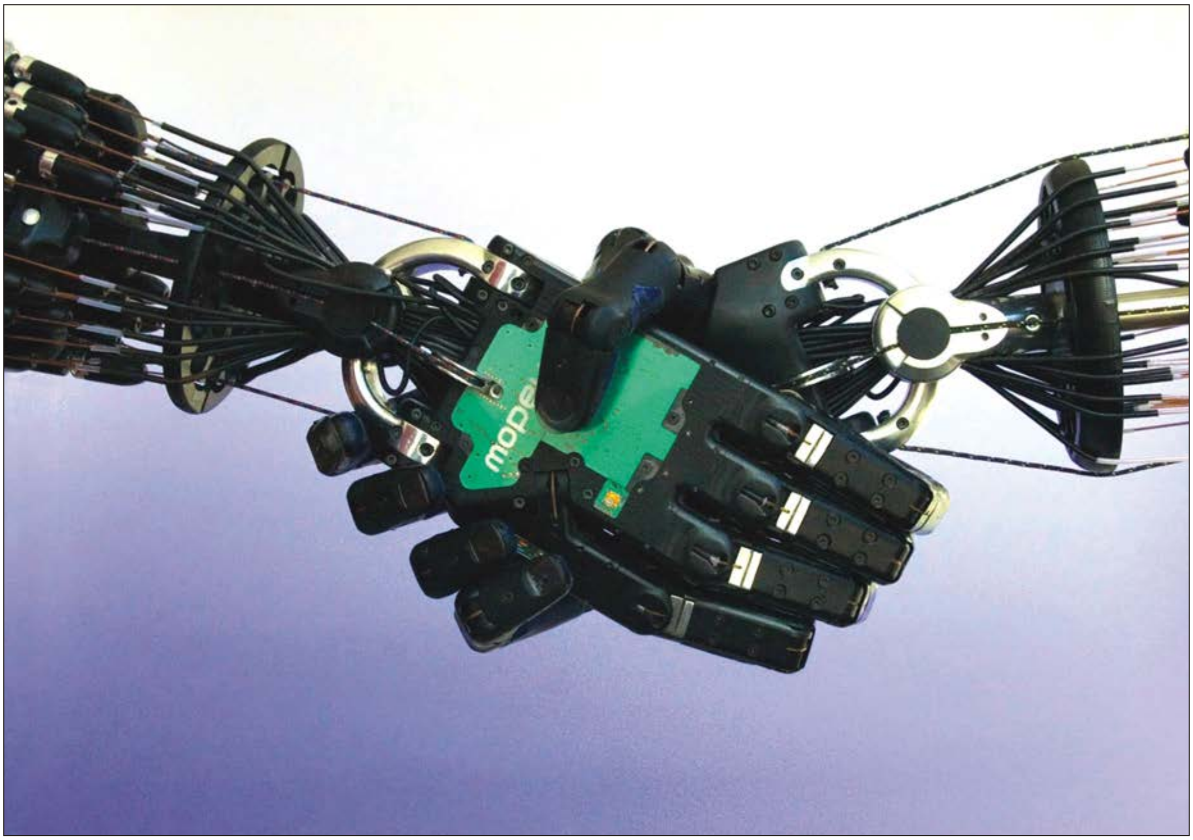

Journal of Artificial Intelligence

ISSN 1994-5450

science alert

ANSInet
an open access publisher
http://ansinet.com

OPEN ACCESS Journal of Artificial Intelligence

ISSN 1994-5450
DOI: 10.3923/jai.2017.1.21

Review Article

Data Security Through Data Hiding in Images: A Review

[1]Ahmad Shaik, [1]V. Thanikaiselvan and [2]Rengarajan Amitharajan

[1]School of Electronics Engineering, VIT University, 632014 Vellore, Tamilnadu, India
[2]School of Electrical and Electronics Engineering, SASTRA University, 613 401 Thanjavur, India

Abstract

High speed communication networks facilitate the simple and rapid mode of online information sharing with high data rates. But the channels which are used for data sharing are not secure. The subject of data security emerges in such scenarios. To achieve this, different security methods are being used in digital communication. Cryptography is one of the popular techniques, but the scrambled appearance of encrypted information can lead to high probability of attacks. Hiding information in a cover is one of the alternatives to cryptography. The main objective of this study is to provide an overall idea about the popular as well as emerging data hiding techniques in spatial and transform domains. This study deals with both reversible and non-reversible data hiding methods. Also, this study briefly discusses some common steganalytic techniques and concludes with an idea of the future scope of Reversible Data Hiding (RDH). The wide range of these techniques will provide a good overview about current trends in transform domain steganography to the researchers who are interested in steganography.

Key words: Data hiding, steganography, watermarking, spatial domain, transform domain, information security

Received: August 10, 2016 Accepted: November 03, 2016 Published: December 15, 2016

Citation: Ahmad Shaik, V. Thanikaiselvan and Rengarajan Amitharajan, 2017. Data security through data hiding in images: A review. J. Artif. Intel., 10: 1-21.

Corresponding Author: Rengarajan Amirtharajan, School of Electrical and Electronics Engineering, SASTRA University, 613 401 Thanjavur, India

Competing Interest: The authors have declared that no competing interest exists.

Data Availability: All relevant data are within the paper and its supporting information files.

INTRODUCTION

Communication of digital information becomes frequent nowadays, because of its fast access capability. A wide range of technologies for end-to-end protection are needed to resist the security threats in modern communication. Figure 1 represents the different types of available information security systems.

Data hiding and cryptography are the two main techniques for secure communication. In cryptography, the plain data is changed into an unreadable form called cipher data. The limitation of cryptography is that the third party is always conscious about the communication of incomprehensible data. In data hiding, the data is hidden in a cover file and it will be transmitted over the network. Hiding the existence of secret information is the main advantage of data hiding techniques over cryptography. There are some applications which use both encryption and data hiding in same process[1-3].

Digital watermarking, steganography and Reversible Data Hiding (RDH) are the types of data hiding approaches. Watermarking is a sequence of digital bits placed in a digital cover file that recognizes the file's copyright information[4]. Steganography is dedicated for covert communication. It changes the image in such a way that only the sender and the intended receiver can detect the message sent through it. Since it is invisible, the detection of secret data is not simple. In steganography, the cover file does not hold any significance after extraction of secret data. Whereas in RDH the cover file also holds the information like secret data. The RDH allows one to embed a relatively large amount of data into an image in such a way that the original image can be reconstructed from the marked image. This makes it an ideal technique for applications where one wants to store metadata into the cover signal, while recover the original signal without loss after data extraction. Thorough knowledge about data hiding can be found by Amirtharajan *et al.*[5], Amirtharajan and Rayappan[6], Chandramouli *et al.*[7], Chanu *et al.*[8], Goel *et al.*[9], Hussain and Hussain[10] and Saha and Sharma[11]. This study mainly concentrates on data hiding in digital images in terms of steganography and RDH.

Steganography or the concept of data hiding was first mentioned in a work by Johannes Trithemus (1462-1516) titled "Steganographia". The word "Steganography" is derived from two Greek words "Steganos" and "graphia" (στεγανό-ς, γραφ-ειν) meaning "Covered" and "Writing". Steganography has been used over the centuries. It is documented that in 480BC Demaratus sent a warning to the spartans using steganography to intimate the allies that Xerxe's army approaching their country for war. According to the modern world, the idea of information hiding or steganography was initially presented with the case of prisoner's mystery message by Simmons[12] and Petitcolas *et al.*[13].

Applications of data hiding: In an age where knowledge is power, data hiding gives a good way to secure data as it gives a way to hide information in a host (cover) without destroying its original value. Watermarks are used to hide known messages in pieces of data to protect the copyright information of the data. Steganography hides secret messages in digital cover files so as to conceal the fact that some message is being transmitted.

Digital watermarking techniques are used to protect the copyright of digital files. A variety of watermarking schemes have been suggested to safeguard the digital media like music, images, official documents, etc. Digital watermarks can be used in the form of logos or images in a corner of a document or they can be invisible like in the case of digital signatures. Digital watermarking is commonly used in E-commerce to provide conditional and user specific access to some resources. Hence, the use of digital watermarking encourages creative professionals to use the internet so that their work can reach a wider audience.

As opposed to watermarking, the data hidden in the cover is of utmost importance in steganography. Steganography hides secret and sensitive data in host files such that its existence is concealed. Hence, it provides secure communication with privacy in the internet. This can have numerous applications in areas where secrecy is crucial. It can be used in medical, military, law enforcement, intelligence and counter-intelligence agencies to achieve covert data exchange.

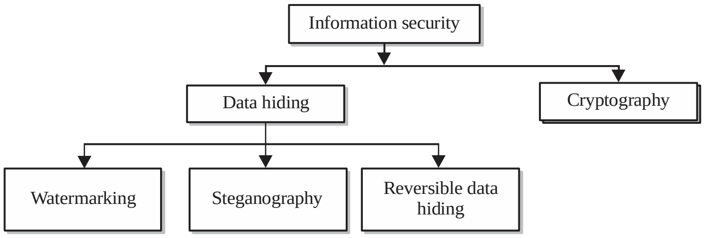

Fig. 1: Types of information security systems

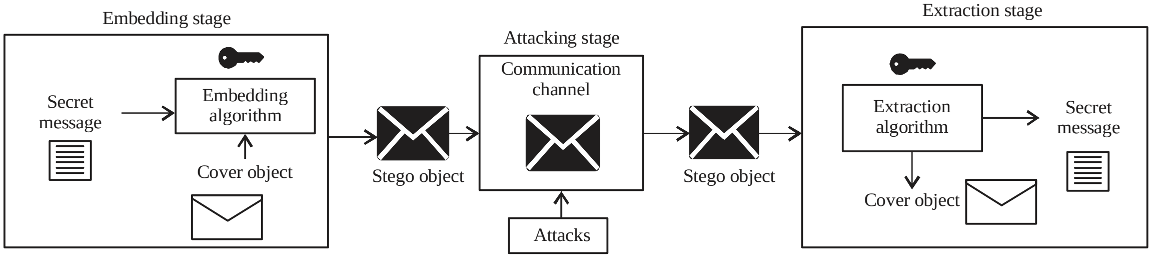

Fig. 2: Process of data hiding system

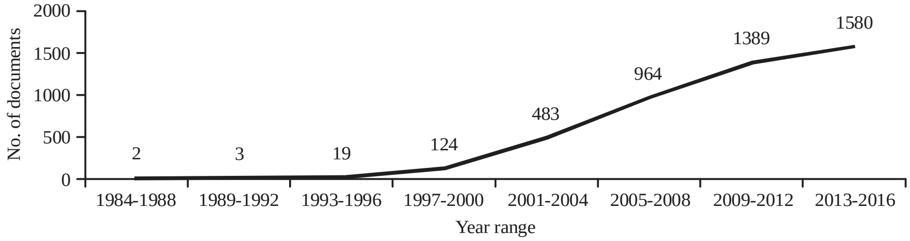

Fig. 3: Scopus search results for image data hiding (http://www.scopus.com/results/results.uri?)

Process of data hiding: The process of data hiding can be classified into three stages namely embedding stage, attacking stage and extraction stage as shown in Fig. 2. In the embedding stage the secret data is embedded in the cover object by using the embedding algorithm and the secret key. Then the stego object is created and transmitted over the network. In the extraction stage, the secret data is extracted from the stego object by performing the extraction algorithm using secret key. In the network, there is a possibility that either someone attacks the stego file or it gets corrupted by some noise. If this happened means, the stego data is either altered or destroyed, hence, it is called as the attacking stage[14].

