CHAPTER 1

Data Hiding Schemes: A Survey

Musrrat Ali, Chang Wook Ahn and Millie Pant

Data hiding is the process of hiding an amount of data, called secret message or watermark, into a cover media that may be audio, video, or image signal, in an imperceptible way for different purposes. Due to the advances in generation, storage, and communication technology of digital media, the necessity and importance of data hiding has drawn the attention of many researchers all over the world resulting in a lot of variants of data hiding scheme. This chapter provides a detailed review of the basic concepts of data hiding and a survey of its major variants developed so far. The chapter classifies the data hiding schemes based on several aspects of data hiding comprising artificial intelligence. Furthermore, the chapter also provides the recommendations to the interested users for further research. This review may be a useful insight and a good source for the users who are interested in the application of artificial intelligence in data hiding.

Musrrat Ali, Chang Wook Ahn
Department of Computer Engineering, Sungkyunkwan University
Suwon-440746, Republic of Korea
e-mail: musrrat.iitr@gmail.com, cwan@skku.edu

Millie Pant
Department of Applied Science and Engineering,IIT
Roorkee-247667, India
e-mail: millifpt@iitr.ac.in

Editors: C.W. Ahn, M. Ali, M. Pant, *Embodying Intelligence in Multimedia Data Hiding*
DOI: 10.15579/gcsr.vol5.ch1, GCSR Vol. 5, pp. 1-19, 2016

1.1 Introduction

Data hiding is the art and science for embedding data into cover media such as audio, video, or image to build a covert channel for secret communication, for the purpose of verifying the integrity, for the copyright protection, or for other purpose [21, 31, 34, 43, 50, 52, 56, 70, 72, 75, 78, 107, 115, 122]. Data hiding schemes can be categorized into two groups: watermarking and steganography [17, 92]. Stenography and digital watermarking have made great progress due to the rapid development of information technology, multimedia tools and their wide applications. In the application of copyright protection, an owner of a digital media can use the digital watermarking technique to embed a digital watermark into the cover media, resulting in a watermarked media, to claim the ownership [51, 102]. While, the steganography is used for covert communication [92] in which people hide a secret data into a cover media, resulting in a stego-media; and a receiver of this stego-media can extract the hidden data from it to complete the communication. The main concern of a watermarking scheme is the robustness and transparency. That is, the watermark must be retrieved even if the watermarked-media is seriously distorted by the manipulation attacks such as lossy compression, rescaling, noise addition, cropping etc. While, the goal of steganography is different from watermarking. The key goal of steganography is to embed the maximum amount (capacity) of secret data to hide its existence with minimal distortion (transparency) of the cover media. A classification of data hiding techniques based on different factors is given in Fig.(1.1) [92] and comparison of steganography and watermarking is given in Table 1.1 [87].

Both the data hiding technologies embed the information in the cover media in order to send this information imperceptibly. However, in steganography, the communication is carried out between two parties. As a result, steganography is mainly concerned with concealing the existence of the communication and protecting the embedded data against any modifications that may happen during the transmission such as format change or compression. Thus, steganography has limited robustness. On the other hand, watermarking schemes are used when the cover is available to parties who know the existence of the hidden information and may try to destroy it. An important application of watermarking is the copyright protection of digital content [31, 51, 66, 85, 102, 108, 113]. Hence, the embedded information should be robust against intentional attacks that try to remove or change the watermark [5, 8, 26, 47, 49, 73, 74, 81, 88, 106].

In the literature, many conventional data hiding schemes have been proposed in spatial domain and frequency (transform) domain [34, 43, 50, 56, 72, 122]. The data hiding can cause damage to the sensitive information present in the cover media. Therefore, at the receiving end, the exact recovery of cover media may not be possible by these schemes. Furthermore, there exist certain applications such as military communication, healthcare, and law-enforcement that may not accept even small quality degradation of cover media prior to the downstream processing. In such cases, reversible data hiding schemes [32, 52, 56] are employed instead of conventional data hiding schemes. Reversible data hiding of digital content allows full extraction of the hidden data along with the complete restoration of the cover media. In other words, if the data hiding scheme is irreversible, then the extractor can extract only the hidden

data and the original cover media cannot be restored. While, a reversible data hiding scheme allows the extractor to recover the original cover media completely upon extraction of the hidden data. In the recent past, several reversible data hiding schemes have been developed based on different concepts such as lossless compression [31], difference expansion [1, 112], histogram-shifting [16, 30, 36, 40, 65, 96, 100, 110], vector quantization [13, 56, 68, 89, 98, 97, 101], and prediction-error [30, 33, 55, 80, 114]. A detailed review of reversible watermarking schemes is given in [46].

Depending on the variety of applications of data hiding schemes, the requirement of features (transparency, robustness, capacity) that must be satisfied varies accordingly. These features are conflicting with each other, so it is a very difficult task to satisfy all the requirements at the same time. Some of the researchers tried to find out the solution of this problem utilizing the artificial intelligence approaches [2, 4, 5, 6, 7, 8, 47, 52, 71, 72, 76, 81, 85, 94, 95, 108, 121]. There are different versions of data hiding based on different approaches. Therefore, the focus of this chapter is to provide a critical review of data hiding schemes.

The rest of the chapter is structured as follows. General characteristics of the data hiding are given in Section 1.2. Digital watermarking schemes are reviewed in Section 1.3. Section 1.4 provides a survey of steganography schemes. Intelligent data hiding schemes are given in Section 1.5. Finally, the summary of the chapter is given in Section 1.6.

1.2 The Requirements for Data Hiding

Depending on a variety of applications each data hiding scheme must have some basic requirements. These are transparency or imperceptibility, robustness, and capacity, which are in brief given below. It is hard to satisfy all the requirements at the same time as these are contradictory to each other (Fig.(1.2)) [90].

1.2.1 Transparency or Imperceptibility

Due to the insertion of secret data into cover media (audio, video, image etc.) distortion is expected in the cover media. Perceptual similarity of the original cover media with the embedded cover media is referred as transparency. The aim of data hiding is not to introduce the visible distortions in cover media to maintain its commercial value. For the assessment of perceptual similarity no universal effective measure exists [81]. However, Peak Signal to Noise Ratio ($PSNR$) [5] and structural similarity index ($SSIM$) [81] are widely adopted by the data hiding community.

