

A Survey on Intelligent Security Techniques for High-Definition Multimedia Data

S.D. Desai, N.R. Pudakalakatti and V.P. Baligar

Abstract Multimedia security has advanced tremendously over the decades due to the change in variety and volume of data. In the current security context, intelligent systems for multimedia security are very much in demand. Various applications such as biometric, e-commerce, medical imaging, forensics, aerospace, and defense require high-end data security systems. Conventional cryptography, watermarking, and steganography fall in short to provide security for high-resolution 2D/3D image and high-definition video. Persistent demand exists for designing new security algorithms for 3D graphics, animations, and HD videos. Traditional encryption method does not suffice the current need, as its securing ability is limited when it gets decoded. Steganography techniques are reported for securing text, audio, and video content, but observed to be few in number compared to image steganography techniques. Watermarking techniques for securing video content, text, and animations are reported in the literature but seem to be few in numbers as compared to image watermarking techniques. Majority of the literature is observed to apply digital watermarking as security means for video and image data. However, digital watermarking for 3D graphics is a current research topic. On the other hand, video watermarking techniques shall be broadly classified based on domain and human perception. Usually, video watermarking techniques do not alter video contents. But current trend shows that security techniques are designed based on video content. This kind of security methods is claimed to be far superior as they concentrate not only on watermarking but also on synchronization of watermark. In this chapter, we present a comprehensive review of multimedia security techniques emphasizing on their applicability, scope, and shortcomings especially when applied to high-definition multimedia data. Problematic issues of intelligent

S.D. Desai (✉)

Department of IS&E, BVB CET, Hubli 580031, India
e-mail: sd_desai@bvb.edu

N.R. Pudakalakatti · V.P. Baligar

Department of CS&E, BVB CET, Hubli 580031, India
e-mail: nehapud.np@gmail.com

V.P. Baligar

e-mail: vpbaligar@bvb.edu

techniques in signal processing for multimedia security and outlook for the future research are discussed too. The major goal of the paper was to provide a comprehensive reference source for the researchers involved in designing multimedia security technique, regardless of particular application areas.

Keywords Robustness · Multimedia · Security systems · Cryptography · Steganography · Watermarking

1 Introduction

In the recent years, the exponential growth of digital media and the ease with which digital content is exchanged over the Internet have created security issues. Hence, there is a need for good security systems. In this section, we present a comprehensive categorization and classification of security system for multimedia. Figure 1 represents the categorization and classification of security systems. Security systems shall be broadly categorized based on the information encrypting or information hiding process as shown in Fig. 1. Three categories such as digital watermarking, steganography, and cryptography fall under the security systems. All these three categories have common purposes but different approaches.

When a digital signal or pattern is embedded in the host such as image, audio, video, or text, it is called as digital watermarking. It is mainly used to identify ownership of copyright for such signals. Extraction is said to be major factor in watermarking because any kind of distortion during retrieval is unacceptable [1–5]. Imperceptibility and robustness are the two most desirable properties of a digital watermarking [6–9]. Digital watermark should be imperceptible to the human eye, and illegal removal of the watermark should be prevented. The watermark should be robust toward various intentional and unintentional attacks [10]. Nowadays, digital watermarking has been successfully used in wide range of application as it provides a high level of security. Applications related to medical, defense, and agriculture are unlimited.

Current applications are as follows:

- Content identification and management,
- Content protection for audio and video content,
- Broadcast monitoring,
- Locating content online, and
- Audience measurement.

Steganography is the art and science of hiding vital information. It aims at hiding the message so that there is no knowledge of the existence of the message. Due to the increase in popularity of IP telephony, it is attracting the attention of research community as a perfect carrier medium. Good qualities of steganography are hiding capacity, imperceptibility, and irrecoverability.