Basic properties of data hiding: To design a perfect data hiding system, the following factors are to be considered:

- **Imperceptibility:** It is the capability of the technique to pass information undetected by the Human Visual System (HVS)
- **Security:** It is the resistance of the technique to an attack even after realization of the existence of secret data
- **Capacity (Payload):** It is the amount of data that can be concealed in the cover object without affecting its visual quality
- **Robustness:** It is the ability of the stego object to oppose unintentional actions like filtering, cropping, rotation, compression, etc.
- **Embedding complexity:** It measures the complexity of the data embedding algorithm

Different types of digital objects like text, image, audio and video are popular as cover files in data hiding[11]. Text data hiding lacks in security and embedding capacity. Audio and video files are moving streams of information, any small change is noticeable. Image data hiding provides acceptable static redundant information to embed secret data, therefore, the images are the most commonly used file format. Data hiding in digital images is a rapidly growing area of research. Figure 3 shows the data for documents published on image data hiding in scopus indexed publications from the year 1984-2016.

Steganalysis is an art of detecting hidden data in the stego objects. Along with the data hiding techniques, data detecting methods have also improved in their performance. The developments in steganalysis improved the standards of the steganography and vice versa. Steganalysis is of two major types namely targeted and blind steganalysis.

IMAGE DATA HIDING

Image data hiding is mainly used for covert communication. In image steganography the embedding algorithm E_M will convert the cover image I_C into stego image I_S by embedding secret data D into it. The embedding process may use the stego key K for high security. Mathematically, the embedding and extraction processes are represented using Eq. 1 and 2:

$$I_S = E_M (I_C, D, K) \quad (1)$$

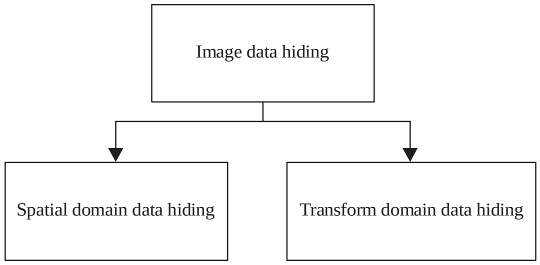

Fig. 4: Types of image data hiding

$$D \approx E_X (I_S, K) \approx E_X (E_M (I_C, D, K), K) \quad (2)$$

where, E_X is the extraction algorithm. With the help of the key K it performs the inverse operation of E_M and recovers the secret data D from received stego image.

For some special cases, along with secret data the cover image should also be recovered. This type of data hiding is called Reversible Data Hiding (RDH)[15]. The RDH is of utmost importance in medical and military images wherein the cover file is more precious and should not be damaged. Kodak's patent[16] is the first proposed study on RDH. After that a number of RDH algorithms have been proposed[17,18].

Based on the way of embedding the secret bits, data hiding can be classified into two different types as shown in Fig. 4. Both the techniques are discussed in this study.

Performance evaluation parameters: This study introduces the parameters used to evaluate the performance of the data hiding techniques.

Bit Error Rate (BER): The BER gives the ratio of the bits in the stego image I_S which have intensities different from that of the cover image I_C giving by Thanikaiselvan *et al.*[14]. The BER is given as shown in Eq. 3:

$$\text{Bit error rate} = \frac{B_E}{B_C} \quad (3)$$

where, B_C is the total number of bits in the grayscale cover image. And B_E is the total number of bits differed from the stego image I_S. The B_E can be calculated using Eq. 4:

$$B_E = \sum_{i=1}^{n} \left| I_{Cbin} - I_{Sbin} \right| \quad (4)$$

where, I_{Cbin} and I_{Sbin} are the binary representations of the cover and stego images, respectively. The BER ranges from 0-1. Zero represents that the stego image is exactly equal to the cover image and 1 represents that stego image intensities are completely different from the cover image.

Peak Signal to Noise Ratio (PSNR): The PSNR is generally used to measure the quality of stego image in decibels (dB). Equation 5 gives the expression for PSNR in which I_{Cmax} is the maximum pixel value of the cover image and MSE is the mean square error:

$$\text{PSNR} = 10 \log_{10} \left(\frac{I_{Cmax}^2}{\text{MSE}} \right) \text{dB} \quad (5)$$

Where:

$$\text{MSE} = \frac{1}{MN} \sum_{x=1}^{M} \sum_{y=1}^{N} \left(I_{Sxy} - I_{Cxy} \right)^2 \quad (6)$$

In Eq. 6, x and y are the image coordinates, M and N are the dimensions of the image, I_{Sxy} is the generated stego-image and I_{Cxy} is the cover image.

Structural similarity (SSIM) index: The SSIM is a method for finding the similarity between cover image and the stego image. It is a perception-based model that considers image degradation as perceived change in structural information[14]. The SSIM measure between two images I_C and I_S is represented in Eq. 7:

$$\text{SSIM}(I_C, I_S) = \frac{\left(2\mu_{I_C}\mu_{I_S} + k_1\right)\left(2\sigma_{I_C,I_S} + k_2\right)}{\left(\mu_{I_C}^2 + \mu_{I_S}^2 + k_1\right)\left(\sigma_{I_C}^2 + \sigma_{I_S}^2 + k_2\right)} \quad (7)$$

where, μ_{I_C} is the average of I_C, μ_{I_S} is the average of I_S, $\sigma_{I_C}^2$ is the variance of I_C, $\sigma_{I_S}^2$ is the variance of I_S, σ_{I_C,I_S} is the covariance between I_C and I_S and k_1, k_2 are two the variables used to stabilize the division with weak denominator.

SPATIAL DOMAIN DATA HIDING

Spatial domain data hiding methods use a set of simple pixel manipulation techniques which generate space in the cover image to hide secret data where alterations won't be easily noticeable[1]. The various approaches for embedding in spatial domain are shown in the Fig. 5.

Least Significant Bit (LSB) modification: The LSB modification[19] was one of the first algorithms proposed for data hiding. It embeds the secret data in the LSBs of the cover

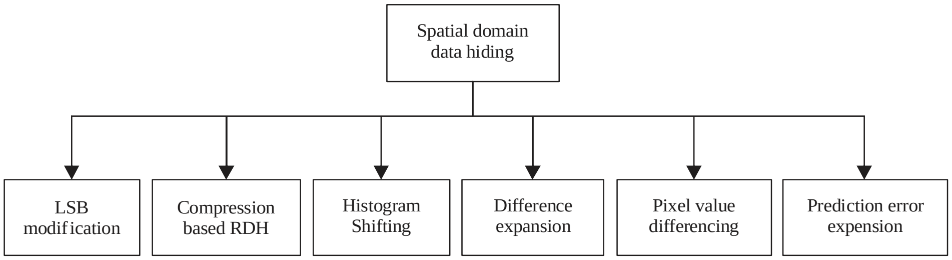

Fig. 5: Spatial domain data hiding techniques

Table 1: LSB based data hiding techniques

References	PSNR (dB)	Features
Chan and Cheng[19]	45.19	Optimal Pixel Adjustment Process (OPAP) is used to improve the quality of the stego image after embedding in k-bit LSB planes Performs well at high embedding rates (4 bpp) compared to standard LSB embedding
Wang *et al.*[21]	51.14	Randomized optimal LSB substitution is used to improve the data security Requires a very large processing time Embedding capacity is the same as Chan and Cheng[19]
Yang[22]	34.93	Inverted Pattern (IP) technique is used to reduce the error difference between original and modified values Visual quality is improved but MSE is decreased
Liao *et al.*[24]	41.58	Number of bit planes used is decided by the average difference values Marked images have decent PSNR values with high embedding capacities
Chen *et al.*[25]	42.30	Secret data is embedded in the edge areas of the cover image A combination of canny and fuzzy edge detection is used to detect the edges
Kuo *et al.*[23]	52.00	Uses Modified Signed Digit (MSD) and Exploiting Modification Direction (EMD) to embed secret data Maintains a minimum embedding capacity of 1 bpp Performs well against visual bit plane analysis and RS steganalysis
Lu *et al.*[26]	49.13	LSB matching and Dual imaging based RDH technique Supports capacity of 1 bpp Improved image quality as compared to Chan and Cheng[19]
Kanan and Nazeri[27]	45.12	Pixels are selected using a Genetic Algorithm (GA) Secure against RS steganalysis Maintains a good visual quality up to 4 bpp

image. Let be the 8 bit grayscale cover image of size MN and D be the n bit secret data. Equation 8 represents the mathematical representation of standard LSB embedding:

$$I_{Si} = I_{Ci} - I_{Ci} \bmod 2^k + d_i \tag{8}$$

where, I_{Si} is the ith modified pixel or stego image pixel value and d_i is ith k-bit secret data which is taken from D where k represents the number of bits embedded in each pixel. Hence, this technique is also called as k-bit LSB substitution. The hidden data can be extracted by using the same set of pixels used in Eq. 8 and doing a mod operation with 2^k. For k = 1, the steganographer will get a maximum capacity of 1 bpp (bits per pixel). As the k value increases the embedding capacity will improve but the stego image quality will reduce. After extraction of the secret data, the recovered image would not be the same as the cover image.

Primitive LSB[20,19] embedding techniques are insecure because of sequential embedding. This gave rise to random embedding techniques which have better security[21]. Later, a lot of other techniques were introduced to improve the security of LSB embedding techniques such as Inverted pattern[22] and Dynamic Programming Strategy (DPS)[23]. Some of the popular LSB based data hiding techniques are illustrated in Table 1.

The LSB modification techniques support high embedding capacity while maintaining better PSNR. But any modifications in the stego image leads to modification in secret data. Hence robustness of these methods is very low.

Compression based RDH: In this approach, spatial domain compression techniques are applied on bit planes of the cover image to generate space for secret data embedding[28]. A Generalized LSB (GLSB)[17] embedding is one of the earliest works in compression based data hiding. According to this scheme, the cover image is quantized and then the difference between quantized pixel value and cover pixel value are calculated. Those differences are compressed using lossless compression techniques. The compression provides some empty space to store the secret data. The compressed data and secret data are stored in the cover image to obtain the stego image. In the extraction stage, the secret data and

Table 2: Compression domain based data hiding techniques

References	PSNR (dB)	Features
Chang *et al.*[32]	32.48	VQ with three sub-groups of codewords are used in data hiding to find the closest match with secret data codewords Preprocessing improves the capacity and the visual quality of the stego image Achieves an average embedding capacity of 0.5 bpp
Lee *et al.*[31]	26.56	Data is hidden using VQ and Search Order Coding (SOC) Achieves capacity of 49 kb with low visual quality Resistant to image compression attacks
Tsai[34]	27.49	A prediction VQ-encoded image histogram is used to hide the data Low capacity (5 kb) and PSNR Robust against the chi-square test
Shie and Lin[35]	32.73	Uses VQ and SOC for adaptive data hiding Hiding capacity improves to almost double as compared to Lee *et al.*[31] Slight PSNR improvement as compared to Lee *et al.*[31]
Chang *et al.*[33]	30.78	Uses Side Match Vector Quantization (SMVQ) for compression Very less embedding capacity (16 kb) Longer processing time Restoring the original SMVQ-compressed cover image without any distortion is difficult
Shie and Jiang[36]	30.74	Uses Side Match Vector Quantization (SMVQ) for compression Capacity is improved almost 5.5 times and processing time is reduced four times compared to Chang *et al.*[33] Performs well against statistical chi-square attack
Wang *et al.*[37]	33.14	BTC and Prediction Error Expansion (PEE) based data hiding Low embedding capacity (20 kb)
Lin and Liu[38]	29.69	BTC and Histogram Shifting (HS) based data hiding Capacity is improved to 30 kb but PSNR is very less
Sun *et al.*[39]	33.19	Joint Neighbor Coding (JNC) and BTC-compression based data hiding Achieves good embedding capacity (60 kb) with a moderate PSNR

original cover data are recovered using decompression. This method is simple, but it requires huge auxiliary data that seriously affects the image quality and the capacity.