PSNR: It is widely used for the performance evaluation of data hiding systems. In context of image, it is the ratio between the power of an image with maximum allowable pixel intensity (255 for 8-bit images) to the power of the noise. The noise power is defined as the power the of difference between original and watermarked images. Mathematically, it is defined as [5]:

$$PSNR\left(X,Y\right)=10\log_{10}\left(\frac{\left(255\right)^{2}}{\frac{1}{n\times n}\sum_{i=1}^{n}\sum_{j=1}^{n}\left(X\left(i,j\right)-Y\left(i,j\right)\right)^{2}}\right) \tag{1.1}$$

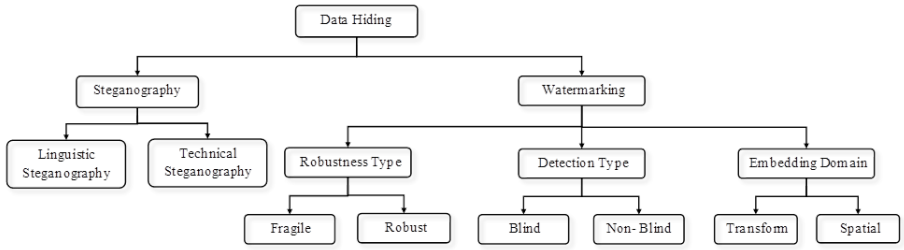

Figure 1.1: Classification of data hiding techniques based on different requirements [92].

Table 1.1: Comparison of watermarking and steganography [87].

Attributes	Watermarking	Steganography
Objective	Protect the embedded data against intentional attacks applied to remove or destroy it	Conceal the existence of the communications
Carrier	Any digital media	Any digital media
Perceptual quality of cover media	Application dependent	Must exist
Embedding data	Application dependent	Large
Output	Watermarked media	Stego-media
Goal fails when	Embedded watermark changed or removed	Existence of secret message is detected
Challenges	Robustness and perceptual transparency	Perceptual transparency, Hiding capacity and Robustness

where X and Y stand for the original and the processed images; subscripts i and j denote the location of the pixel value in the respective images; and n is the height or width of the square image.

SSIM: The structural similarity index (SSIM) is a relatively new method that is used to measure the similarity between the reference (original) image (X) and the embedded image (Y). It is developed by Wang et al. [109], and is considered to be correlated with the quality perception of the human visual system (HVS). It is designed by modeling an image distortion as a combination of three factors that are loss of correlation, luminance distortion and contrast distortion. The SSIM is defined as [81]:

$$SSIM\left(X,Y\right)=\frac{\left(2\mu_X\mu_Y+C_1\right)\left(2\sigma_{XY}+C_2\right)}{\left(\mu_X^2+\mu_Y^2+C_1\right)\left(\sigma_X^2+\sigma_Y^2+C_2\right)} \tag{1.2}$$

$$with \left\{ \begin{array}{l} C_1=K_1L \\ C_2=K_2L \end{array} \right\}, \left\{ \begin{array}{l} K_1=0.01 \\ K_2=0.03 \end{array} \right\} and\ L=255$$

where μ, σ^2, and σ_{XY} are the mean, variance, and covariance of the images X and Y. The constants C_1, and C_2 are the stabilizing constants that are used to avoid a null denominator. The value of SSIM index ranges over the interval $[0,1]$. A value of 0 means no correlation between images, and 1 means that both images are same.

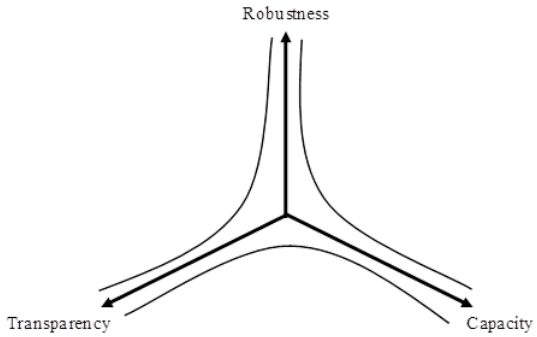

Figure 1.2: Tradeoffs between robustness, transparency and capacity [90].

1.2.2 Robustness

Robustness is defined as the ability of a data hiding system to withstand against modifications imposed on the watermarked/stego media. It is the most important property of a data hiding system for the correct detection of embedded data. A data hiding scheme used for the copyright protection is supposed to survive any kind of intentional and unintentional modification imposed on the watermarked/stego media. The purpose of these attacks is to remove the synchronization between the embedder and the detector. Robustness of a data hiding system is evaluated using different methods such as bit error rate (BER) [45] and normalized correlation (NC) [2, 6]. The normalized correlation between an image and its processed image is defined as:

$$NC\left(X,Y\right)=\frac{\sum_{i=1}^{n}\sum_{j=1}^{n}X\left(i,j\right)\times Y\left(i,j\right)}{\sqrt{\sum_{i=1}^{n}\sum_{j=1}^{n}X\left(i,j\right)^{2}}\sqrt{\sum_{i=1}^{n}\sum_{j=1}^{n}Y\left(i,j\right)^{2}}} \tag{1.3}$$

where X and Y stand for the original and the processed images; subscripts i and j denote the location of the pixel value in the respective images; and n is the height or width of the square image. The bit error rate (BER) is defined irrespective of the host image size as [45]:

$$BER=\frac{Number\,of\,incorrect\,bits}{Number\,of\,total\,bits} \tag{1.4}$$

1.2.3 Capacity

The capacity describes the maximum amount of secret data that can be hidden in the cover media. Different data hiding applications have different capacity requirements [17, 24, 92, 115]. Capacity estimation is a fundamental problem of steganography, where the question is how much data can safely be hidden without being detected? However, in watermarking, the primary constraint for the capacity is its mutual dependence on a few other properties (e.g., transparency, robustness) rather than the detection problem as in steganography. Usually, capacity is expressed in bits per pixel

in images, bits per sample in audio and bits per frame in videos. Data hiding algorithms with high capacity and low robustness are called steganography techniques, while the general term of watermarking usually refers to a low-capacity robust data hiding scheme. The capacity of a data hiding scheme defined as [53]:

$$Capacity = \frac{Maximum\,embedded\,data\,size}{Cover\,media\,size} \tag{1.5}$$

1.3 Digital watermarking

The huge expansion of Internet and computer networks have made the digital data (e.g. audio, video, image, etc.) acquisition and distribution very easy nowadays. Also, the digital data having the same quality as that of the original one can be created easily with the help of advanced multimedia technologies. But, besides all of these advantages, there are many undesired issues, including the piracy and misuse of digital contents. This concern has drawn the attention of the researchers towards the development of digital watermarking scheme [21, 20, 63]. Digital watermarking is the process of embedding a watermark into cover media imperceptibly. Generally, digital watermarking has three different stages; embedding, distortion implemented to remove the watermark and detection/extraction. A schematic illustration of watermarking is given in Fig.(1.3).