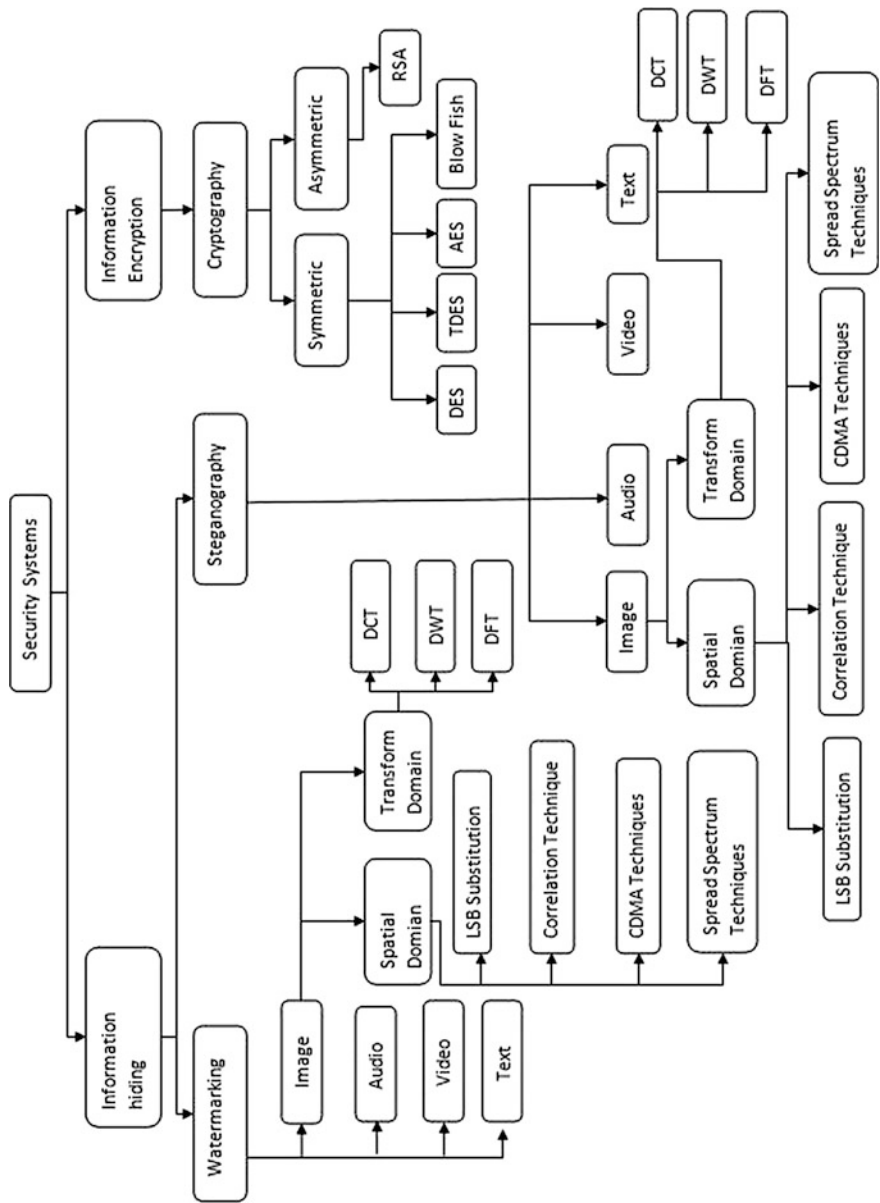


Fig. 1 Classification of security algorithms

Current applications are as follows:

- Documents protection against forgery,
- Medical imaging,
- Protection of data alteration, and
- Media database systems.

On the other hand, cryptography or information encryption scrambles messages so that they cannot be understood. Confidentiality, integrity, access control, and authentication are that main purposes of the cryptography.

Current applications are as follows:

- ATM encryption,
- Online banking, and
- E-mail privacy.

Presently, there are many embedding/extraction schemes proposed, but only few techniques have a commercial value. Both watermarking and steganography belong to the same category of information hiding, but the objective of both the techniques is totally opposite. In watermarking, important information is external data. The internal data are additional data for protecting external data. But in steganography, external data are not important as it is just a carrier medium for internal data (secret data). Generally, the watermarking and steganography are broadly classified into two main categories: first one as spatial domain and second one as transform domain. Spatial domain techniques are said to be less robust compared to transform domain techniques. Cryptography is broadly classified based on encryption algorithms.

In the recent years, audio and video technologies have better resolution compared to the previously used standards. HDM videos are defined by 3 attributes such as number of lines in the vertical display resolution, the scanning system, and the number of frames per second. The most common HD video modes are presented in Table 1.