Primitive compression[17,28] based techniques are not robust against intentional attacks. Vector Quantization (VQ)[29] and Block Truncation Coding (BTC)[30] are two popular techniques used in compressed domain RDH. In VQ compression based data hiding, the compressed codewords of cover image are replaced with secret data codewords. But compressed conventional VQ indices require more bits for reconstruction. To overcome this, the Search Order Coding (SOC)[31] algorithm is developed. Some techniques use cluster of codewords[32] to increase the similarity between codewords of cover image and secret data. But all these methods fail to restore the cover image perfectly. Side Match Vector Quantization (SMVQ) has been developed[33], in order to get a perfect restoration of the cover image.

In BTC based data hiding, the secret data is hidden in the compressed block truncation codes. They use block based prediction techniques to generate residual values which are then used to embed data. Some of the other compression based techniques are reviewed in Table 2.

Compressed domain techniques perform well against standard stego attacks. But it requires high auxiliary data to recover the cover image, hence the data capacity and PSNR are low. Most of these algorithms require more time to process because of the computational complexity of the compression algorithms.

Histogram Shifting (HS): The HS scheme utilizes the knowledge of cover image histogram for data embedding. A set of the Peak Points (PP) and Zero Points (ZP) are selected from the cover image histogram. Then the values between PP and ZP are shifted towards ZP by 1 position. Now, there will no longer be an empty or minimum bin in ZP position. The empty bin would appear near PP. This is called the pre-processing stage which prepares the cover image for data hiding[15].

In the data embedding stage, the entire image is scanned pixel by pixel in a specific order. When an intensity value equals to PP is encountered, the secret data sequence is checked. If the corresponding secret bit is 1, the pixel value is modified such a way that it occupies the empty bin near PP. But, if the secret bit is 0, the pixel value is not changed. Along with the secret data, the location of PP and ZP are also embedded to get a perfect restoration of the cover at the receiving end. The overall process is shown in the Fig. 6. The capacity of this technique will be equal to the number of pixels in PP. If the payload is more than the number of pixels in PP, then a second pair of peak and zero points embed the remaining data.

In the extraction phase, the stego pixels are scanned in the same order as in the embedding phase. During the scan, the occurrences of PP represent the secret data '0' and the occurrence of pixel value of the adjacent bin represents secret data '1'. Multiple sets of the PP and ZP can be utilized in the HS scheme to improve capacity but the increase in PP and ZP points would increase the size of the auxiliary information.

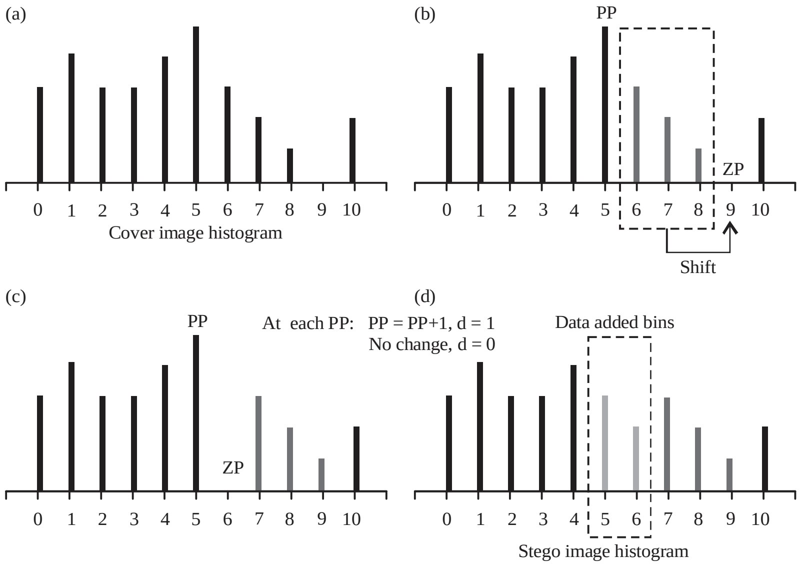

Fig. 6(a-d): Histogram shifting

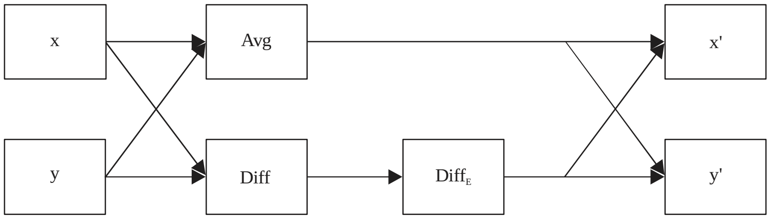

Fig. 7: Difference expansion

The probability of perfect extraction reduces if any distortion happens in the auxiliary information. Because of the low embedding capacity, HS produces high visual quality and moderately secure stego images.

Existing HS based schemes require more auxiliary information to support higher embedding capacity which affects the image quality. Due to these effects, new methods which use minimum auxiliary information to improve the capacity are proposed. Residual Histogram Shifting (RHS)[43] approach is proposed to improve the hiding capacity. The central pixels in all divided blocks are considered as the basic pixels for linear prediction. Residual values are generated by performing linear prediction on every pixel in each block. This residual histogram is used for data embedding. In the same manner multiple, sets of PP and ZP can be used to improve the hiding capacity[40,48]. Multilevel Difference Histogram Modification (MDHM)[42] is another technique which is used to improve the data capacity. Table 3 gives a summary of some recent HS based data hiding techniques.

The HS requires more auxiliary information and it leads to relatively low embedding capacity. Any changes in the pixel intensities make the secret data extraction difficult and hence, the robustness is low. It maintains security by using dispersive embedding locations. But, an analysis of changes in the histogram during the data embedding procedure will show the presence of secret data[49].

Difference Expansion (DE): Tian[50] discovered the extra space by exploring the redundancy in the image content. In this scheme, the secret data is embedded into LSBs of the expanded differences between the adjacent pixels. A pixel pair with intensities x and y are selected from an 8 bit grayscale cover image. Then their integer average and difference are calculated as given in Eq. 9. The total DE based embedding process is illustrated in Fig. 7:

$$\mathrm{Avg} = \frac{x+y}{2},\ \mathrm{Diff} = x - y \qquad (9)$$

The difference value is expanded by multiplying with a factor of 2 and then appended with the secret binary bit d into the expanded difference value. Mathematically, the difference expansion embedding is represented in Eq. 10:

$$\mathrm{Diff}_E = 2\times\mathrm{Diff}+d \qquad (10)$$

Table 3: Histogram shifting based data hiding

References	PSNR (dB)	Features
Li *et al.*[40]	50.82	Adjacent Pixel Difference (APD) is used to generate the histogram of pixel differences APD improves the number of peak points to embed more data Achieves average embedding capacity greater than 60 kb
Hong and Chen[41]	50.48	Image interpolation and pixel distribution mechanism is used to detect the smooth and complex regions in the cover The interpolation errors are used for data embedding during histogram shifting Achieves average data capacity of 86 kb and outperforms[42,43]
Li *et al.*[44]	59.78	Two-dimensional difference histogram modification is performed on the difference pairs of cover image to achieve free space Uses pixel-pair-selection strategy and Difference-Pair-Mapping (DPM) to perform data embedding The embedding capacity is relatively less (around 20 kb)
Wu *et al.*[45]	30.38	Enhances the contrast of a cover image to improve stego image visual quality while data embedding Supports an average embedding rate of 0.3 bpp High payload leads to over enhancement of the image which in turn leads to distortion in the image
Liu *et al.*[46]	50.19	Histogram shifting is performed on the Bit Plane Truncated Image (BPTI) Maintains an average capacity of 36 kb
Pan *et al.*[47]	42.83	Data is embedded in two neighboring positions of the histogram Achieves an average capacity of 50 kb while maintaining a good PSNR

Table 4: DE based data hiding techniques

References	PSNR (dB)	Features
Tian[50]	34.51	Supports average capacity of 191 kb while maintaining average PSNR of 34.51 dB Stego image visual quality is low for multilayer embedding applications Requires high auxiliary information
Liu *et al.*[55]	40.65	Uses Reduced Difference Expansion (RDE) Supports multilayer data embedding with an improvement of at least 6 dB PSNR over[50]
Hu *et al.*[54]	52.00	Two directional difference expansion is used to hide data Improved histogram-based difference selection and shifting scheme gives a better flexibility for different types of images Achieves 0.05 bpp improvement in embedding capacity as compared to Tian[50]
Lu *et al.*[56]	38.52	Uses DE, HS and interpolation for data hiding The reference pixel is also utilized for data embedding High prediction error decreases capacity
Govind and Wilscy[57]	38.56	Performs data hiding based on bidirectional interpolation and DE Bidirectional interpolation is used for pixel approximation Achieves average embedding capacity 177 kb with average SSIM 0.9931

Finally, the stego image I_S pixel pair x’and y’ is computed using the new difference value $Diff_E$ and the original integer average value Avg, using Eq. 11:

$$x' = Avg + \frac{Diff_E + 1}{2},\ y' = Avg - \frac{Diff_E}{2} \tag{11}$$

The embedded bits can be extracted from the LSBs of the modified difference. The cover image is then restored using:

$$x = Avg'+[Diff'+1/2] \text{ and } Avg'-[Diff'/2]$$

where, Avg’ and Diff’ are the average and difference values of the stego pixel pair x’ and y’[51].

The DE scheme is prone to overflow and underflow problems because sometimes the modified pixels are either greater than 255 or less than 0. Therefore, a location map is required in DE schemes to achieve reversibility. The standard DE uses a large location map and hence the data capacity is low (lesser than 0.5 bpp). Alattar[52] improved the standard DE process by generalizing the DE technique for triplets and quads of pixels and achieved an ideal capacity of 0.75 bpp. Payload independent location maps[53,51] are developed to further improve the embedding capacity. If multilayer embedding[54,55] is used to further improve the capacity, the visual quality of the embedded image will degrade drastically. Reduced DE[55] and two directional difference expansions[54] achieve good visual quality in stego image. Table 4 gives the summary and features of some of the DE based data hiding techniques.

The DE based techniques are low in complexity. These methods support high embedding capacity, while maintaining a decent PSNR. Security against statistical attacks is fair but the robustness is low.

Pixel Value Differencing (PVD): The PVD works based on human visual perception capabilities. It divides the cover image into collection of non-overlapping two pixel blocks and finds the difference between each block. Based on the differences, blocks are divided into smooth and edge areas. The absolute difference value and a predefined range-table determine the amount of secret data to be embedded in each block. Data bits are embedded by altering the pixel block values such that the difference lies in the same range after modification[58].