The watermarking schemes given in the literature can be classified into numerous categories based on different sets of criteria [20, 41]. One of them is the domain in which the watermark is inserted; spatial domain schemes and frequency domain schemes. In spatial domain schemes, the watermark is directly inserted into the cover media by altering the pixel values [62, 79, 115]. These methods have the advantages of easy implementation and low cost operation, but generally are not resistant enough to signal processing or other geometric attacks. While frequency domain schemes transform the representation of spatial domain into the frequency domain and then modify its frequency coefficients to embed the watermark. There are many transform domain watermarking schemes such as discrete cosine transforms (DCT) [4, 9, 57, 39, 37, 38, 113], singular value decomposition (SVD) [8, 14, 22, 27, 28, 34, 48, 52, 63, 74, 77, 84, 85, 90, 91, 113], discrete Fourier transforms (DFT) [18, 64, 67, 70, 94], and discrete wavelet transforms (DWT) [7, 28, 51, 83, 90, 102, 117]. These methods typically provide higher imperceptibility and are much more robust to distortion attacks, but the computational cost is higher than spatial-domain watermarking methods. The performance of watermarking methods further improved by combining two or more transformations [4, 2, 5, 28, 37, 48, 52, 74, 76, 84, 85, 90, 102, 113, 121]. The idea was based on the fact that the combined effect of the transforms would be more effective than the sum of their individual effects.

The literature review of SVD based watermarking reveals that, the watermarking schemes developed in spatial domain or frequency domain, generally embed singular values of the watermark and the rest of the information is kept safe for its extraction. Various researchers pointed out the false positive detection problem in most of the SVD-based algorithms and proved that the verification watermark unreasonably can

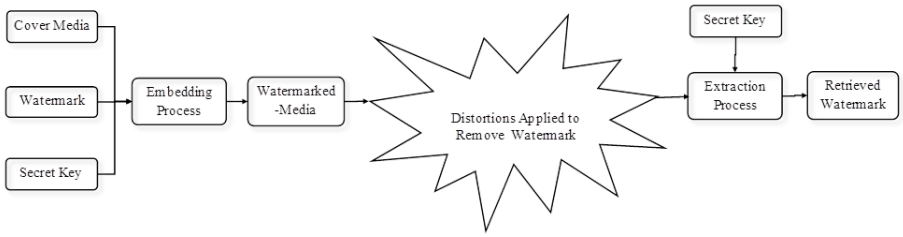

Figure 1.3: Illustration of watermark embedding and its retrieval.

be extracted [3, 19, 34, 35, 60, 61, 59, 86, 93, 120]. This creates an ambiguous situation, indicating the futility of such schemes for copyright protection purpose. To overcome this problem, numerous researchers have proposed improved versions of SVD based image watermarking schemes. A robust image watermarking scheme based on SVD that embeds the entire watermark is proposed by Mohammad et al. [77]. Run et al. [85] introduced an image watermarking scheme employing SVD and embedding the principal component of the watermark. Particle swarm optimization is applied to get the optimal scaling factors for embedding. It is based on the fact that SVD subspace (left and right singular vectors) can preserve a significant amount of information about an image. Because different regions of an image have different local features, so some visual models may be incorporated in finding the suitable embedding regions to improve robustness while maintaining imperceptibility. Based on this concept, a blind SVD-based watermarking scheme is presented in [14]. The host image is segmented into non-overlapping blocks, then the embedding blocks (most textured) are selected depending upon the number of non-zero singular values. The watermark bits are embedded by modifying the coefficients in the first column of the left singular vector matrix of the target blocks. Lai et al. [48] has introduced an image watermarking scheme based on human visual system (HVS) and SVD. The embedding process of the scheme is same as in [14], while the embedding blocks are selected based on the sum of visual and edge entropy. The scheme of Fan et al. [27] is an advanced version of the scheme proposed by Chang [14], that promoted the transparency of the scheme by incorporating compensation operation. According to their scheme, the damage in the quality due to insertion of the watermark in the left singular vector matrix is compensated by modifying the right singular vector matrix.

1.4 Steganography

For decades, people attempted to develop innovative methods for secret communication. Steganography is an area of information security, which conceals information in a cover media for secret communication. A thorough history of steganography can be found in the literature [82]. The word steganography is of Greek origin. It is derived from two Greek words “stegos” which means “cover” and “grafia” which means “writing” [87]. It is generally used for the secure communication to hide it from attackers that create difficulties for unintended user to extract the information.

Only the receiver of stego-media has the ability to extract the secret data. Steganalysis [65] is used for the detection of hidden information. Steganography is illustrated with a block diagram given in Fig.(1.4). It follows the similar computational steps as employed by a watermarking scheme. However, the goals are different of both the schemes. In the monarchy of this digital world, steganography has created an atmosphere of corporate vigilance that has produced various interesting applications. The challenge of steganography is to embed as much information as possible with maximum transparency.

In the recent past, many steganographic approaches have been proposed for secure communications. A detailed study of steganographic approaches and their classification based on different criteria are given in [17, 87, 92]. In this chapter steganographic schemes have been classified into spatial and frequency domain. The steganography schemes in spatial domain directly embed the secret data into the cover media by modifying its values to generate the stego-media [98]. Chang et al. [11] proposed a scheme to hide secret data in the least significant bit (LSB) of image pixels by using a dynamic programming strategy. Chan and Cheng [10] proposed a simple LSB substitution-based hiding technique, and Wang et al. [104] proposed an image-hiding method based on optimal LSB substitution and a genetic algorithm. Wu et al. [111] proposed a secret image sharing scheme by applying optimal pixel adjustment process to enhance the image quality under different payload capacity and various authentication bits conditions.

In order to speed up the transmission time over the Internet and reduce bandwidth usage, data compression is commonly used to reduce the amounts of data traveling over a communication network. Several widely accepted compression methods are vector quantization (VQ), discrete wavelet transformation (DWT), and discrete cosine transformation (DCT). One of the most common compression algorithms is VQ, which is an attractive option because of its simplicity and cost-effectiveness. Recently, Tu et al. [98] presented an advanced version of the steganographic scheme proposed in [15], which is based on a vector quantization image compression technique. The steganographic schemes based on DWT and DCT can be found in [12, 42, 58, 118].

