection of cover image affects the steganography system in terms of visual quality and security, appropriate selection criteria for cover image will lead to a secure steganography system while maintaining high payload capacity.

6. Future directions

The previous sections highlight the details of how algorithms have evolved over time in various domains. A good steganographic algorithm should have high fidelity, maximum embedding capacity and acceptable level of security. At the same time, complexity of algorithm and universal applicability should also be considered. Some of the approaches to design such scheme can be summarized as below:

1. Trade off between embedding rate and steganographic security: We know that security level of transform domain techniques is much better as compared to spatial domain schemes as they embed secret message in transform coefficients. However, simplicity and larger embedding capacity are the significant characteristics of spatial

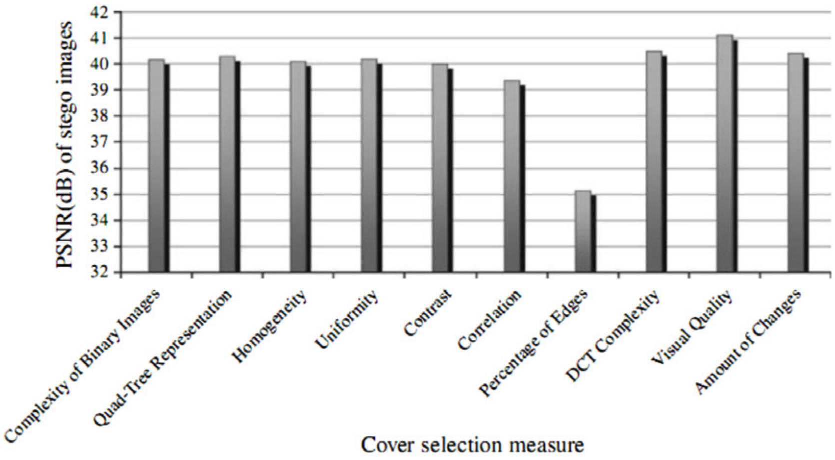


Fig. 14 – Visual quality of stego images when cover images are selected using various complexity measures [105].

domain method which cannot be ignored. Spatial domain methods exploits redundancy in image to embed secret data hence they are more appropriate for lossless image formats such as PNG, TIFF, GIF, BMP etc. as compared to lossy compressed images such as JPEG and JPEG2000. At the same time, in transform domain approach secret data is embedded in transform coefficients so they are more robust against image processing operations and immune to stego attacks. Therefore, the steganography algorithm should be modeled such that it comprises of simplicity and larger embedding rate of spatial domain and robustness of transform domain.

2. Improving the steganographic algorithm: To improve the steganography algorithm, a variety of measures can be considered.
   a. Statistics aware modeling: Steganography and steganalysis play hide and seek game. They try to defeat and develop with each other. With the several advances in steganalytic algorithms, the task of designing most secure steganography algorithm is day by day becoming crucial. One of the ways to achieve this include embedding secret data in specific regions only rather than in entire cover image. Such region is known as Region of interest (ROI). These regions should be selected in such a way that embedding in these portions of image will result in minimum distortion e.g. in transform domain approach high frequency regions are more suitable to embed secret data. Hence we can conclude that embedding secret data in ROI by considering statistical properties of an image will help to achieve desired results.
   b. Soft computing tools: Selection of appropriate embedding locations has a major role in data embedding process. Choice of embedding locations from the cover image can be made using soft computing tools. Use of optimization algorithms like genetic algorithm, particle swarm optimization etc., neural networks, fuzzy logic and hybrid network may help to adaptively embed data in cover image in such a way that it improves embedding capacity, stego image quality and innocuousness.
   c. Improving the security of secret data: Use of encrypted secret data will help to enhance security. Techniques like RSA, DES can be used to obtain encrypted version of secret information to be embedded.
   d. Selection of best cover to hide data: In past, researchers used to focus only on the optimum choice of data embedding locations so as to obtain good image quality. However, it has been found that selection of proper cover image can also make the system immune to stego attacks while maintaining high payload capacity. Different cover selection measures are discussed and compared in Section 5.
   e. Another important aspect regarding the judgment of stego image quality is the performance metric used to access and compare the quality of stego image with that of cover image. A list of performance metrics that can be used for image quality analysis is discussed in Section 4. According to the nature of application, suitable metric can be utilized.