Table 5: PVD based data hiding techniques

References	PSNR (dB)	Features
Yang *et al.*[62]	38.91	Processes four pixels at a time
		Data is embedded in the edge areas which leads to more hiding capacity
		Supports average capacity of 420 kb
		Resistant to RS steganalytic attack
Thanikaiselvan *et al.*[63]	34.50	PVD is performed on randomized blocks using Randomized Block Selection (RBS) scheme
		Improved security because of randomization of block selection procedure
Hong *et al.*[64]	51.74	Uses PVD and diamond encoding based on Multiple Base Notational System (MBNS)
		Supports average capacity of 300 kb
		Secure against RS attacks and difference histogram attacks
Hong[65]	44.15	Uses Patched Reference Table (PRT) based PVD
		Gives a little higher PSNR than some other methods
		Achieves maximum embedding capacity of 4 bpp with good visual quality
		Secure against statistical steganalytic attacks
Chen[66]	47.50	PVD is performed on blocks of four pixels in a randomized manner
		Achieves average embedding capacity of 434 kb
		Average PSNR improvement of 4.4 dB as compared to IMF-PVD[67]
		Resistant to difference histogram analysis and chi-square test
Shen and Huang[68]	49.16	Uses Hilbert curve based PVD
		Histogram of original and marked images resemble
		Supports an average capacity of 400 kb
		Robust against RS steganalytic attacks

For a cover image I_C, the ith block I_{Ci} having two neighboring pixels (P_i, P_{i+1}) is considered. The absolute difference between the two pixels is represented by Eq. 12:

$$\text{Diff}_i = P_i\text{-}P_{i+1} \tag{12}$$

A range table R consists of different ranges and the width of each range is selected to be a power of 2, which is used to estimate embedding capacity of each block. The absolute differences of image blocks are associated with any one of the sub-range in the range table. The hiding capacity of each range is calculated by Eq. 13:

$$t = \log_2^{u_j - l_j + 1} \tag{13}$$

where, u_j and l_j are upper and lower limits of the jth sub-range associated with Diff_i and t is the number of bits that can be embedded in this range. To embed data, the first t bits from the secret data are selected and converted into a decimal value. A new difference is computed using Eq. 14:

$$\text{Diff}_i' = \begin{cases} L_j + b & \text{if Diff} \geq 0; \\ -(L_j + b) & \text{if Diff} < 0; \end{cases} \tag{14}$$

where, L_j is the lower boundary of the jth sub range. After that the stego pixel values are calculated using Eq. 15:

$$\left(P_i', P_{i+1}'\right) = \begin{cases} \left(P_i - \dfrac{\text{Diff}_i' - \text{Diff}_i}{2}, P_{i+1} + \dfrac{\text{Diff}_i' - \text{Diff}_i}{2}\right) & \text{if Diff}_i \text{ is odd;} \\ \left(P_i - \dfrac{\text{Diff}_i' - \text{Diff}_i}{2}, P_{i+1} + \dfrac{\text{Diff}_i' - \text{Diff}_i}{2}\right) & \text{if Diff}_i \text{ is even;} \end{cases} \tag{15}$$

In data extraction, the stego image I_S is scanned in the same order. Suppose P_i^*, P_{i+1}^* is the selected two-pixel block and the difference of the two pixels Diff* is with sub range j. The embedded secret data value b can be extracted using the Eq. 16:

$$b = \begin{cases} \text{Diff}^* - L_j & \text{if Diff}^* \geq 0; \\ -\text{Diff}^* - L_j & \text{if Diff}^* < 0; \end{cases} \tag{16}$$

In PVD, falling-off-boundary is checked before embedding, to eliminate the blocks which overflow or underflow. To enhance security of PVD, a pseudo-random dithering to the division of ranges is introduced in Zhang and Wang[59] which avoids data detection. Similar study can be found by Thanikaiselvan *et al.*[60] which embeds data in the scrambled RGB images. Diamond Encoding (DE) and modulus functions[61] are used solve the noise problems in the stego image. Table 5 gives a summary and features some of the other DE based data hiding techniques.

Most of the PVD techniques are resistant to visual attacks and state of the art statistical attacks. But there are some targeted attacks which exploit the flaws in the differences histogram. The robustness of these techniques is less as any pixel modification in the stego image directly leads to the change in actual secret data.

Prediction Error Expansion (PEE): The PEE is a hybrid algorithm which uses both histogram shifting and differential expansion for data hiding. The redundancy among the reference and its neighboring pixels is used to embed the secret data[51]. In PEE, initially each pixel P is predicted by a prediction algorithm which uses two neighboring pixels P_i and P_{i+1} to predict the new value $\hat{P}$. Prediction error P_E is calculated from the selected pixel value p and its corresponding estimated pixel value $\hat{p}$ using the formula $\hat{P}-P$. A predefined threshold T is used to select the pixels which don't result in overflow or underflow. The difference expansion and histogram modification are used based on the following conditions.

Case 1: If P_E value ranges between, then the difference expansion operation is used to embed the data as shown in Eq. 17:

$$P' = \begin{cases} \hat{P} + 2P_E + d & \text{if } P > \hat{P} \\ \hat{P} - 2P_E - d & \text{if } P < \hat{P} \end{cases} \tag{17}$$

where, d is secret data.

Case 2: If P_E value ranges between $T \le P_E < T + \frac{T}{2}$ then the pixel shifting operation is used as shown in Eq. 18:

$$P' = \begin{cases} P - \frac{T}{2} & \text{if } P > \hat{P} \\ P + \frac{T}{2} & \text{if } P < \hat{P} \end{cases} \tag{18}$$

Case 3: If P_E value is greater than equals to $T + \frac{T}{2}$ then the pixel shifting operation is used as shown in Eq. 19:

$$P' = \begin{cases} P + \frac{T}{2} & \text{if } P > \hat{P} \\ P - \frac{T}{2} & \text{if } P < \hat{P} \end{cases} \tag{19}$$

In the extraction process, the stego image is read in the same order that is used in embedding. From the stego image, the embedded pixels are selected and the original prediction errors are retrieved using Eq. 20:

$$P = \begin{cases} \left[P'/2\right] & \text{if } T/2 \le P' < T \\ P' - T & \text{if } T \le P' < T + \left[T/2\right] \\ P' + T & \text{if } P' \ge T + \left[T/2\right] \end{cases} \tag{20}$$

The secret bits are the LSBs of P'. The cover pixels are then recovered using the retrieved prediction errors. The PEE is one of the most popular techniques for RDH[69,70]. The predictor plays a prominent role in the PEE embedding. A smaller prediction error leads to better visual quality and a greater hiding capacity.

There are some PEE methods which were used with interpolation techniques (Bi-linear interpolation and bi-cubic interpolation) as the predictors$_{41}$. They modified the prediction error histogram and achieved good PSNR with a capacity almost five times that of standard histogram shifting[15]. Median-Edge-Detector (MED)[71,53,72], Gradient Adjusted Predictor (GAP)[73-75], Mean Value Predictor (MVP)[76] and Pixel Value Ordering (PVO) are some of the newly proposed predictors. The detailed description about predictors can be found by Hiary *et al.*[77]. Compared with all the other predictors, the stego image fidelity is more in PVO based PEE techniques. Table 6 gives a summary and features some PEE based data hiding techniques.

The PEE gives high security and capacity with a good PSNR behavior. The only drawback of PEE is the use of predictors which need a lot of computations.

Most of the spatial techniques provide high data capacity with a good PSNR. But the reality is that the stego-images face various geometrical and image processing attacks. Because of the direct embedding these techniques are less robust and insecure against any image processing operations and steganalysis attacks.

TRANSFORM DOMAIN DATA HIDING

In an image, spatial pixel values are converted to frequency coefficients by using two dimensional transforms like DCT, DWT, IWT, etc. These coefficients are used for embedding the secret data in transform domain data hiding. Here coefficients are modified according to the secret data. On the other hand, this modification does not affect the stego image quality. Mostly, transform domain data hiding methods are developed from spatial domain data hiding algorithms. Figure 8 shows transforms which are popularly used in data hiding.

Table 6: PEE based data hiding techniques

References	PSNR (dB)	Features
Tseng and Hsieh[70]	47.31	Uses side match predictor Correlations between the pixels are used to apply the DE Auxiliary information is more as compared to secret data
Lee *et al.*[69]	48.50	Works based on prediction of differences Location map is not required for data retrieval Outperforms the scheme given by Tseng and Hsieh[70] with respect to embedding rate by achieving maximum of 1 bpp
Lee and Chen[78]	37.15	Uses an adjustable predictor Predicted value of each cover pixel is derived from the average value of its surrounding pixels Uses relatively high and small prediction errors for difference expansion Average embedding capacity improves to 154 kb
Qin *et al.*[79]	34.25	Prediction error is taken from top and left neighboring pixels using raster-scan Prediction error and the pre-determined threshold select the suitable pixels for embedding The histogram squeezing technique is used for avoiding underflow and overflow problems
Feng and Fan[80]	49.02	Uses an edge sensing prediction in sub sampled interpolation pattern Achieves satisfactory de-correlation between the predictive image and the cover image
Li *et al.*[81]	59.86	Uses Pixel-Value-Ordering (PVO) based predictor to improve the fidelity of the image Smooth blocks are selected to embed data Achieves an average capacity of 30 kb with a PSNR improvement of 1.31 dB as compared to Thodi and Rodríguez[51]
Ou *et al.*[82]	57.43	Generalized invariant PVO based predictor is proposed Pixel values are predicted by combination of PVO-1 and PVO-2 predictors PSNR improves by 16.68 dB for 10 kb embedding capacity as compared to Hong[83]
Fu *et al.*[84]	30.36	Uses the side-match predictors to obtain prediction-error histogram EMD and multi-layer embedding mechanism are used for embedding Supports high embedding capacity of 1.5 bpp

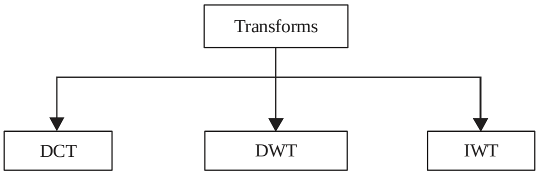

Fig. 8: Image data hiding transforms

DCT based data hiding: The DCT place a prominent role in transform domain image processing. Because it contributes in Joint Photographic Experts Group (JPEG) compression process. In the data hiding scenario JPEG data hiding is one of the simplest and relatively robust methods. The DCT converts spatial pixel intensities into Alternate Current (AC) and Direct Current (DC) coefficients. Equation 21 represents DCT of an image of size N×N:

$$C(u, v) = \alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x, y)\cos\left[\frac{(2x+1)u\pi}{2N}\right] \times \cos\left[\frac{(2x+1)v\pi}{2N}\right] \tag{21}$$

Where:

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

From the literature, it is observed that most of the DCT based data hiding process use JPEG compression model which is shown Fig. 9. In this process, initially the cover image would be divided into non-overlapping blocks each of size 8×8. These blocks are applied to DCT in a raster scan order. The DCT transformed coefficients are quantized using the quantization table. This process facilitates the developer to hide secret data. Embedding algorithm alters the quantized coefficients according to the secret data. Here the DC component plays an important role in the retrieval process, hence any change in the DC component degrades the image quality. Because of that, most of the algorithms embed secret data in high frequency coefficients to achieve imperceptibility. Here the shaded portion indicates the modified part for data hiding. Then stego coefficients are coded using encoding algorithms like Run-length of Huffman coding to remove redundancy. After that, inverse DCT is applied to obtain stego image[85].

The data retrieval process, follows the embedding process in reverse order. In the receiving end, just like the embedding stage, the stego image is divided and transformed using DCT in raster scan order. After that the secret data would be extracted from the coefficients using extraction algorithm.