Steganographic schemes in frequency domain make use of frequency oriented mechanisms such as discrete cosine transform (DCT), discrete wavelet transform (DWT), and Fresnel transform (FT). Chang et al. [12] have proposed the reversible data hiding in DCT coefficients of the medium frequency components in each block. Lin [58] has used a histogram shifting method for reversible data hiding in DCT coefficients. The bit-plane compression technique has been used in [118]. A frequency domain steganography based information hiding technique using Fresnel transform (FT), has been proposed in [69]. In this method, the Fresnelet coefficients of the least significant bit (LSB) at high frequency subbands are used to embed the QR coded secret message.

Due to their simplicity and speed, spatial domain schemes, and in particular least significant bit (LSB) replacement techniques are widely used for steganographic applications. However, LSB replacement techniques are vulnerable to statistical analysis, as well as slight manipulations of the stego-media. Hence, an attacker can destroy the hidden information by simply zeroing out the least significant bits of all pixels in the stego-media.

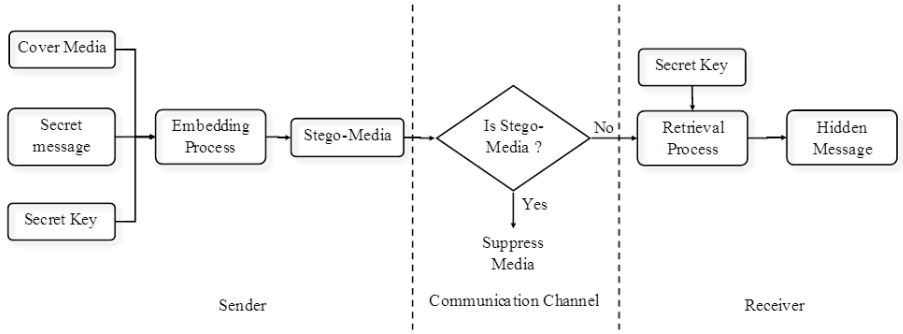

Figure 1.4: Illustration of steganography scheme for secret message hiding and its retrieval.

1.5 Application of Artificial Intelligence in Data Hiding

Many schemes ranging from conventional to artificial intelligence-based have been proposed to deal with multimedia data hiding problems [23, 33, 43, 50, 54, 55, 56, 98, 100, 101, 103, 114]. In the implementation of conventional data hiding schemes the users need to provide a good combination of algorithmic parameters to get the best performance. Furthermore, the hand-tuning of these parameters itself is a difficult task due to the complex interactions, even if one were to carry out preliminary experimentation, the optimal parameter settings may never be found. Also, the performance of data hiding schemes depends on the locations in cover media and the data to be hidden. To find the solution of all these problems many researchers have developed intelligent data hiding schemes [6, 71, 72, 108, 99, 116]. It is expected that intelligent data hiding schemes have better results in terms of robustness, transparency or tradeoff between them.

In the last two decades, artificial intelligence (AI) techniques such as evolutionary algorithms (EAs), support vector machine, fuzzy logic and neural networks have played an important role in data hiding [25, 71, 72, 83, 95, 94, 99, 105, 116, 121] for improving the performance. Under the category of evolutionary algorithms, genetic algorithm (GA) [7, 23, 25, 47, 71, 72, 81], particle swarm optimization (PSO) [53, 85, 94, 99, 108], differential evolution (DE) [4, 6, 2, 8, 52], Firefly algorithm [76], and artificial bee colony (ABC) [5] have made numerous valuable contributions to the field of data hiding. An image watermarking technique which uses a GA to find the optimal scaling factors for watermark insertion is designed by Lai [47]. In [81], the introduced technique is making use of a simple genetic algorithm in order to optimize the set of parameters for moments that significantly influences the locality properties alongside with the overall performance of the watermarking procedure. A blind image watermarking scheme in discrete wavelet transform-discrete cosine transform (DWT-DCT) utilizing GA, to achieve a predefined image quality after watermark insertion, is proposed in [7]. Application of GA in video steganography can be found in [23],

which is based on the concept of least significant bit (LSB). Wang et al. [108] have applied PSO to find the optimal threshold for quantization of wavelet coefficients. In [85] principal component of watermark was embedded instead of singular values of the watermark to prevent the false positive problem. Principal component was embedded in frequency domain and scaling factor was obtained by PSO. Fındık et al. [29], have applied the PSO for color image watermarking. A new audio watermarking scheme based on self-adaptive particle swarm optimization (SAPSO) and quaternion wavelet transform (QWT) is proposed by Lei et al. [53]. By obtaining optimal watermark strength using a uniquely designed objective function, SAPSO addresses the conflicting problem of robustness, imperceptibility, and capacity of audio watermarking scheme using self-adjusted parameters. Applications of DE algorithm for finding the optimal parameters for image watermarking can be found in [4, 6, 2, 8, 52]. Recently, Mishra et al. [76] implemented Firefly algorithm to find the optimal values of multiple scaling factors (MSFs) for watermark embedding. A relatively new member of evolutionary algorithms, artificial bee colony (ABC), is introduced in [5] for finding optimal watermarking parameters. It is observed from the literature that all these evolutionary algorithm based data hiding schemes have given better results in comparison to the conventional data hiding schemes.

The neural networks have shown a good potency in dealing with the data hiding problems [44, 83, 119]. The neural structure of the human eye is considered in human visual system (HVS). Therefore, it may be a good choice to achieve imperceptibility in the data hiding process. Hence, the data may be embedded to the locations, which are least sensitive to the human eyes. Since the human eye sensitivity is relatively complex, neural networks can learn the process and help data hiding schemes. Karimi et al. [44] applied the artificial neural networks to predict the most suitable areas for embedding to achieve the imperceptibility. The blocks, which produce the least amount of perceivable changes are selected by this method. A blind robust digital image watermarking approach based on back propagation neural network in DWT domain is presented in [83]. The back propagation neural network is implemented during both the process; embedding and extraction. Yu et al. [119] proposed a watermarking technique based on neural network for color images which can remind the relation between the logo and watermarked image. Since it modifies the intensity values of luminance in spatial domain, the watermark can easily be lost by image compression. A robust lossless watermarking technique, based on α-trimmed mean algorithm and support vector machine (SVM), for image authentication is proposed in [95]. SVM is trained to memorize relationship between the watermark and the image-dependent watermark other than embedding watermark into the host image. While needing to authenticate the ownership of the image, the trained SVM is used to recover the watermark and then the recovered watermark is compared with the original watermark to determine the ownership. Further application of SVM can be found in [105, 121].