7. Conclusion

In this paper, we reviewed some of the fundamental concepts, performance measures and other significant parameters that impact image steganography. With the survey papers presented earlier, some of the important aspects that contribute to steganography system such as cover image selection, image quality metrics etc. are relatively less investigated. Hence, we have focused on such issues. Different ways to embed secret bits with various types, their merits and demerits are discussed. There are three different approaches to design secure, high capacity image steganography system: (a) Choose suitable cover image form the database. (b) Select appropriate embedding locations (c) Use encrypted version of secret data for embedding. All these possibilities are discussed in detail. Thus, suitable cover image, selection of optimum data hiding locations and use of appropriate data embedding algorithm will result in secure, high capacity steganography system that may defeat several statistical attacks.

Please cite this article in press as: M.S. Subhedar, V.H. Mankar, Current status and key issues in image steganography: A survey, Computer Science Review (2014), http://dx.doi.org/10.1016/j.cosrev.2014.09.001

REFERENCES

[1] G.J. Simmons, The prisoner's problem and the subliminal channel, in: Advances in Cryptology: Proceedings of CRYPTO'83, in: Lecture Notes in Computer Science, Plenum, New York, 1983, pp. 51–67.

[2] N. Provos, P. Honeyman, Hide and seek: An introduction to steganography, IEEE Secur. Privacy 1 (2003) 32–44.

[3] R.J. Anderson, F.A. Petitcola, On the limits of steganography, IEEE J. Sel. Areas Commun. 16 (1998) 474–481.

[4] A. Cheddad, J. Condell, K. Curran, P.M. Kevitt, Digital image steganography: survey and analysis of current methods, Signal Process. 90 (2010) 727–752.

[5] F.N. Johnson, S. Jajodia, Steganalysis of images created using current steganography software, in: Proc. of Second International Workshop on Information Hiding, vol. 1525, pp. 273–277.

[6] T. Fawcett, Roc graphs: Notes and practical considerations for researchers, Technical Report HPL-2003-4, HP Laboratories, 2003.

[7] R. Chandramouli, M. Kharrazi, N. Memon, Image steganography and steganalysis: Concepts and practice, in: Proc. of International Workshop on Digital-forensics and Watermarking, vol. 2939, pp. 35–49.

[8] H. Wang, S. Wang, Cyber warfare: Steganography vs. steganalysis, Commun. ACM 47 (2004) 76–82.

[9] V. Sabeti, S. Samavi, M. Mahdavi, S. Shirani, Steganalysis and payload estimation of embedding in pixel differences using neural networks, Pattern Recognit. 43 (2010) 405–415.

[10] A.P. Fabien, R.J. Anderson, M.G. Kuhn, Information hiding: A survey, in: Proc. of IEEE Special Issue on Protection of Multimedia Content, vol. 87, pp. 1062–1078.

[11] N.-I. Wu, M.-S. Hwang, Data hiding: Current status and key issues, Int. J. Netw. Secur. 4 (2007) 1–9.

[12] B. Li, J. He, J. Huang, Y.Q. Shi, A survey on image steganography and steganalysis, Int. J. Inf. Hiding Multimedia Signal Process. 2 (2011) 142–172.

[13] T. Pevny, J. Fridrich, Benchmarking for steganography, in: Proc. of the 10th International Workshop on Information Hiding, vol. 5284, pp. 251–267.

[14] F. Zhang, Z. Pan, K. Cao, F. Zheng, F. Wu, The upper and lower bounds of the information hiding capacity of digital images, Inform. Sci. 178 (2008) 2950–2959.

[15] V. Korzhik, H. Imai, J. Shikata, On the use of bhattacharyya distance as a measure of the detectability of steganographic systems, in: Transactions on Data Hiding and Multimedia Security, in: Lecture Notes in Computer Science, vol. 4920, Springer-Verlag, Heidelberg, 2008, pp. 23–32.

[16] T. Kailath, The divergence and bhattacharyya distance measures in signal selection, IEEE Trans. Commun. Technol. 15 (1967) 52–60.