The JPEG steganographic method (Jsteg) is one of the classic data hiding algorithm in DCT domain. It performs the LSB embedding on the quantized coefficients except zeros and ones to hide the secret data. Currently it is used as an online data hiding tool to hide personal information in the

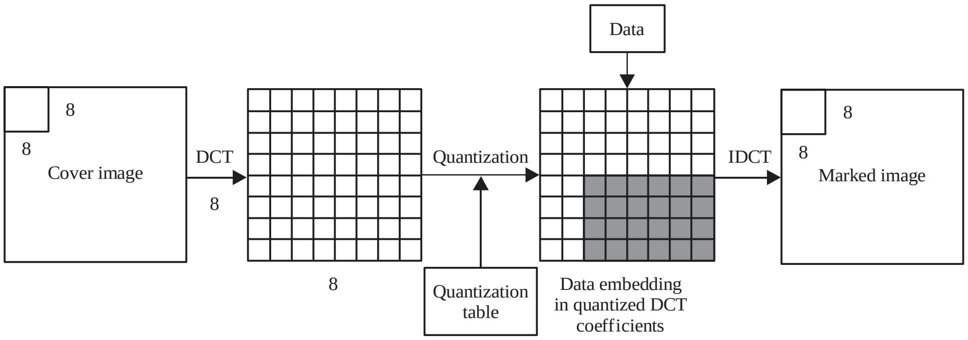

Fig. 9: DCT based data hiding

Table 7: DCT based data hiding techniques

References	PSNR (dB)	Features
Chang *et al.*[85]	39.10	LSB embedding in middle DCT coefficients Embedding capacity and PSNR are low Requires more time to process
Almohammad *et al.*[87]	44.10	Block size is increased to 16×16 2-bit LSB embedding is performed on DCT coefficients except -1, 0 and 1 Embedding capacity improves to 24 kb and computation time reduces to half as compared to Chang *et al.*[85]
Vongurai and Phimoltares[88]	39.60	Block size is increased to 32×32 Embedding in LSBs of DCT coefficients Computation time reduces to half as compared to Almohammad *et al.*[87]
Sun *et al.*[89]	38.10	Uses adaptive steganography approach with Block Discrete Cosine Transform (BDCT) and visual model Data is embedded using sub-band coefficient adjustment Robust to common visual attacks, filtering and compression operations
Amin *et al.*[91]	44.20	Embeds data in the LSBs of all DCT coefficients Embedding capacity is improved (100 kb) as compared to Chang *et al.*[85] and Jsteg
Habib *et al.*[92]	59.69	Uses random LSB embedding based on Piece Wise Linear Chaotic Map (PWLCM) Performs well against supervised universal steganalysis approach based on Fisher Linear Discriminator (FLD) Achieves average SSIM index value of 0.9974
Chang *et al.*[93]	40.49	Two consecutive zero coefficients of each DCT block are used as embedding location Modified quantization table improves the PSNR by 2 dB as compared to standard quantization table Chang *et al.*[85] Performs well against chi-square test
Chen *et al.*[94]	40.82	Uses theoretical model of RDH based on Recursive Code Construction (RCC) Maximum capacity of 20 kb Stego image size varies with respect to payload
Huang *et al.*[90]	37.50	Uses HS and Block Selection Strategy (BSS) based RDH technique on JPEG images Visual quality improves and variations in storage size is controlled compared to Chen *et al.*[94] Average capacity of 30 kb
Nikolaidis[95]	47.17	Uses zero quantized DCT coefficients modification for RDH Achieves an average capacity of 22 kb with a SSIM value of 0.9858

image. Similar to Jsteg there are some other tools which uses LSB data hiding in DCT domain are Yet Another Steganographic Scheme (YASS), F5 and OutGuess. But these schemes are highly vulnerable to attacks[86] and provides limited capacity. To overcome these, quantization table modification[87,88], coefficient compression[89] and histogram shifting[90] are developed. Table 7 provides evolution of DCT based data hiding schemes.

The DCT based schemes are robust as compared to its counter parts in spatial domain like LSB, compression and histogram based data hiding. Because of indirect modification these schemes perform well against statistical stego attacks and histogram analysis based stego attacks. But, it is not robust against chi-square tests. Blocking artifacts is main problem in DCT based techniques, these artifacts degrades the visual quality of the reconstructed image[90]. It supports the moderate embedding capacity and fails to support the RDH. To overcome the correlation problem, we move to the DWT transform where the whole image would be processed as a single unit.

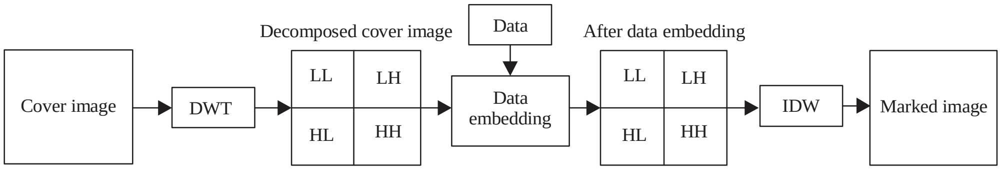

Fig. 10: DWT based data hiding

DWT based data hiding: The DWT is a translated and dilated versions of time limited signals known as wavelets. It supports the multi-resolution analysis and classifies the input signal into frequency ranges with different spatial resolutions. Equation 22 and 23 represents the one dimensional DWT (1D-DWT)[96]:

$$a_{j+1}[p] = \sum_{n=-\infty}^{\infty} l[n-2p]x_j[n] \tag{22}$$

$$d_{j+1}[p] = \sum_{n=-\infty}^{\infty} h[n-2p]x_j[n] \tag{23}$$

In DWT, the image I of size N×N is decomposed by performing row operation followed by column operation. In row operation, considering each row x at a time, the filtering operation by decimation using Eq. 22 and 23 is performed. For first level of decomposition, low pass filter l[n] extracts the approximate components a_1 and high pass filter h[n] extracts the detail components d_1 each having length N/2. For a Haar wavelet filer, the high pass and low pass filter coefficients are $\left[\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}\right]$ and $\left[\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right]$ respectively. As a result, the whole image is decomposed into two low frequency (L) and high frequency (H) components with each of size N×N/2. Then the same operation is performed column wise using two halves, as a result, the whole image is decomposed into four components called approximation (LL), horizontal (LH), vertical (VH) and diagonal (HH) sub-bands. After one level decomposition, an N×N image will divide into four sub images each of size N/2×N/2.

After image decomposition, the embedding algorithm is performed on the sub bands. The approximation (LL) component contains the low frequency information of the image, any changes in LL band leads to poor stego image quality. Hence, in most cases the data embedding is performed in the middle (LH and HL) and high (HH) frequency bands (shaded portion). After data embedding, inverse transform is used to create the stego image[97]. The whole process is illustrated in Fig. 10.

In DWT, based LSB embedding, the secret data bits are stored in the LSB positions of the quantized DWT sub-band coefficients. In DWT and HS based techniques, the histogram of wavelet coefficients will change according to the secret data[98]. The DWT or IWT coefficients are more suitable for HS, because medium and high frequency sub-band coefficients contain more number of zeros and the histogram follows the Laplacian-like distribution[99]. In compression based data hiding, the coefficients of the high frequency bands are compressed by using compression techniques like Huffman, arithmetic coding, etc. It then embeds the compressed data along with the secret data in the high frequency bands[100,101]. The block partitioning on DWT coefficients improves the fidelity of the system[102]. Table 8 illustrates the recent advancements in the DWT based data hiding.

Standard DWT is not suitable for RDH because it is not invertible. The DWT converts an image into floating point coefficients in the transform domain. Truncation of DWT coefficients is necessary to achieve integer coefficients for proper data hiding which results in information loss. During the embedding phase, the truncated coefficients are altered according to the secret data. To achieve reversibility, the fractional values need to be stored as auxiliary information along with the secret data. But it would reduce the embedding capacity. The implementation of invertible integer-to-integer wavelet transforms (IWT) shows a solution to this reversible problem in data hiding[96,105-107].

IWT based data hiding: The IWT transforms the spatial domain integer values into transform domain integer coefficients using lifting scheme. Lifting scheme uses simple pair wise averages and differences to transform the signal[108]. The 1D Haar wavelet transform in lifting scheme is represented in Eq. 24 and 25:

$$d_k = x_{2k+1} - x_{2k} \tag{24}$$

$$s_k = x_{2k} + \frac{d_k}{2} \tag{25}$$

where, x is a 1D vector of size N, which is equal to multiple powers of 2. Predication and update parameters or low frequency and high frequency components of x are given by d and s, respectively[109].

Table 8: DWT based data hiding techniques

References	PSNR (dB)	Features
Luo *et al.*[99]	43.30	Middle and high frequency coefficients of two-level Haar DWT difference histogram are shifted to hide data Payload capacity of 0.78 bpp while maintaining good visual quality
Chan *et al.*[100]	44.78	Huffman coding is used to compress the high frequency coefficients of Haar DWT Secret data and compression data are stored on the high frequency sub bands Requires more auxiliary data to restore the cover image
Chang *et al.*[101]	43.43	A high payload frequency-based reversible image hiding (HPFRIH) method Uses adaptive arithmetic coding to compress high frequency band coefficients Compression data is reduced as compared to Chan *et al.*[100]
Kamila *et al.*[102]	60.21	Block wise LSB embedding is performed on Haar DWT high frequency sub-bands Average SSIM value of 0.99973 Performs well against statistical steganalytic tests
Mishra *et al.*[103]	50.00	DWT and SVD based embedding Data is hidden in LL3 sub-band of a 3 level DWT decomposed image using Multiple Scaling Factors (MSFs) Robust against most of the common image processing attacks
Baby *et al.*[104]	54.43	3-level DWT is used Secret color images stored on the color cover image Average SSIM value of 0.3946

Except kernels, the overall process remains same for both DWT and IWT. Bit-Plane Complexity Segmentation (BPCS)[110] and Generalized Histogram Shifting (GHS)[111] are used with the IWT coefficients to improve embedding capacity and imperceptibility. In IWT and HS based lossless data hiding techniques, the data embedding is performed by shifting the part of the histogram[112]. These techniques improved the capacity and reduced the BER. In transform domain contrast enhancement based data hiding, the Haar IWT coefficients are used to store the data while enhancing the stego image contrast[113]. This technique yields around 231 kb embedding capacity but it gives poor visual quality of around 25 dB. To avoid the over contrast enhancement problems contrast control mechanism[45] is used. Some more IWT based techniques are reviewed in Table 9.

There are some data hiding techniques which use combination of two transforms to enhance the security and visual quality further[114-118]. A technique based on combination of DCT and IWT uses assignment algorithm to improve the matching quality of the stego image[117]. Similarly a combination of DWT and IWT based techniques[115] use IWT for secret data and DWT to decompose the cover image. To improve the security, Reversible Karhunen-Loêve transform (RKLT) and IWT are applied on multispectral images[119]. In this method, multilevel histogram modification is applied to store the data.

The IWT based data hiding techniques outperformed the DWT based techniques with respect to embedding capacity. These techniques provide good security against stego attacks as compared DCT based techniques. But they do not fare well when there's a need for a higher capacity and good imperceptibility.

STEGANALYSIS

Steganalysis is defined as an art of detecting the existence of secret data in a suspect file. The changes in the characteristics of stego images will provide opportunities to detect them. There are two approaches in steganalysis; one is specific to a particular steganographic algorithm also called as targeted steganalysis and the other is independent of the algorithm to be analyzed called as blind steganalysis. Targeted steganalysis relays on the method used to hide the data and known distinguishing statistics to detect stego images. Blind steganalysis is independent of the embedding algorithm so it is more suitable for forensics.

The steganalysis attacks can also be classified into visual and statistical attacks. Visual attacks involve observing the unusual patterns and noisy blurred regions in some places of the stego image. Statistical attacks are done to find out the statistical weaknesses of the embedding algorithm[124]. Chi-squared test, RS statistical test, Sample Pair Analysis (SPA), Difference Image Histogram (DIH) and Least Squares Method (LSM) are some examples[49,125-129] of statistical steganalysis.

According to Westfeld and Pfitzmann[124] without any external processing, detecting message in a stego image using human eye is extremely difficult[124]. Hence, a statistical method based on Pairs of Values (POVs) was introduced. It performs well for sequential embedding[13]. A statistical method called RS steganalysis for detection of LSB embedding uses dual statistics derived from spatial correlation of an image. Histogram based steganalysis techniques detect the existence of secret data from smoothness of the stego image histogram[130,131]. Similarly, a targeted active steganalysis technique is implemented for HS embedding using the change in the characteristics of histogram during data embedding[49].