The performance of data hiding schemes also improved by the hybridization of these artificial intelligence techniques [25, 71, 72, 94]. Tsai et al. [94] proposed a zero-watermark (lossless) scheme with geometrical invariants using support vector machine (SVM) classifier against geometrical attacks for image authentication. And the nearly optimal parameters of the SVM are obtained by particle swarm optimization (PSO)

algorithm. The hybridization of genetic algorithm and neural networks for the data hiding schemes can be found in [25, 72]. Maity et al. [71] proposed a watermarking scheme based on GA and fuzzy hybridization.

1.6 Summary

This chapter has reviewed some recent data hiding schemes. The aim of the chapter was to provide the complete detail of data hiding schemes that may help the new researchers to get the maximum knowledge of the topic. We tried to classify the data hiding schemes in all the known aspects like steganography watermarking, and data hiding schemes utilizing artificial intelligence. The exact classification of data hiding schemes is not possible, as many researchers have combined different approaches to develop hybrid schemes. Based on this review, the following recommendations may help interested users in data hiding for different purposes:

1. Steganography that is used for covert communication favor large capacity in comparison to watermarking.

2. Watermarking may be used for different purposes such as copyright protection and tamper detection.

3. Reversible data hiding schemes are quite useful where the quality of cover media is highly demanding such as military communication, healthcare, and law-enforcement.

4. Transformed domain data hiding schemes have better performance in comparison to spatial domain but computationally are expensive.

5. Artificial intelligence based data hiding schemes are easy to implement, as these performs without user intervention, and effective in comparison to conventional data hiding schemes.

Acknowledgments

This work was supported under the framework of international cooperation program managed by NRF of Korea (NRF-2013K2A1B9066056).

References

[1] O.M. Al-Qershi and B.E. Khoo. High capacity data hiding schemes for medical images based on difference expansion. *Journal of Systems and Software*, 84(1):105–112, 2011.

[2] M. Ali and C.W. Ahn. An optimized watermarking technique based on self-adaptive DE in DWT–SVD transform domain. *Signal Processing*, 94:545–556, 2014.

[3] M. Ali and C.W. Ahn. Comments on 'Optimized gray-scale image watermarking using DWT-SVD and Firefly Algorithm'. *Expert Systems with Applications*, 42(5):2392–2394, 2015.

[4] M. Ali, C.W. Ahn, and M. Pant. A robust image watermarking technique using SVD and differential evolution in DCT domain. *Optik - International Journal for Light and Electron Optics*, 125(1):428–434, 2014.

[5] M. Ali, C.W. Ahn, M. Pant, and P. Siarry. An image watermarking scheme in wavelet domain with optimized compensation of singular value decomposition via artificial bee colony. *Information Sciences*, 301:44–60, 2015.

[6] M. Ali, C.W. Ahn, and P. Siarry. Differential evolution algorithm for the selection of optimal scaling factors in image watermarking. *Engineering Applications of Artificial Intelligence*, 31:15–26, 2014.

[7] S.H. Amiri and M. Jamzad. Robust watermarking against print and scan attack through efficient modeling algorithm. *Signal Processing: Image Communication*, 29(10):1181–1196, 2014.

[8] V. Aslantas. An optimal robust digital image watermarking based on SVD using differential evolution algorithm. *Optics Communications*, 282(5):769–777, 2009.

[9] A. Cedillo-Hernandez, M. Cedillo-Hernandez, M. Garcia-Vazquez, M. Nakano-Miyatake, H. Perez-Meana, and A. Ramirez-Acosta. Transcoding resilient video watermarking scheme based on spatio-temporal HVS and DCT. *Signal Processing*, 97:40–54, 2014.

[10] C.K. Chan and L.M. Cheng. Hiding data in images by simple LSB substitution. *Pattern Recognition*, 37(3):469–474, 2004.

[11] C.C. Chang, J.Y. Hsiao, and C.S. Chan. Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy. *Pattern Recognition*, 36(7):1583–1595, 2003.

[12] C.C. Chang, C.C. Lin, C.S. Tseng, and W.L. Tai. Reversible hiding in DCT-based compressed images. *Information Sciences*, 177(13):2768–2786, 2007.

[13] C.C. Chang, T.S. Nguyen, and C.C. Lin. A reversible compression code hiding using SOC and SMVQ indices. *Information Sciences*, 300:85–99, 2015.

[14] C.C. Chang, P. Tsai, and C.C. Lin. SVD-based digital image watermarking scheme. *Pattern Recognition Letters*, 26(10):1577–1586, 2005.

[15] C.C. Chang, W.C. Wu, and Y.C. Hu. Lossless recovery of a VQ index table with embedded secret data. *Journal of Visual Communication and Image Representation*, 18(3):207–216, 2007.

[16] I.C. Chang, Y.C. Hu, W.L. Chen, and C.C. Lo. High capacity reversible data hiding scheme based on residual histogram shifting for block truncation coding. *Signal Processing*, 108:376–388, 2015.

[17] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt. Digital image steganography: survey and analysis of current methods. *Signal Processing*, 90(3):727–752, 2010.

[18] B. Chen, G. Coatrieux, G. Chen, X. Sun, J.L. Coatrieux, and H. Shu. Full 4-D quaternion discrete Fourier transform based watermarking for color images. *Digital Signal Processing*, 28:106–119, 2014.

[19] T.H. Chen, C.C. Chang, C.S. Wu, and D.C. Lou. On the security of a copyright protection scheme based on visual cryptography. *Computer Standards &*

Interfaces, 31(1):1–5, 2009.

[20] I. Cox, M.L. Miller, and J.A. Bloom. *Digital watermarking*. Morgan Kaufmann Publishers Inc. San Francisco, CA, USA, 2002.

[21] I.J. Cox, J. Kilian, F.T. Leighton, and T. Shamoon. Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, 6(12):1673–1687, 1997.

[22] S. Dadkhah, A.A. Manaf, Y. Hori, A.E. Hassaniend, and S. Sadeghi. An effective SVD-based image tampering detection and self-recovery using active watermarking. *Signal Processing: Image Communication*, 29(10):1197–1210, 2014.

[23] K. Dasgupta, J.K. Mondal, and P. Dutta. Optimized video steganography using Genetic Algorithm (ga). *Procedia Technology*, 10:131–137, 2013.

[24] J.J. Eggers, R. Baeuml, and B. Girod. Communications approach to image steganography. In *Security and Watermarking of Multimedia Contents IV*, volume 4675 of *SPIE*, pages 26–37, 2002.

[25] N.N. El-Emam and R.A.S. AL-Zubidy. New steganography algorithm to conceal a large amount of secret message using hybrid adaptive neural networks with modified adaptive genetic algorithm. *Journal of Systems and Software*, 86(6):1465–1481, 2013.