[17] C. Cachin, An information-theoretic model for steganography, in: Lecture Notes in Computer Science, vol. 1525, Springer-Verlag, Heidelberg, 1998, pp. 306–318.

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

[19] H. Yang, X. Sun, G. Sun, A high-capacity image data hiding scheme using adaptive LSB substitution, Radio Eng. 18 (2009) 509–516.

[20] M.U. Celik, G. Sharma, A.M. Tekalp, E. Saber, Lossless generalized-LSB data embedding, IEEE Trans. Image Process. 14 (2005) 253–266.

[21] Z.-H. Wang, C.-C. Chang, M.-C. Li, Optimizing least-significant-bit substitution using cat swarm optimization strategy, Inform. Sci. 192 (2012) 98–108.

[22] S. Wang, B. Yang, X. Niu, A secure steganography method based on genetic algorithm, J. Inf. Hiding Multimedia Signal Process. 1 (2010) 28–35.

[23] Z. Zhao, H. Luo, Z.-M. Lu, J.-S. Pan, Reversible data hiding based on multilevel histogram modification and sequential recovery, Int. J. Electron. Commun. 65 (2011) 814–826.

[24] C.-C. Lin, W.-L. Tai, C.-C. Chang, Multilevel reversible data hiding based on histogram modification of difference images, Pattern Recognit. 41 (2008) 3582–3591.

[25] M.K. Ramaiya, N. Hemrajani, A.K. Saxena, Security improvisation in image steganography using des, in: Proc. of 3rd IEEE International Conference on Advance Computing, pp. 1094–1099.

[26] B. Cong, N. Sang, M. Yoon, H.-K. Lee, Multi bit plane image steganography, in: International Workshop on Digital-forensics and Watermarking, vol. 4283 of Lecture Notes in Computer Science, pp. 61–70.

[27] E. Kawaguchi, R.O. Eason, Principle and applications of BPCS steganography, in: Proc. of Multi-media Systems and Applications, in: SPIE, vol. 3528, 1998, pp. 464–473.

[28] V.M. Potdar, E. Chang, Gray level modification steganography for secret communication, in: Proc. of 2nd IEEE International Conference on Industrial Informatics, pp. 223–228.

[29] D. Wu, W.H. Tsai, A steganographic method for images by pixel value differencing, Pattern Recognit. Lett. 24 (2003) 1613–1626.

[30] X. Zhang, S. Wang, Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security, Pattern Recognit. Lett. 25 (2004) 331–339.

[31] J.-C. Joo, H.-Y. Lee, H.-K. Lee, Improved steganographic method preserving pixel-value differencing histogram with modulus function, EURASIP J. Adv. Signal Process. 2010 (2010).

[32] C.-H. Yang, C.-Y. Weng, H.-K. Tso, S.-J. Wang, A data hiding scheme using the varieties of pixel-value differencing in multimedia images, J. Syst. Softw. 84 (2011) 669–678.

[33] Y.-P. Lee, J.-C. Lee, W.-K. Chen, K.-C. Chang, I.-J. Su, C.-P. Chang, High-payload image hiding with quality recovery using tri-way pixel-value differencing, Inform. Sci. 191 (2012) 214–225.

[34] X. Liao, Q. yan Wen, J. Zhang, A steganographic method for digital images with four-pixel differencing and modified LSB substitution, J. Vis. Commun. Image Represent. 22 (2011) 1–8.

[35] G. Liu, W. Liu, Y. Dai, S. Lian, Adaptive steganography based on block complexity and matrix embedding, Multimedia Syst. (2013) 1–12.

[36] G. Swain, S.K. Lenka, Steganography using two sided, three sided and four sided side match methods, CSI Trans. ICT 1 (2013) 127–133.

[37] B. Chen, G.W. Wornell, Quantization index modulation: A class of provably good methods for digital watermarking and information embedding, IEEE Trans. Inform. Theory 47 (2001) 1423–1443.

[38] K.L. Chung, C.H. Shen, L.C. Chang, A novel SVD and VQ based image hiding scheme, Pattern Recognit. Lett. 22 (2001) 1051–1058.