Table 9: DWT based data hiding techniques

References	PSNR (dB)	Features
Torres-Maya *et al.*[110]	35.00	Bit-Plane Complexity Segmentation (BPCS) selects bit planes of IWT sub-bands to embed secret bits Supports embedding capacity of 2 bpp with maintaining PSNR above 35 dB Error Control Coding (ECC) is used to increase the robustness
Yang *et al.*[120]	41.35	Symmetrical histogram expansion technique is applied on the piecewise linear Haar IWT coefficients Data length and pivotal bin location are stored in LSB positions of the first row coefficients Achieves average capacity of 114 kb with an average PSNR of 41.35 dB
Yamato *et al.*[121]	40.00	Uses 2 Dimensional Wavelet Coefficient Histogram (2D WCH) based on two dimensional histogram expansion Coefficient Pair Selection (CPS) is used to select the coefficients having same value and position in the selected sub bands Approximately achieves an average capacity of 60 kb with an average PSNR of 40 dB
Fang *et al.*[112]	38.48	Histogram shifting on 3D IWT coefficients Location map and overhead information is not required for data extraction Robust against JPEG 2000 compression, salt and pepper noise and cropping attacks Achieves capacity of 49 kb with a BER value of 0.47%
Yamato *et al.*[111]	40.00	2D histogram and GHS is applied on the IWT middle sub-band coefficients to store the data Performs well for embedding capacity more that 100kb as compared to Jinna and Ganesan[98]
Gao and Shi[113]	25.00	Transformed domain contrast enhancement based data hiding Controlled Contrast Enhancement (CCE) used on Haar IWT coefficients to stop the over enhancement Achieves average capacity of 231 kb
Thanikaiselvan *et al.*[122]	44.00	Graph theory is used to hide the secret data randomly in the high frequency sub-bands of the Haar IWT Supports maximum capacity of 266646 bits with a PSNR of 44 dB Robust against blind attacks
Maheswari and Hemanth[123]	50.34	Arithmetic coding is used to compress the high frequency sub-bands of IWT Supports average embedding capacity of 139 kb with a good visual quality
Hemalatha *et al.*[115]	44.30	Payload is transformed using IWT to hide secret data and DWT is used to decompose the cover Middle planes of DWT are used for data hiding Supports average capacity of around 131 kb

Table 10: Performance evaluation of image data hiding techniques

Features	LSB	Compression based RDH	HS	DE	PVD	PEE	DCT	DWT	IWT
Capacity	High	Low	Moderate	High	High	High	Moderate	Low	High
PSNR	High	Low	High	Moderate	High	High	Moderate	Low	Moderate
Robustness	Low	Low	Low	Low	Low	Moderate	Moderate	High	High
Security	Low	Moderate	Moderate	Moderate	Low	Moderate	High	High	High

Multi-class steganalysis systems are proposed in transform domain for JPEG stego images. It comprises of DCT coefficient features and calibrated Markov features[132]. This technique can detect the model-based steganography, F5, OutGuess, Steghide and JP Hide and Seek[124].

ANALYSIS AND RECOMMENDATIONS

Security, robustness, imperceptibility and capacity are the basic characteristics of a data hiding system. But these parameters conflict each other. That is an increase in the payload capacity results in a decrease in the imperceptibility of the secret data. Also decrease in the capacity improves the robustness. This study provides an overview of the data hiding techniques in spatial and transform domain. Table 10 provides the overall performances of data hiding techniques in both domains with respect to capacity, PSNR, robustness and security.

Transform domain data hiding techniques are not too vulnerable to stego attacks, mainly because of small secret data. The DWT based data hiding systems are facing quantization problems which result in reduced capacity for RDH applications. Integer representation of wavelet transforms (IWT) shows a better solution to this drawback. But DWT and IWT transforms fail to represent the image with non-linear shapes sparsely. It is well known that the efficient representation of images in transform domain provide more opportunities to extract details from them. There are many advanced transforms related to wavelet families like curvelet, contourlet, shearlet, etc. to represent the image. Like conventional DWT these transforms face quantization problems in the embedding stage. Hence there is a need for implementation of new transforms which represent the cover image details such as edges, smooth regions etc., perfectly while maintaining reversibility.

Adaptive random selection of pixels aims to avoid the sensitive areas like uniform regions or smooth regions[5]. Because of its random nature, this scheme embeds data like additive noise. Hence, it enhances the security as compared to sequential and normal independent pseudo random selection schemes. Also this improves the robustness against standard image processing operations[92,133,59].

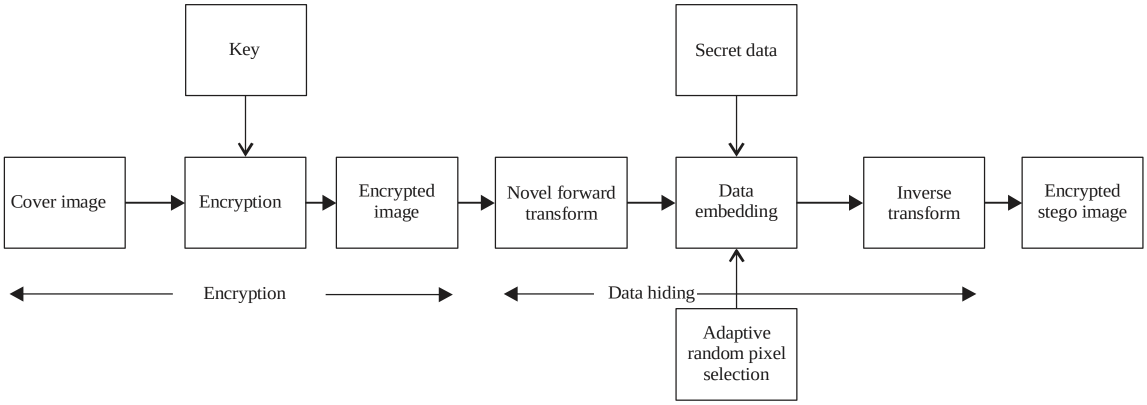

Fig. 11: Recommended data embedding process

Most of the researchers are taking extra care on imperceptibility and payload as compared to robustness. But robustness is essential to protect the secret data against various geometrical and image processing attacks. Hence, the data hiding systems should be planned to maintain an acceptable robustness along with security and imperceptibility. To meet this requirement, utilization of cryptography in the data hiding systems is a better approach[134-140].

Based on this review, a further study is recommended to implement a novel data hiding technique that contains: (1) A new transform to provide reversibility, high payload capacity and high security, (2) An adaptive random pixel selection scheme to enhance security and (3) A secure image encryption algorithm to improve robustness. With these developments in data hiding, it is feasible that this approach could serve as a relatively secure and robust communication method. The complete proposed scheme for data hiding technique is illustrated in Fig. 11.

CONCLUSION

This study presented the recent study in the field of data hiding. The basic functions of the information hiding system are discussed. The major features of spatial and transform domain techniques are reviewed with respect to visual quality, capacity, PSNR, robustness and security. The spatial domain techniques perform well with respect to image visual quality and capacity but they fail to provide robustness and the security. In order to increase security of the stego image, the cover image can be encrypted before embedding the data. Randomizing the embedding process using adaptive random process can enhance the security further more. Transform domain information hiding techniques are secure and give a good imperceptibility of marked image but they offer a lower embedding capacity in comparison with spatial domain information hiding techniques. From the discussion of the transform domain techniques it is observed that there is a need for more research which will enable the user to increase the embedding capacity and imperceptibility of the stego image. A brief description about the steganalysis techniques is presented and some basic attacks on the data hiding systems are then discussed. It can be seen from the discussion that a lot of attention is being given to make the embedded data imperceptible. But stego images experience various geometrical and image processing attacks while transmission. Hence more attention needs to be given to increase the robustness of the embedding algorithm. Implementation of blind steganalysis techniques is difficult compared to targeted steganalysis. An implementation hybrid method which includes encryption and transforms would provide a better performance than the existing data hiding schemes.

SIGNIFICANCE STATEMENTS

- The applications of data hiding in defense for covert communications and medical field for storing patient details in the reports were presented
- State of the art spatial domain techniques like LSB embedding, compression based RDH, histogram shifting, difference expansion, pixel value differencing and prediction error expansion were discussed
- Transform domain techniques like DCT, DWT and IWT based data hiding algorithms were discussed in detail
- Steganalysis and its importance were discussed briefly
- The importance of randomness, cryptography and novel transforms in a secured algorithm was discussed and a better model was recommended

REFERENCES

1. Cheddad, A., J. Condell, K. Curran and P. McKevitt, 2010. Digital image steganography: Survey and analysis of current methods. Signal Process., 90: 727-752.
2. Subhedar, M.S. and V.H. Mankar, 2014. Current status and key issues in image steganography: A survey. Comput. Sci. Rev., 13-14: 95-113.
3. Shi, Y.Q., X. Li, X. Zhang, H.T. Wu and B. Ma, 2016. Reversible data hiding: Advances in the past two decades. IEEE Access, 4: 3210-3237.
4. Alsaade, F.W., 2016. Watermarking system for the security of medical image databases used in telemedicine. Res. J. Inform. Technol., 8: 88-97.
5. Amirtharajan, R., J. Qin and J.B.B. Rayappan, 2012. Random image steganography and steganalysis: Present status and future directions. Inform. Technol. J., 11: 566-576.
6. Amirtharajan, R. and J.B.B. Rayappan, 2013. Steganography-time to time: A review. Res. J. Inform. Technol., 5: 53-66.
7. Chandramouli, R., M. Kharrazi and N. Memon, 2003. Image steganography and steganalysis: Concepts and practice. Proceedings of the 2nd International Workshop on Digital Watermarking, October 20-22, 2003, Seoul, South Korea, pp: 35-49.
8. Chanu, Y.J., T. Tuithung and K.M. Singh, 2012. A short survey on image steganography and steganalysis techniques. Proceedings of the 3rd National Conference on Emerging Trends and Applications in Computer Science, March 30-31, 2012, Nagapattinma, India, pp: 52-55.
9. Goel, S., A. Rana and M. Kaur, 2013. A review of comparison techniques of image steganography. Global J. Comput. Sci. Technol., 13: 8-14.
10. Hussain, M. and M. Hussain, 2013. A survey of image steganography techniques. Int. J. Adv. Sci. Technol., 54: 113-124.
11. Saha, B. and S. Sharma, 2012. Steganographic techniques of data hiding using digital images. Defence Sci. J., 62: 11-18.
12. Simmons, G.J., 1984. The Prisoners' Problem and the Subliminal Channel. In: Advances in Cryptography, Chaum, D. (Ed.). Springer, New York, USA., ISBN-13: 9781468447323, pp: 51-67.
13. Petitcolas, F.A.P., R.J. Anderson and M.G. Kuhn, 1999. Information hiding-a survey. Proc. IEEE, 87: 1062-1078.
14. Thanikaiselvan, V., S. Shastri and S. Ahmad, 2017. Information Hiding: Steganography. In: Intelligent Techniques in Signal Processing for Multimedia Security, Dey, N. and V. Santhi (Eds.). Springer, Germany, ISBN-13: 978-3319447896, pp: 65-91.
15. Ni, Z., Y.Q. Shi, N. Ansari and W. Su, 2006. Reversible data hiding. IEEE Trans. Circuits Syst. Video Technol., 16: 354-362.
16. Honsinger, C.W., P.W. Jones, M. Rabbani and J.C. Stoffel, 2001. Lossless recovery of an original image containing embedded data. U.S. Patent No. 6,278,791, August 21, 2001, Washington, DC.
17. Celik, M.U., G. Sharma, A.M. Tekalp and E. Saber, 2005. Lossless generalized-LSB data embedding. IEEE Trans. Image Process., 14: 253-266.
18. Feng, J.B., I.C. Lin, C.S. Tsai and Y.P. Chu, 2006. Reversible watermarking: Current status and key issues. Int. J. Netw. Secur., 2: 161-171.
19. Chan, C.K. and L.M. Cheng, 2004. Hiding data in images by simple LSB substitution. Pattern Recognit., 37: 469-474.
20. Bender, W., D. Gruhl, N. Morimoto and A. Lu, 1996. Techniques for data hiding. IBM Syst. J., 35: 313-336.
21. Wang, R.Z., C.F. Lin and J.C. Lin, 2001. Image hiding by optimal LSB substitution and genetic algorithm. Pattern Recognit., 34: 671-683.
22. Yang, C.H., 2008. Inverted pattern approach to improve image quality of information hiding by LSB substitution. Pattern Recognit., 41: 2674-2683.
23. Kuo, W.C., C.C. Wang and H.C. Hou, 2016. Signed digit data hiding scheme. Inform. Process. Lett., 116: 183-191.
24. Liao, X., Q.Y. Wen and J. Zhang, 2011. A steganographic method for digital images with four-pixel differencing and modified LSB substitution. J. Vis. Commun. Image Represent., 22: 1-8.
25. Chen, W.J., C.C. Chang and T.H.N. Le, 2010. High payload steganography mechanism using hybrid edge detector. Exp. Syst. Applic., 37: 3292-3301.
26. Lu, T.C., C.Y. Tseng and J.H. Wu, 2015. Dual imaging-based reversible hiding technique using LSB matching. Signal Process., 108: 77-89.
27. Kanan, H.R. and B. Nazeri, 2014. A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm. Expert Syst. Applic., 41: 6123-6130.
28. Fridrich, J., M. Goljan and R. Du, 2002. Lossless data embedding-new paradigm in digital watermarking. EURASIP J. Applied Signal Process., 2002: 185-196.
29. Chang, C.C., G.M. Chen and M.H. Lin, 2004. Information hiding based on search-order coding for VQ indices. Pattern Recognit. Lett., 25: 1253-1261.
30. Lu, Z., C. Liu and S. Sun, 2002. Digital image watermarking technique based on block truncation coding with vector quantization. Chin. J. Electron., 11: 152-157.
31. Lee, C.C., W.H. Ku and S.Y. Huang, 2009. A new steganographic scheme based on vector quantisation and search-order coding. IET Image Process., 3: 243-248.
32. Chang, C.C., W.C. Wu and Y.C. Hu, 2007. Lossless recovery of a VQ index table with embedded secret data. J. Visual Commun. Image Representation, 18: 207-216.