[26] E.H. Elshazly, O.S. Faragallah, A.M. Abbas, M.A. Ashour, E.S.M. El-Rabaie, H. Kazemian, S.A. Alshebeili, F.E. Abd El-Samie, and H.S.El-sayed. Robust and secure fractional wavelet image watermarking. *Signal, Image and Video Processing*, 2014. in press.

[27] M.Q. Fan, H.X. Wang, and S.K. Li. Restudy on SVD-based watermarking scheme. *Applied Mathematics and Computation*, 203(2):926–930, 2008.

[28] O.S. Faragallah. Efficient video watermarking based on singular value decomposition in the discrete wavelet transform domain. *AEU - International Journal of Electronics and Communications*, 67(3):189–196, 2013.

[29] O. Findik, I. Babaoglu, and E. Ulker. A color image watermarking scheme based on hybrid classification method: particle swarm optimization and k-nearest neighbor algorithm. *Optics Communications*, 283(24):4916–4922, 2010.

[30] D.S. Fu, Z.J. Jing, S.G. Zhao, and J. Fan. Reversible data hiding based on prediction-error histogram shifting and EMD mechanism. *AEU - International Journal of Electronics and Communications*, 68(10):933–943, 2014.

[31] X. Gao, L. An, Y. Yuan, D. Tao, and X. Li. Lossless data embedding using generalized statistical quantity histogram. *IEEE Transactions on Circuits and Systems for Video Technology*, 21(8):1061–1070, 2011.

[32] Q. Gu and T. Gao. A novel reversible robust watermarking algorithm based on chaotic system. *Digital Signal Processing*, 23(1):213–217, 2013.

[33] X. Gui, X. Li, and B. Yang. A high capacity reversible data hiding scheme based on generalized prediction-error expansion and adaptive embedding. *Signal Processing*, 98:370–380, 2014.

[34] J.M. Guo and H. Prasetyo. False-positive-free SVD-based image watermarking. *Journal of Visual Communication and Image Representation*, 25(5):1149–11632, 2014.

[35] J.M. Guo and H. Prasetyo. Security analyses of the watermarking scheme

based on redundant discrete wavelet transform and singular value decomposition. *AEU - International Journal of Electronics and Communications*, 68(9):816–834, 2014.

[36] W. Hong. Adaptive reversible data hiding method based on error energy control and histogram shifting. *Optics Communications*, 285(2):101–108, 2012.

[37] H.T. Hu and L.Y. Hsu. Exploring DWT¨cSVD¨cDCT feature parameters for robust multiple watermarking against JPEG and JPEG2000 compression. *Computers & Electrical Engineering*, 41:52–63, 2015.

[38] H.T. Hu and L.Y. Hsu. Robust, transparent and high-capacity audio watermarking in DCT domain. *Signal Processing*, 109:226–235, 2015.

[39] H.T. Hu, L.Y. Hsu, and H.H. Chou. Perceptual-based DWPT-DCT framework for selective blind audio watermarking. *Signal Processing*, 105:316–327, 2014.

[40] L.C. Huang, L.Y. Tseng, and M.S. Hwang. A reversible data hiding method by histogram shifting in high quality medical images. *Journal of Systems and Software*, 86(3):716–727, 2013.

[41] E. Hussein and M.A. Belal. Digital watermarking techniques, applications and attacks applied to digital media: a survey. *International Journal of Engineering Research & Technology*, 1(7):1–8, 2012.

[42] R. Jafari, D. Ziou, and M.M. Rashidi. Increasing image compression rate using steganography. *Expert Systems with Applications*, 40(17):6918–6927, 2013.

[43] K.H. Jung and K.Y. Yoo. Data hiding method in binary images based on block masking for key authentication. *Information Sciences*, 277:188–196, 2014.

[44] M. Karimi, M. Mohrekesh, S. Azizi, and S. Samavi. Transparent watermarking based on psychovisual properties using neural networks. In *8th Iranian Conference on Machine Vision and Image Processing (MVIP)*, pages 33–37, 2013.

[45] M. Khalil and A. Adib. Audio watermarking with high embedding capacity based on multiple access techniques. *Digital Signal Processing*, 34:116–125, 2014.

[46] A. Khan, A. Siddiqa, S. Munib, and S. A. Malik. A recent survey of reversible watermarking techniques. *Information Sciences*, 279:251–272, 2014.

[47] C.C. Lai. A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm. *Digital Signal Processing*, 21(4):522–527, 2011.

[48] C.C. Lai. An improved SVD-based watermarking scheme using human visual characteristics. *Optics Communications*, 284(4):938–944, 2011.

[49] J. Lang and Z.G. Zhang. Blind digital watermarking method in the fractional Fourier transform domain. *Optics and Lasers in Engineering*, 53:112–121, 2014.

[50] C.W. Lee and W.H. Tsai. A data hiding method based on information sharing via PNG images for applications of color image authentication and metadata embedding. *Signal Processing*, 93(7):2010–2025, 2013.

[51] S.H. Lee. DWT based coding DNA watermarking for DNA copyright protection. *Information Sciences*, 273:263–286, 2014.

[52] B. Lei, E.L. Tan, S. Chen, D. Ni, T. Wang, and H. Lei. Reversible watermarking scheme for medical image based on differential evolution. *Expert Systems with Applications*, 41(7):3178–3188, 2014.

[53] B. Lei, F. Zhou, E.L. Tanc, D. Ni, H. Lei, S. Chen, and T. Wang. Optimal and secure audio watermarking scheme based on self-adaptive particle swarm optimization and quaternion wavelet transform. *Signal Processing*, 113:80–94,

2015.

[54] H.Y. Leung, L.M. Cheng, F. Liu, and Q.K. Fu. Adaptive reversible data hiding based on block median preservation and modification of prediction errors. *Journal of Systems and Software*, 86(8):2204–2219, 2013.

[55] X. Li, J. Li, B. Li, and B. Yang. High-fidelity reversible data hiding scheme based on pixel-value-ordering and prediction-error expansion. *Signal Processing*, 93(1):198–205, 2013.

[56] C.C. Lin, X.L. Liu, and S.M. Yuan. Reversible data hiding for VQ-compressed images based on search-order coding and state-codebook mapping. *Information Sciences*, 293:314–326, 2015.

[57] S.D. Lin, S.-C. Shie, and J.Y. Guo. Improving the robustness of DCT-based image watermarking against JPEG compression. *Computer Standards & Interfaces*, 32(1-2):54–60, 2010.