[39] C.-C. Chang, T.S. Nguyen, C.-C. Lin, A novel VQ-based reversible data hiding scheme by using hybrid encoding strategies, J. Syst. Softw. 86 (2012) 389–402.

[40] C.-C. Chang, T.S. Nguyen, C.-C. Lin, A reversible data hiding scheme for VQ indices using locally adaptive coding, J. Vis. Commun. Image Represent. 22 (2011) 664–672.

[41] X. Zhang, S. Wang, Steganography using multiple-base notational system and human vision sensitivity, IEEE Signal Process. Lett. 12 (2005) 67–70.

[42] S. Geetha, V. Kabilan, S. Chockalingam, N. Kamaraj, Varying radix numeral system based adaptive image steganography, Inform. Process. Lett. 111 (2011) 792–797.

[43] D. Kieu, C.-C. Chang, A steganographic scheme by fully exploiting modification directions, Expert Syst. Appl. 38 (2011) 10648–10657.

[44] W. Hong, T.-S. Chen, C.-W. Luo, Data embedding using pixel value differencing and diamond encoding with multiple-base notational system, J. Syst. Softw. 85 (2012) 1166–1175.

[45] H.-C. Wu, H.-C. Wang, C.-S. Tsai, C.-M. Wang, Reversible image steganographic scheme via predictive coding, Displays 31 (2010) 35–43.

[46] C.W. Honsinger, P.W. Jones, M. Rabbani, J.C. Stoffel, Lossless recovery of an original image containing embedded data, US 6278791 B1, 2001.

[47] B. Macq, F. Dewey, Trusted headers for medical images, in: Proc. of Watermarking Workshop, vol. II.

[48] J. Fridrich, M. Goljan, R. Du, Invertible authentication, in: Proc. of SPIE Security and Watermarking of Multimedia Contents, SPIE, San Jose, CA, 2001, pp. 197–208.

[49] M. Goljan, J. Fridrich, R. Du, Distortion-free data embedding for images, in: Proc.of 4th Information Hiding Workshop, Pittsburgh, PA, pp. 27–41.

[50] C.D. Vleeschouwer, J.F. Delaigle, B. Macq, Circular interpretation of histogram for reversible watermarking, in: Proc. of 4th International IEEE Workshop on Multimedia Signal Process, pp. 345–350.

[51] G. Xuan, J. Zhu, J. Chen, Y.Q. Shi, Z. Ni, W. Su, Distortion less data hiding based on integer wavelet transform, IEE Electron. Lett. 38 (2002) 1646–1648.

[52] M.U. Celik, G. Sharma, A.M. Tekalp, E. Saber, Reversible data hiding, in: Proc. of IEEE International Conference on Image Processing, vol. 2, pp. 157–160.

[53] Z. Ni, Y.-Q. Shi, N. Ansari, W. Su, Reversible data hiding, IEEE Trans. Circuits Syst. Video Technol. 16 (2006) 354–362.

[54] D. Upham, Jsteg, 1993. http://zooid.org/paul/crypto/jsteg.html (accessed: 2013-07-05).

[55] A. Latham, Jphide, 1999 http://linux01.gwdg.de/alatham/stego.html (accessed: 2013-07-05).

[56] K. Solanki, A. Sarkar, B.S. Manjunath, Yass: yet another steganographic scheme that resists blind steganalysis, in: Proc. of the 9th Information Hiding Workshop. vols. 45–67, Springer, 2000, pp. 16–31.

[57] A. Westfeld, F5-a steganographic algorithm: High capacity despite better steganalysis, in: Proc. of the 4th Information Hiding Workshop, vols. 21–37, pp. 289–302.

[58] N. Provos, Defending against statistical steganalysis, in: Proc. of the 10th USENIX Security Symposium, pp. 323–336.

[59] V. Sachnev, H.J. Kim, Modified BCH data hiding scheme for JPEG steganography, EURASIP J. Adv. Signal Process. (2012) 1–10.

[60] P. Thiyagarajan, G. Aghila, Reversible dynamic secure steganography for medical image using graph coloring, Health Policy Technol. 2 (2013) 151–161.

[61] Y. Hu, K. Wang, Z.-M. Lu, An improved VLC-based lossless data hiding scheme for JPEG images, J. Syst. Softw. 86 (2013) 2166–2173.