33. Chang, C.C., W.L. Tai and C.C. Lin, 2006. A reversible data hiding scheme based on side match vector quantization. IEEE Trans. Circ. Syst. Video Technol., 16: 1301-1308.
34. Tsai, P., 2009. Histogram-based reversible data hiding for vector quantisation-compressed images. IET Image Proces., 3: 100-114.
35. Shie, S.C. and S.D. Lin, 2009. Data hiding based on compressed VQ indices of images. Comput. Standards Interfaces, 31: 1143-1149.
36. Shie, S.C. and J.H. Jiang, 2012. Reversible and high-payload image steganographic scheme based on side-match vector quantization. Signal Proces., 92: 2332-2338.
37. Wang, K., Y. Hu and Z.M. Lu, 2012. Reversible data hiding for block truncation coding compressed images based on prediction-error expansion. Proceedings of the 8th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, July 18-20, 2012, Athens, Greece, pp: 317-320.
38. Lin, C.C. and X.L. Liu, 2012. A reversible data hiding scheme for block truncation compressions based on histogram modification. Proceedings of the 6th International Conference on Genetic and Evolutionary Computing, August 25-28, 2012, Kitakyushu, Japan, pp: 157-160.
39. Sun, W., Z.M. Lu, Y.C. Wen, F.X. Yu and R.J. Shen, 2013. High performance reversible data hiding for block truncation coding compressed images. Signal Image Video Process., 7: 297-306.
40. Li, Y.C., C.M. Yeh and C.C. Chang, 2010. Data hiding based on the similarity between neighboring pixels with reversibility. Digital Signal Process., 20: 1116-1128.
41. Hong, W. and T.S. Chen, 2011. Reversible data embedding for high quality images using interpolation and reference pixel distribution mechanism. J. Vis. Commun. Image Represent., 22: 131-140.
42. Kim, K.S., M.J. Lee, H.Y. Lee and H.Y. Lee, 2009. Reversible data hiding exploiting spatial correlation between sub-sampled images. Pattern Recognit., 42: 3083-3096.
43. Tsai, P.Y., Y.C. Hu and H.L. Yeh, 2009. Reversible image hiding scheme using predictive coding and histogram shifting. Signal Process., 89: 1129-1143.
44. Li, X., W. Zhang, X. Gui and B. Yang, 2013. A novel reversible data hiding scheme based on two-dimensional difference-histogram modification. IEEE Trans. Inform. Forensics Secur., 8: 1091-1100.
45. Wu, H.T., J.L. Dugelay and Y.Q. Shi, 2015. Reversible image data hiding with contrast enhancement. IEEE Signal Process. Lett., 22: 81-85.
46. Liu, L., C.C. Chang and A. Wang, 2016. Reversible data hiding scheme based on histogram shifting of *n*-bit planes. Multimedia Tools Applic., 75: 11311-11326.
47. Pan, Z., S. Hu, X. Ma and L. Wang, 2015. Reversible data hiding based on local histogram shifting with multilayer embedding. J. Visual Commun. Image Represent., 31: 64-74.
48. Wu, H.T. and J. Huang, 2012. Reversible image watermarking on prediction errors by efficient histogram modification. Signal Process., 92: 3000-3009.
49. Lou, D.C., C.L. Chou, H.K. Tso and C.C. Chiu, 2012. Active steganalysis for histogram-shifting based reversible data hiding. Opt. Commun., 285: 2510-2518.
50. Tian, J., 2003. Reversible data embedding using a difference expansion. IEEE Trans. Circ. Syst. Video Technol., 13: 890-896.
51. Thodi, D.M. and J.J. Rodriguez, 2007. Expansion embedding techniques for reversible watermarking. IEEE Trans. Image Process., 16: 721-730.
52. Alattar, A.M., 2003. Reversible watermark using difference expansion of triplets. Proceedings of the International Conference on Image Processing, Volume 1, September 14-17, 2003, Barcelona, Spain, pp: 501-504.
53. Hu, Y., H.K. Lee and J. Li, 2009. DE-based reversible data hiding with improved overflow location map. IEEE Trans. Circuits Syst. Video Technol., 19: 250-260.
54. Hu, Y., H.K. Lee, K. Chen and J. Li, 2008. Difference expansion based reversible data hiding using two embedding directions. IEEE Trans. Multimedia, 10: 1500-1512.
55. Liu, C.L., D.C. Lou and C.C. Lee, 2007. Reversible data embedding using reduced difference expansion. Proceedings of the 3rd International Conference on Intelligent Information Hiding and Multimedia Signal Processing, November 26-28, 2007, Kaohsiung, Taiwan, pp: 433-436.
56. Lu, T.C., C.C. Chang and Y.H. Huang, 2014. High capacity reversible hiding scheme based on interpolation, difference expansion and histogram shifting. Multimedia Tools Applic., 72: 417-435.
57. Govind, P.V.S. and M. Wilscy, 2015. A new reversible data hiding scheme with improved capacity based on directional interpolation and difference expansion. Procedia Comput. Sci., 46: 491-498.
58. Wu, D.C. and W.H. Tsai, 2003. A steganographic method for images by pixel-value differencing. Pattern Recognit. Lett., 24: 1613-1626.
59. Zhang, X. and S. Wang, 2004. Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security. Pattern Recognit. Lett., 25: 331-339.
60. Thanikaiselvan, V., S. Subashanthini and R. Amirtharajan, 2014. PVD based steganography on scrambled RGB cover images with pixel indicator. J. Artif. Intell., 7: 54-68.
61. Wang, C.M., N.I. Wu, C.S. Tsai and M.S. Hwang, 2008. A high quality steganographic method with pixel-value differencing and modulus function. J. Syst. Software, 81: 150-158.

62. Yang, C.H., C.Y. Weng, H.K. Tso and S.J. Wang, 2011. A data hiding scheme using the varieties of pixel-value differencing in multimedia images. J. Syst. Software, 84: 669-678.
63. Thanikaiselvan, V., P. Arulmozhivarman, R. Amirtharajan and J.B.B. Rayappan, 2012. Horse riding and hiding in image for data guarding. Proc. Eng., 30: 36-44.
64. Hong, W., T.S. Chen and C.W. Luo, 2012. Data embedding using pixel value differencing and diamond encoding with multiple-base notational system. J. Syst. Software, 85: 1166-1175.
65. Hong, W., 2013. Adaptive image data hiding in edges using patched reference table and pair-wise embedding technique. Inform. Sci., 221: 473-489.
66. Chen, J., 2014. A PVD-based data hiding method with histogram preserving using pixel pair matching. Signal Proc.: Image Commun., 29: 375-384.
67. Joo, J.C., H.Y. Lee and H.K. Lee, 2010. Improved steganographic method preserving pixel-value differencing histogram with modulus function. EURASIP J. Adv. Signal Process. 10.1155/2010/249826
68. Shen, S.Y. and L.H. Huang, 2015. A data hiding scheme using pixel value differencing and improving exploiting modification directions. Comput. Secur., 48: 131-141.
69. Lee, C.F., H.L. Chen and H.K. Ts, 2010. Embedding capacity raising in reversible data hiding based on prediction of difference expansion. J. Syst. Software, 83: 1864-1872.
70. Tseng, H.W. and C.P. Hsieh, 2009. Prediction-based reversible data hiding. Inform. Sci., 179: 2460-2469.
71. Hong, W., T.S. Chen and C.W. Shiu, 2009. Reversible data hiding for high quality images using modification of prediction errors. J. Syst. Software, 82: 1833-1842.
72. Weinberger, M.J., G. Seroussi and G. Sapiro, 2000. The LOCO-I lossless image compression algorithm: Principles and standardization into JPEG-LS. IEEE Trans. Image Process., 9: 1309-1324.
73. Fallahpour, M., 2008. Reversible image data hiding based on gradient adjusted prediction. IEICE Electr. Exp., 5: 870-876.
74. Li, X., B. Yang and T. Zeng, 2011. Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection. IEEE. Trans. Image Process., 20: 3524-3533.
75. Wu, X. and N. Memon, 1997. Context-based, adaptive, lossless image coding. IEEE Trans. Commun., 45: 437-444.
76. Sachnev, V., H.J. Kim, J. Nam, S. Suresh and Y.Q. Shi, 2009. Reversible watermarking algorithm using sorting and prediction. IEEE Trans. Circ. Syst. Video Technol., 19: 989-999.
77. Hiary, S., I. Jafar and H. Hiary, 2016. An efficient multi-predictor reversible data hiding algorithm based on performance evaluation of different prediction schemes. Multimedia Tools Applic., (In Press). 10.1007/s11042-015-3161-9.
78. Lee, C.F. and H.L. Chen, 2012. Adjustable prediction-based reversible data hiding. Digital Signal Process., 22: 941-953.
79. Qin, C., C.C. Chang and L.T. Liao, 2012. An adaptive prediction-error expansion oriented reversible information hiding scheme. Pattern Recognit. Lett., 33: 2166-2172.
80. Feng, G. and L. Fan, 2012. Reversible data hiding of high payload using local edge sensing prediction. J. Syst. Software, 85: 392-399.
81. Li, X., J. Li, B. Li and B. Yang, 2013. High-fidelity reversible data hiding scheme based on pixel-value-ordering and prediction-error expansion. Signal Process., 93: 198-205.
82. Ou, B., X. Li, Y. Zhao and R. Ni, 2014. Reversible data hiding using invariant pixel-value-ordering and prediction-error expansion. Signal Process.: Image Commun., 29: 760-772.
83. Hong, W., 2012. Adaptive reversible data hiding method based on error energy control and histogram shifting. Optics Commun., 285: 101-108.
84. Fu, D.S., Z.J. Jing, S.G. Zhao and J. Fan, 2014. Reversible data hiding based on prediction-error histogram shifting and EMD mechanism. AEU-Int. J. Electr. Commun., 68: 933-943.
85. Chang, C.C., T.S. Chen and L.Z. Chung, 2002. A steganographic method based upon JPEG and quantization table modification. Inform. Sci., 141: 123-138.
86. Fridrich, J., M. Goljan and R. Du, 2001. Invertible authentication watermark for JPEG images. Proceedings of the International Conference on Information Technology: Coding and Computing, April 2-4, 2001, Las Vegas, NV., USA., pp: 223-227.
87. Almohammad, A., R.M. Hierons and G. Ghinea, 2008. High capacity steganographic method based upon JPEG. Proceedings of the 3rd International Conference on Availability, Reliability and Security, March 4-7, 2008, Barcelona, Spain, pp: 544-549.
88. Vongurai, N. and S. Phimoltares, 2012. Frequency-based steganography using 32x32 interpolated quantization table and discrete cosine transform. Proceedings of the 4th International Conference on Computational Intelligence, Modelling and Simulation, September 25-27, 2012, Kuantan, Malaysia, pp: 249-253.
89. Sun, Q., Y. Qiu, W. Ma, W. Yan and H. Dai, 2010. Image steganography based on sub-band coefficient adjustment in BDCT domain. Proceedings of the International Conference on Multimedia Technology, October 29-31, 2010, Ningbo, China, pp: 1-4.
90. Huang, F., X. Qu, H.J. Kim and J. Huang, 2016. Reversible data hiding in JPEG images. IEEE Trans. Circ. Syst. Video Technol., 26: 1610-1621.
91. Amin, M., H.M. Abdullkader, H.M. Ibrahem and A.S. Sakr, 2014. A steganographic method based on DCT and new quantization technique. Int. J. Netw. Secur., 16: 265-270.