Table 1 Common HD modes

Video Mode	Frame size in pixels ($W * H$)	Pixels per image	Scanning type	Frame rate
720p	$1,280 \times 720$	921,600	Progressive	23.976, 24, 25, 29.97, 30, 50, 59.94, 60, 72
1080i	$1,920 \times 1,080$	2,073,600	Interlaced	25 (50 fields/s), 29.97 (59.94 fields/s), 30 (60 fields/s)
1080p	$1,920 \times 1,080$	2,073,600	Progressive	24 (23.976), 25, 30 (29.97), 50, 60 (59.94)
1440p	$2,560 \times 1,440$	3,686,400	Progressive	24 (23.976), 25, 30 (29.97), 50, 60 (59.94)

HD audio also known as high-resolution audio in a trend in the audio market. In fact, there is no standard definition for HD audio. It basically describes audio signals with bandwidth and dynamic range as compared to compact disk digital audio. Some of the well-known HD audio formats are FLAC, ALAC, WAV, AIFF, and DSD.

In preceding sections, we discuss in detail about different security systems, comparison among them, classification, and algorithms used.

2 Digital Watermarking

Presently, digital watermarking is a widely used technique for data encryption. Digital watermarking is applied on image, audio, video, and text. Image watermarking is predominantly being used other than audio, video, and text. Watermarking is of two types: (i) blind watermarking and (ii) non-blind watermarking. When original data are not needed during extraction of the watermark, it is said to be blind. On the other hand, when original data and key are required during extraction process, it is said to be non-blind. Based on the human perception, digital watermarking can be classified as visible and invisible watermarking. In visible watermarking, embedded watermark is visible to human eye. Those which fail can be classified as invisible watermarks.

2.1 Digital Image Watermarking

Image watermarking has a lot of attention in the research community compared to all other watermarking techniques. There are two main categories of digital image watermarking techniques, which are based on the embedding position, spatial domain, and transform domain.

2.1.1 Spatial Domain

The spatial domain image is represented by pixels. In this technique, watermark embedding is achieved by directly modifying the pixel value of the host image.

Techniques in spatial domain generally share the following characteristics:

- Watermark is applied in pixel domain.
- Simple operations are applied when combining with host signal.
- No transforms are applied.
- Watermark is detected by correlating expected pattern with received signal [11].

The methods used in the spatial domain are the least significant bit (LSB), correlation-based, and spread-spectrum techniques. LSB is easiest, and the most commonly method used in spatial domain [11].

A. LSB

The LSB technique works by replacing some of the information in a given pixel with information from the data in the image. The LSB embedding is performed on the least significant bit because it minimizes the variation in colors that the embedding creates [12]. LSB substitution suffers from drawbacks. Any addition of noise would likely to defeat the watermark. Once the algorithm is discovered, the embedded watermark could be easily modified by the hackers [13].

Advantages of LSB are as follows:

- Easiest method of watermarking.
- Can insert lot of data if image is simple.
- Enhances security when used with more sophisticated approach such as pseudorandom generator.

Disadvantages of LSB are as follows:

- Less robust.
- Highly sensitive to signal processing operations and easily corrupted.
- Less secured because if small portion of watermarked image is detected, then the whole message can be extracted.

The mean square error (MSE) and the peak signal-to-noise ratio (PSNR) are the two metrics used to compare image quality and are described as follows [11]:

$$\text{MSE}(x, y) = \frac{1}{N} \sum_{i=1}^N (x_i - y_i)^2 \quad (1)$$

$$\text{PSNR} = 10 \log_{10} \frac{L^2}{\text{MSE}} \quad (2)$$

where x and y are two finite-length discrete signals, where N is the number of signal samples (pixels, if the signals are images), x_i and y_i are the values of the i th samples in x and y , and L is the dynamic range of allowable image pixel intensities [11].

A.1. Watermark embedding and extraction using LSB

Select an image as a cover image or a base image in which watermark will be inserted. n represents the number of least significant bits to be utilized to hide most significant bits of watermark under the base image. LSB embedding and extraction are shown in Figs. 2 and 3.