[62] K. Wang, Z.-M. Lu, Y.-J. Hu, A high capacity lossless data hiding scheme for JPEG images, J. Syst. Softw. 86 (2013) 1965–1975.

[63] M. Behbahani, P. Ghayour, A.H. Farzaneh, Steganography based on eigen characteristics of quantized DCT matrices, in: Proc. of the 5th International Conference on IT & Multimedia, pp. 14–16.

[64] S.N. Mali, P.M. Patil, R.M. Jalnekar, Robust and secured image-adaptive data hiding, Digit. Signal Process. 22 (2012) 314–323.

[65] R. Chu, X. You, X. Kong, X. Ba, A DCT-based image steganographic method resisting statistical attacks, in: Proc. of IEEE International Conference on Acoustics, Speech, and Signal Processing, vol. 5, pp. 953–956.

[66] K. Solanki, K. Sullivan, V. Madhow, B. Manjunath, S. Chandrasekaran, Provably secure steganography: Achieving zero $k-l$ divergence using statistical restoration, in: Proc. of IEEE International Conference on Image Processing, pp. 125–128.

[67] A. Almohammad, H.G. Ghinea, High capacity steganographic method based upon JPEG, in: Proc. of Third IEEE International Conference on Availability, Reliability and Security, pp. 544–549.

[68] H.-W. Tseng, C.-C. Chang, High capacity data hiding in JPEG-compressed images, Informatica 15 (2004) 127–142.

[69] C.-L. Liu, S.-R. Liao, High-performance JPEG steganography using complementary embedding strategy, Pattern Recognit. 41 (2008) 2945–2955.

[70] C.-C. Chang, C.-C. Lin, C.-S. Tseng, W.-L. Tai, Reversible hiding in DCT based compressed images, Inform. Sci. 177 (2007) 2768–2786.

[71] J.K. Mandal, A. Khamrui, A genetic algorithm based steganography in frequency domain (GASFD), in: Proc. of International Conference on Communication and Industrial Application, pp. 1–4.

[72] X. Li, J. Wang, A steganographic method based upon JPEG and particle swarm optimization algorithm, Inform. Sci. 177 (2007) 3099–3109.

[73] L. Yu, Y. Zhao, R. Ni, Z. Zhu, Pm1 steganography in JPEG images using genetic algorithm, Soft Comput. 13 (2009) 393–400.

[74] G. Yanqing, K. Xiangwei, Y. Xingang, Secure steganography based on binary particle swarm optimization, J. Electron. 26 (2009) 285–288.

[75] A.M. Fard, M.R. Akbarzadeh-T, A.F. Varasteh, A new genetic algorithm approach for secure jpeg steganography, in: Proc. of IEEE International Conference on Engineering of Intelligent Systems, pp. 1–6.

[76] G. Prabakaran, R. Bhavani, K. Kanimozhi, Dual transform based steganography using wavelet families and statistical methods, in: Proc. of the 2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering, PRIME, pp. 287–293.

[77] P.V. Nadiya, B.M. Imran, Image steganography in DWT domain using double stegging with RSA encryption, in: Proc. of International Conference on Signal Processing, Image Processing & Pattern Recognition, ICSIPR, pp. 283–287.

[78] H.-Y. Huang, S.-H. Chang, A 9/7 wavelet-based lossless data hiding, in: Proc. of IEEE Symposium on Computational Intelligence for Multimedia, Signal and Vision Processing, CIMSIVP, pp. 1–6.

[79] A. Phadikar, S.P. Maity, Data hiding based quality access control of digital images using adaptive qim and lifting, J. Signal Process. Image Commun. 26 (2011) 646–661.

[80] W. Liu, Data hiding in jpeg2000 code streams, in: International Conference on Image Processing, ICIP, pp. 1557–1560.

[81] S.M. Youssef, A.A. Elfarag, Raouf, C7. A multi-level information hiding integrating wavelet-based texture analysis of block partition difference images, in: Proc. of 29th National Radio Science Conference, NRSC, pp. 203–210.

[82] S. Sarreshtedari, S. Ghaemmaghami, High capacity image steganography in wavelet domain, in: Proc. of 7th IEEE Consumer Communications and Networking Conference, pp. 1–5.