92. Habib, M., B. Bakhache, D. Battikh and S. El Assad, 2015. Enhancement using chaos of a Steganography method in DCT domain. Proceedings of the 5th International Conference on Digital Information and Communication Technology and its Applications, April 29-May 1, 2015, Beirut, Lebanon, pp: 204-209.

93. Chang, C.C., C.C. Lin, C.S. Tseng and W.L. Tai, 2007. Reversible hiding in DCT-based compressed images. Inform. Sci., 177: 2768-2786.

94. Chen, B., W. Zhang, K. Ma and N. Yu, 2014. Recursive code construction for reversible data hiding in DCT domain. Multimedia Tools Applic., 72: 1985-2009.

95. Nikolaidis, A., 2015. Reversible data hiding in JPEG images utilising zero quantised coefficients. IET Image Process., 9: 560-568.

96. Daubechies, I. and W. Sweldens, 1998. Factoring wavelet transforms into lifting steps. J. Fourier Anal. Applic., 4: 247-269.

97. Liu, T. and Z.D. Qiu, 2002. A DWT-based color image steganography scheme. Proceedings of the 6th International Conference on Signal Processing, Volume 2, August 26-30, 2002, Beijing, China, pp: 1568-1571.

98. Jinna, S.K. and L. Ganesan, 2010. Reversible image data hiding using lifting wavelet transform and histogram shifting. Int. J. Comput. Sci. Inform. Secur., 7: 283-289.

99. Luo, X.R., C.H.J. Lin and T.L. Yi, 2011. Reversible data hiding based on two-level HDWT coefficient histograms. Adv. Comput.: Int. J., 2: 1-16.

100. Chan, Y.K., W.T. Chen, S.S. Yu, Y.A. Ho, C.S. Tsai and Y.P. Chu, 2009. A HDWT-based reversible data hiding method. J. Syst. Software, 82: 411-421.

101. Chang, C.C., P.Y. Pai, C.M. Yeh and Y.K. Chan, 2010. A high payload frequency-based reversible image hiding method. Inform. Sci., 180: 2286-2298.

102. Kamila, S., R. Roy and S. Changder, 2015. A DWT based steganography scheme with image block partitioning. Proceedings of the 2nd International Conference on Signal Processing and Integrated Networks, February 19-20, 2015, Noida, New Delh, pp: 471-476.

103. Mishra, A., C. Agarwal, A. Sharma and P. Bedi, 2014. Optimized gray-scale image watermarking using DWT-SVD and firefly algorithm. Expert Syst. Applic., 41: 7858-7867.

104. Baby, D., J. Thomas, G. Augustine, E. George and N.R. Michael, 2015. A novel DWT based image securing method using steganography. Procedia Comput. Sci., 46: 612-618.

105. Calderbank, A.R., I. Daubechies, W. Sweldens and B.L. Yeo, 1998. Wavelet transforms that map integers to integers. Applied Comput. Harmon. Anal., 5: 332-369.

106. Hui, F., G. Lanying and X. Jinsheng, 2006. The lifting scheme based on the second generation wavelets. Wuhan Univ. J. Nat. Sci., 11: 503-506.

107. Thanikaiselvan, V., P. Arulmozhivarman, S. Chakrabarty, A. Agarwa, S. Subashanthini and R. Amirtharajan, 2014. Comparative analysis of (5/3) and Haar IWT based steganography. Inform. Technol. J., 13: 2534-2543.

108. Wang, X., X. Li, B. Yang and Z. Guo, 2010. Efficient generalized integer transform for reversible watermarking. IEEE Signal Process. Lett., 17: 567-570.

109. Adams, M.D. and F. Kossentni, 2000. Reversible integer-to-integer wavelet transforms for image compression: performance evaluation and analysis. IEEE Trans. Image Proc., 9: 1010-1024.

110. Torres-Maya, S., M. Nakano-Miyatake and H. Perez-Meana, 2006. An image steganography systems based on BPCS and IWT. Proceedings of the 16th IEEE International Conference on Electronics, Communications and Computers, February 27-March 1, 2006, Cholula, Puebla, Mexico, pp: 51-57.

111. Yamato, K., K. Shinoda, M. Hasegawa and S. Kato, 2014. Reversible data hiding based on two-dimensional histogram and generalized histogram shifting. Proceedings of the IEEE International Conference on Image Processing, October 27-30, 2014, Paris, France, pp: 4216-4220.

112. Fang, H., Q. Zhou and X. Li, 2014. Robust reversible data hiding for multispectral images. J. Netw., 9: 1454-1463.

113. Gao, G. and Y.Q. Shi, 2015. Reversible data hiding using controlled contrast enhancement and integer wavelet transform. IEEE Signal Proc. Lett., 22: 2078-2082.

114. Kale, M.C., G. Atac and O.N. Gerek, 2016. A biorthogonal wavelet design technique using Karhunen-Loeve transform approximation. Digital Signal Process., 51: 202-222.

115. Hemalatha, S., U.D. Acharya, A. Renuka and P.R. Kamath, 2013. A secure color image steganography in transform domain. Int. J. Cryptogr. Inform. Secur., 3: 17-24.

116. Kumar, V. and D. Kumar, 2010. Digital image steganography based on combination of DCT and DWT. Proceedings of the International Conference on Information and Communication Technologies, September 7-9, 2010, Kochi, Kerala, India, pp: 596-601.

117. Raftari, N. and A.M.E. Moghadam, 2012. Digital image steganography based on integer wavelet transform and assignment algorithm. Proceeings of the 6th Asia Modelling Symposium, May 29-31, 2012, Bali, Indonesia, pp: 87-92.

118. Sharmila, H. and A. Shamim Banu, 2015. Enhanced image steganography using DCT and DWT. Int. J. Applied Eng. Res., 10: 16381-16385.

119. Fang, H. and Q. Zhou, 2013. Reversible data hiding for multispectral image with high radiometric resolution. Proceedings of the 7th International Conference on Image and Graphics, July 26-28, 2013, Qingdao, China, pp: 125-129.

120. Yang, L., P. Hao and C. Zhang, 2007. Progressive reversible data hiding by symmetrical histogram expansion with piecewise-linear haar transform. Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing, Volume 2, April 15-20, 2007, Honolulu, Hawaii, USA., pp: 265-268.

121. Yamato, K., K. Shinoda, M. Hasegawa and S. Kato, 2014. Two-dimensional histogram expansion of wavelet coefficient for reversible data hiding. Proceedingas of the IEEE Visual Communications and Image Processing Conference, December 7-10, 2014, Valletta, Malta, pp: 258-261.

122. Thanikaiselvan, V., P. Arulmozhivarman, S. Subashanthini and R. Amirtharajan, 2013. A graph theory practice on transformed image: A random image steganography. Scient. World J. 10.1155/2013/464107.

123. Maheswari, S.U. and D.J. Hemanth, 2015. Frequency domain QR code based image steganography using Fresnelet transform. AEU-Int. J. Electron. Commun., 69: 539-544.

124. Westfeld, A. and A. Pfitzmann, 1999. Attacks on steganographic systems: Breaking the steganographic utilities EzStego, Jsteg, steganos and S-tools-and some lessons learned. Lect. Notes Comput. Sci., 1768: 61-67.

125. Dumitrescu, S., X. Wu and Z. Wang, 2003. Detection of LSB steganography via sample pair analysis. IEEE Trans. Signal Process., 51: 1995-2007.

126. Fridrich, J. and M. Goljan, 2004. On estimation of secret message length in LSB steganography in spatial domain. Proceedings of the SPIE Conference on Security, Steganography and Watermarking of Multimedia Contents VI, January 19-22, 2004, San Jose, CA., USA., pp: 23-34.

127. Zhang, J., I.J. Cox and G. Doerr, 2007. Steganalysis for LSB matching in images with high-frequency noise. Proceedings of the IEEE 9th Workshop on Multimedia Signal Processing, October 1-3, 2007, Greece, pp: 385-388.

128. Ker, A.D., 2005. Steganalysis of LSB matching in grayscale images. IEEE Signal Process. Lett., 12: 441-444.

129. Zhang, T. and X. Ping, 2003. A new approach to reliable detection of LSB steganography in natural images. Signal Proces., 83: 2085-2093.

130. Fridrich, J., M. Goljan and R. Du, 2001. Detecting LSB steganography in color and gray-scale images. IEEE Multimedia, 8: 22-28.

131. Xia, Z., X. Wang, X. Sun and B. Wang, 2014. Steganalysis of least significant bit matching using multi-order differences. Security Commun. Networks, 7: 1283-1291.

132. Pevni, T. and J. Fridrich, 2007. Merging markov and DCT features for multi-class JPEG steganalysis. Proceedings of the SPIE Conference on Electronic Imaging, Security, Steganography and Watermarking of Multimedia Contents IX, January 29-February 1, 2007, San Jose, CA., USA., pp: 301-313.

133. Thanikaiselvan, V. and P. Arulmozhivarman, 2015. Rand-Steg: An integer wavelet transform domain digital image random steganography using knight's tour. Secur. Commun. Networks, 8: 2374-2382.

134. Belazi, A., A.A. Abd El-Latif, A.V. Diaconu, R. Rhouma and S. Belghith, 2017. Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms. Optics Lasers Eng., 88: 37-50.

135. Fawaz, Z., H. Noura and A. Mostefaoui, 2016. An efficient and secure cipher scheme for images confidentiality preservation. Signal Proc.: Image Commun., 42: 90-108.

136. Li, M. and Y. Li, 2017. Histogram shifting in encrypted images with public key cryptosystem for reversible data hiding. Signal Process., 130: 190-196.

137. Puech, W., M. Chaumont and O. Strauss, 2008. A reversible data hiding method for encrypted images. Proceedings of the Conference on Security, Forensics, Steganography and Watermarking of Multimedia Contents X, January 28-30, 2008, San Jose, CA., USA.

138. Sae-Tang, W., M. Fujiyoshi and H. Kiya, 2000. Efficient data hiding in encrypted JPEG 2000 codestreams. Proceedings of the International Symposium on Intelligent Signal Processing and Communication Systems, December 1-4, 2014, Kuching, Sarawak, Malaysia, pp: 121-126.

139. Zhang, S., T. Gao and G. Sheng, 2014. A joint encryption and reversible data hiding scheme based on integer-DWT and arnold map permutation. J. Applied Math. 10.1155/2014/861782

140. Zheng, S., D. Li, D. Hu, D. Ye, L. Wang and J. Wang, 2016. Lossless data hiding algorithm for encrypted images with high capacity. Multimedia Tools Applic., 75: 13765-13778.