[58] Y.K. Lin. High capacity reversible data hiding scheme based upon discrete cosine transformation. *Journal of Systems and Software*, 85(10):2395–2404, 2012.

[59] H.C. Ling, R.C.W. Phan, and S.H. Heng. On an optimal robust digital image watermarking based on SVD using differential evolution algorithm. *Optics Communications*, 282(5):769–777, 2009.

[60] H.C. Ling, R.C.W. Phan, and S.H. Heng. On the security of a hybrid watermarking algorithm based on singular value decomposition and Radon transform. *AEU - International Journal of Electronics and Communications*, 65(11):958–960, 2011.

[61] H.C. Ling, R.C.W. Phan, and S.H. Heng. Comment on 'Robust blind image watermarking scheme based on Redundant Discrete Wavelet Transform and Singular Value Decomposition'. *AEU - International Journal of Electronics and Communications*, 67(10):894–897, 2013.

[62] J.C. Liu and S.Y. Chen. Fast two-layer image watermarking without referring to the original image and watermark. *Image and Vision Computing*, 19(14):1083–1097, 2001.

[63] R. Liu and T. Tan. An SVD-based watermarking scheme for protecting rightful ownership. *IEEE Transactions on Multimedia*, 4(1):121–128, 2002.

[64] Y. Liu and J. Zhao. A new video watermarking algorithm based on 1D DFT and Radon transform. *Signal Processing*, 90(2):626–639, 2010.

[65] D.C. Lou, C.L. Chou, H.K. Tso, and C.C. Chiu. Active steganalysis for histogram-shifting based reversible data hiding. *Optics Communications*, 285(10-11):2510–2518, 2012.

[66] D.C. Lou, H.K. Tso, and J.L. Liu. A copyright protection scheme for digital images using visual cryptography technique. *Computer Standards & Interfaces*, 29(1):125–131, 2007.

[67] W. Lu, H. Lu, and F.L. Chung. Feature based robust watermarking using image normalization. *Computers & Electrical Engineering*, 36(1):2–18, 2010.

[68] X. Ma, Z. Pan, S. Hu, and L. Wang. Reversible data hiding scheme for VQ indices based on modified locally adaptive coding and double-layer embedding strategy. *Journal of Visual Communication and Image Representation*, 28:60–70, 2015.

[69] S.U. Maheswari and D.J. Hemanth. Frequency domain QR code based image

steganography using Fresnelet transform. *AEU - International Journal of Electronics and Communications*, 69(2):539–544, 2015.

[70] S.P. Maity and M.K. Kundu. DHT domain digital watermarking with low loss in image informations. *AEU - International Journal of Electronics and Communications*, 64(3):243–257, 2010.

[71] S.P. Maity, S. Maity, J. Sil, and C. Delpha. Collusion resilient spread spectrum watermarking in M-band wavelets using GA-fuzzy hybridization. *Journal of Systems and Software*, 86(1):47–59, 2013.

[72] S.P. Maity, S. Maity, J. Sil, and C. Delpha. Perceptually adaptive MC-SS image watermarking using GA-NN hybridization in fading gain. *Engineering Applications of Artificial Intelligence*, 31:3–14, 2014.

[73] N.M. Makbol and B.E. Khoo. Robust blind image watermarking scheme based on Redundant Discrete Wavelet Transform and Singular Value Decomposition. *AEU - International Journal of Electronics and Communications*, 67(2):102–112, 2013.

[74] N.M. Makbol and B.E. Khoo. A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition. *Digital Signal Processing*, 33:134–147, 2014.

[75] J. Mielikainen. LSB matching revisited. *IEEE Signal Processing Letters*, 13(5):285–287, 2006.

[76] A. Mishra, C. Agarwal, A. Sharma, and P. Bedi. Optimized gray-scale image watermarking using DWT¨CSVD and Firefly Algorithm. *Expert Systems with Applications*, 41(17):7858–7867, 2014.

[77] A.A. Mohammad, A. Alhaj, and S. Shaltaf. An improved SVD-based watermarking scheme for protecting rightful ownership. *Signal Processing*, 88(9):2158–2180, 2008.

[78] P. Moulin and J.A. O'Sullivan. Information-theoretic analysis of information hiding. *IEEE Transactions on Information Theory*, 49(3):563–593, 2003.

[79] N. Nikolaidis and I. Pitas. Robust image watermarking in the spatial domain. *Signal Processing*, 66(3):385–403, 1998.

[80] B. Ou, X. Li, Y. Zhao, and R. Ni. Reversible data hiding using invariant pixel-value-ordering and prediction-error expansion. *Signal Processing: Image Communication*, 29(7):760–772, 2014.

[81] G.A. Papakostas, E.D. Tsougenis, and D.E. Koulouriotis. Moment-based local image watermarking via genetic optimization. *Applied Mathematics and Computation*, 227:222–236, 2014.

[82] N. Provos and P. Honeyman. Hide and seek: an introduction to steganography. *IEEE Security & Privacy*, 1(3):32–44, 2003.

[83] N. Ramamurthy and S. Varadarajan. The robust digital image watermarking scheme with back propagation neural network in DWT domain. *Procedia Engineering*, 38:3769–3778, 2012.

[84] S. Rastegar, F. Namazi, K. Yaghmaie, and A. Aliabadian. Hybrid watermarking algorithm based on Singular Value Decomposition and Radon transform. *AEU - International Journal of Electronics and Communications*, 65(7):658–663, 2011.

[85] R.S. Run, S.J. Horng, J.L. Lai, T.W. Kao, and R.J. Chen. An improved SVD-based watermarking technique for copyright protection. *Expert Systems with*

Applications, 39(1):673–689, 2012.

[86] R. Rykaczewski. Comments on 'An SVD-based watermarking scheme for protecting rightful Ownership'. *IEEE Transactions on Multimedia*, 9(2):421–423, 2007.

[87] M.M. Sadek, A.S. Khalifa, and M.G.M. Mostafa. Video steganography: a comprehensive review. *Multimedia Tools and Applications*, 2014. in press.

[88] M.J. Sahraee and S. Ghofrani. A robust blind watermarking method using quantization of distance between wavelet coefficients. *Signal, Image and Video Processing*, 7(4):799–807, 2013.

[89] S.C. Shie, S.D. Lin, and J.H. Jiang. Visually imperceptible image hiding scheme based on vector quantization. *Information Processing & Management*, 46(5):495–501, 2010.

[90] C. Song, S. Sudirman, and M. Merabti. A robust region-adaptive dual image watermarking technique. *Journal of Visual Communication and Image Representation*, 23(3):549–568, 2012.