[83] J. Xu, A.H. Sung, P. Shi, Q. Liu, JPEG compression immune steganography using wavelet transform, in: Proc. of the International Conference on Information Technology: Coding and Computing, ITCC'04, vol. 2, pp. 704–708.

[84] E. Ghasemi, B. ZahirAzami, A steganographic method based on integer wavelet transform and genetic algorithm, in: Proc. of International Conference on Communication and Signal Processing, pp. 42–45.

[85] S. Kumar, S.K. Muttoo, Distortion less data hiding based on slantlet transform, in: International Conference on Multimedia Information Networking and Security, pp. 48–52.

[86] A.A. Al-Ataby, F.M. Al-Naima, High capacity image steganography based on curvelet transform, Dev. E-Syst. Eng. (2011) 191–196.

[87] S.K. Muttoo, S. Kumar, Secure image steganography based on slantlet transform, in: Proceeding of International Conference on Methods and Models in Computer Science, pp. 1–7.

[88] S. Keshari, S.G. Modani, Weighted fractional Fourier transform based image steganography, in: Proc. of International Conference on Recent Trends in Information Systems, pp. 214–217.

[89] F. Peng, X. Li, B. Yang, Adaptive reversible data hiding scheme based on integer transform, Signal Process. 92 (2012) 54–62.

[90] H. Sajedi, M. Jamzad, Using contourlet transform and cover selection for secure steganography, Int. J. Inf. Secur. 9 (2010) 337–352.

[91] S.K. Muttoo, S. Kumar, A multilayered secure, robust and high capacity image steganographic algorithm, World Comput. Sci. Inform. Technol. J., 1, 239–246.

[92] L.M. Marvel, C.G. Boncelet, C.T. Retter, Spread spectrum image steganography, IEEE Trans. Image Process. 8 (1999) 1075–1083.

[93] S.A. Halim, M.F.A. Sani, Embedding using spread spectrum image steganography with gf 2^m, in: Proc. of the 6th IMT-GT Conference on Mathematics, Statistics and its Applications, pp. 659–666.

[94] A. Valizadeh, Z.J. Wang, Correlation-and-bit-aware spread spectrum embedding for data hiding, IEEE Trans. Inf. Forensics Secur. 6 (2011) 267–282.

[95] P. Sallee, Model-based steganography, in: Proc. of the 2nd International Workshop on Digital Watermarking, vol. 2939, pp. 154–167.

[96] M. Mahajan, N. Kaur, Adaptive steganography: a survey of recent statistical aware steganography techniques, Int. J. Comput. Netw. Inform. Secur. 4 (2012) 76–92.

[97] H. Hioki, A data embedding method using BPCS principle with new complexity measures, in: Proc. of Pacific Rim Workshop on Digital Steganography, pp. 30–47.

[98] M. Kunt, C. van den Branden, Lambrecht, Special issue on image and video quality metrics, Signal Process. 70 (1998).

[99] I. Avcibas, B. Sankur, K. Sayood, Statistical evaluation of image quality measures, J. Electron. Imaging 11 (2001) 206–223.

[100] I. Avcibas, N. Memon, B. Sankur, Steganalysis using image quality metrics, IEEE Trans. Image Process. 12 (2003) 221–229.

[101] C.E. Halford, K.A. Krapels, R.G. Driggers, E.E. Burroughs, Developing operational performance metrics using image comparison metrics and the concept of degradation space, Opt. Eng. 38 (1999) 836–844.

[102] H. Sajedi, M. Jamzad, Cover selection steganography method based on similarity of image blocks, in: Proc. of IEEE 8th CIT Conference, Sydney, pp. 379–384.

[103] Y. Sun, F. Liu, Selecting cover for image steganography by correlation coefficient, in: Proc. of Second International Workshop on Education Technology and Computer Science, vol. 2, pp. 159–162.

[104] M. Kharrazi, H.T. Sencar, N. Memon, Cover selection for steganographic embedding, in: Proc. of ICIP, pp. 117–121.

[105] H. Sajedi, M. Jamzad, Contsteg: contourlet-based steganography method, Wirel. Sensor Netw. 1 (2009) 163–170.