[91] Q. Su, Y. Niu, H. Zou, and X. Liu. A blind dual color images watermarking based on singular value decomposition. *Applied Mathematics and Computation*, 219(16):8455–8466, 2013.

[92] M.S. Subhedar and V.H. Mankar. Current status and key issues in image steganography: a survey. *Computer Science Review*, 13-14:95–113, 2014.

[93] G.C.W. Ting. Ambiguity attacks on the Ganic-Eskicioglu robust DWT-SVD image watermarking scheme. In *Information Security and Cryptology (ICISC)*, volume 3935, pages 378–388, 2006.

[94] H.H. Tsai, Y.S. Lai, and S.C. Lo. A zero-watermark scheme with geometrical invariants using SVM and PSO against geometrical attacks for image protection. *Journal of Systems and Software*, 86(2):335–348, 2013.

[95] H.H. Tsai, H.C. Tseng, and Y.S. Lai. Robust lossless image watermarking based on α-trimmed mean algorithm and support vector machine. *Journal of Systems and Software*, 83(6):1015–1028, 2010.

[96] P. Tsai, Y.C. Hu, and H.L. Yeh. Reversible image hiding scheme using predictive coding and histogram shifting. *Signal Processing*, 89(6):1129–1143, 2009.

[97] Y.S. Tsai and P. Tsai. Adaptive data hiding for vector quantization images based on overlapping codeword clustering. *Information Sciences*, 181(15):3188–3198, 2011.

[98] T.Y. Tu and C.H. Wang. Reversible data hiding with high payload based on referred frequency for VQ compressed codes index. *Signal Processing*, 108:278–287, 2015.

[99] E. Vellasques, R. Sabourin, and E. Granger. Fast intelligent watermarking of heterogeneous image streams through mixture modeling of PSO populations. *Applied Soft Computing*, 13(6):3130–3148, 2013.

[100] C.T. Wang and H.F. Yu. A Markov-based reversible data hiding method based on histogram shifting. *Journal of Visual Communication and Image Representation*, 23(5):798–811, 2012.

[101] L. Wang, Z. Pan, X. Ma, and S. Hu. A novel high-performance reversible data hiding scheme using SMVQ and improved locally adaptive coding method. *Journal of Visual Communication and Image Representation*, 25(2):454–465,

2014.

[102] M.S. Wang and W.C. Chen. A hybrid DWT-SVD copyright protection scheme based on k-means clustering and visual cryptography. *Computer Standards & Interfaces*, 31(4):757–762, 2009.

[103] N. Wang, H. Zhang, and C. Mena. A high capacity reversible data hiding method for 2D vector maps based on virtual coordinates. *Computer-Aided Design*, 47:108–117, 2014.

[104] R.Z. Wang, C.F. Lin, and J.C. Lin. Image hiding by optimal LSB substitution and genetic algorithm. *Pattern Recognition*, 34(3):671–683, 2001.

[105] X.Y. Wang, E.N. Miao, and H.Y. Yang. A new SVM-based image watermarking using Gaussian–Hermite moments. *Applied Soft Computing*, 12(2):887–903, 2012.

[106] X.Y. Wang, Y.P. Yang, and H.Y. Yang. Invariant image watermarking using multi-scale Harris detector and wavelet moments. *Computers & Electrical Engineering*, 36(1):31–44, 2010.

[107] Y. Wang and A. Pearmain. Blind image data hiding based on self reference. *Pattern Recognition Letters*, 25(15):1681–1689, 2004.

[108] Y.R. Wang, W.H. Lin, and L. Yang. An intelligent watermarking method based on particle swarm optimization. *Expert Systems with Applications*, 38(7):8024–8029, 2011.

[109] Z. Wang, A.C. Bovik, H.R. Sheikh, and E.P. Simoncelli. Image quality assessment: from error visibility to structural similarity. *IEEE Transactions on Image Processing*, 13(4):600–612, 2004.

[110] Z.H. Wang, C.F. Lee, and C.Y. Chang. Histogram-shifting-imitated reversible data hiding. *Journal of Systems and Software*, 86(2):315–323, 2013.

[111] C.C. Wu, S.J. Kao, and M.S. Hwang. A high quality image sharing with steganography and adaptive authentication scheme. *Journal of Systems and Software*, 84(12):2196–2207, 2011.

[112] H.C. Wu, C.C. Lee, C.S. Tsai, Y.P. Chu, and H.R. Chen. A high capacity reversible data hiding scheme with edge prediction and difference expansion. *Journal of Systems and Software*, 82(12):1966–1973, 2009.

[113] X. Wu and W. Sun. Robust copyright protection scheme for digital images using overlapping DCT and SVD. *Applied Soft Computing*, 13(2):1170–1182, 2013.

[114] X. Wu and W. Sun. High-capacity reversible data hiding in encrypted images by prediction error. *Signal Processing*, 104:387–400, 2014.

[115] C.H. Yang, C.Y. Weng, S.J. Wang, and H.M. Sun. Adaptive data hiding in edge areas of images with spatial LSB domain systems. *IEEE Transactions on Information Forensics and Security*, 3(3):488–497, 2008.

[116] H.Y. Yang, X.Y. Wang, Y. Zhang, and M. E-nuo. Robust digital watermarking in PDTDFB domain based on least squares support vector machine. *Engineering Applications of Artificial Intelligence*, 26(9):2058–2072, 2013.

[117] N.I. Yassin, N.M. Salem, and M.I. El Adawy. Qim blind video watermarking scheme based on Wavelet transform and principal component analysis. *Alexandria Engineering Journal*, 53(4):833–842, 2014.

[118] H.L. Yeh, S.T. Gue, P. Tsai, and W.K. Shih. Wavelet bit-plane based data hiding for compressed images. *AEU - International Journal of Electronics and*

Communications, 67(9):808–815, 2013.

[119] P.T. Yu, H.H. Tsai, and J.S. Lin. Digital watermarking based on neural networks for color images. *Signal Processing*, 81(3):663–671, 2001.

[120] X.P. Zhang and K. Li. Comments on 'An SVD-based watermarking scheme for protecting rightful Ownership'. *IEEE Transactions on Multimedia*, 7(3):593–594, 2005.

[121] P.P. Zheng, J. Feng, Z. Li, and M. Zhou. A novel SVD and LS-SVM combination algorithm for blind watermarking. *Neurocomputing*, 142:520–528, 2014.

[122] X. Zhu, J. Zhao, and H. Xu. A digital watermarking algorithm and implementation based on improved SVD. In *18th International Conference on Pattern Recognition (ICPR)*, volume 3, pages 651–656, 2006.