Fig. 2 LSB embedding

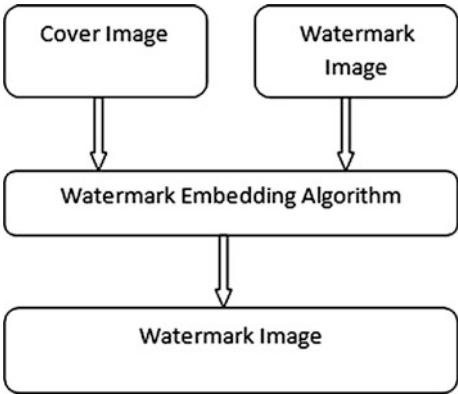
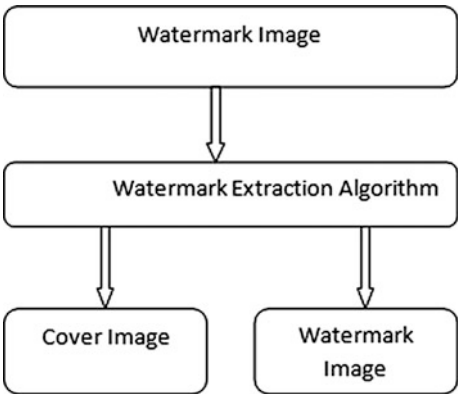


Fig. 3 LSB extraction



Algorithm 1: LSB method

Embedding

Input: Cover Image and Watermark.

Output: Watermarked Image.

- 1: For each pixel in base, watermarked and watermarked image
- 2: Cover image: Set n least significant bits to zero.
- 3: watermark: Shift right by $8-n$ bits.
- 4: Watermarked image: add values from base and watermark.
- 5: End

As an example, let us consider the first pixel of the base image along with first pixel of watermark image. The final first pixel of watermarked image is calculated as follows:

Explanation:	
Consider 1st pixel of cover image:	01101011
Set $n = 1$ and LSB to zero:	01101010
Consider first pixel of watermark and shift right by $8-n$ bits:	1
Watermarked Image:	$\begin{array}{r} 01101010 \\ + \quad 1 \\ \hline 01101011 \end{array}$

Extraction

Input: Watermark Image.

Output: Base Image and Watermark.

- 1: For each pixel in watermarked image and extracted image
- 2: Watermarked image: Shift left by $8-n$ bits.
- 3: Append n bits of zeroes at MSB
- 4: Extracted image: Set to the shifted value of watermarked image.

Explanation:	
Consider watermarked image:	01101011
Shift left by $8-1$ bits:	1101011
Append n bits of zeroes at MSB($n = 1$) which is the cover image:	01101011

A.2. Results of LSB

Figure 4 represents the original, the watermark, and the watermarked images. This is visible watermarking. The figures are the experimental results obtained by Chopra et al. [11].

B. Correlation-based watermarking

Early researches used LSB method for watermarking. And the only disadvantage was that if small portion of watermarked image was detected, then the whole message can be extracted [14]. In this method, to increase the security and the robustness, pseudorandom noise (PN) sequence and key are used [14]. PN sequence is a sequence of binary numbers that appear to be random but is actually deterministic. Here, linear feedback shift register (LFSR) circuit is used to generate pseudorandom sequence. Periodic shift registers are those shift registers which have nonzero initial state and output is feedback to the input [14].

PN sequences are good tool for watermarking because of the following reasons [14]:



Fig. 4 LSB results. **a** Original, **b** watermark, and **c** watermarked images (visible watermarking)

- Periodic sequences are produced by the generator that appears to be random.
- These sequences are generated by algorithm that makes use of initial speed.
- Unless the key and algorithm are known, it is impossible to generate the sequence.

B.1. Watermark embedding and extraction using correlation technique—threshold-based correlation

Figures 5 and 6 represent the embedding and extraction process of threshold-based correlation technique.

Algorithm 2: Correlation Technique

Embedding

Input: Base Image and Watermark.

Output: Watermark Image.

- 1: PN pattern $W(x,y)$ is added to the original image $I(x,y)$ based on the equation 1.3 shown below

$$I_w(x,y) = I(x,y) + k * W(x,y) \quad 1.3$$

where $I(x, y)$ = Original(base) Image

$W(x, y)$ = PN pattern

K = Gain Factor

$I_w(x, y)$ = Watermarked Image

- 2: Apply both watermark and the PN sequence to the product modulator.
- 3: PN pattern $W(x,y)$ is added to the base image $I(x,y)$ to produce the resultant watermarked Image $I_w(x,y)$.

Extraction

Input: Watermarked Image.

Output: -Base Image and Watermark.

- 1: Watermarked Image $I_w(x,y)$ is multiplied at the receiver with the PN sequence which is same as that used during embedding process to extract the watermark $a(x,y)$.

B.2. Results of correlation-based technique

Figure 7 represents the original, the watermark, and the watermarked images. The figures are the experimental results obtained by Gajriya et al. [14]

2.1.2 Transform Domain

The transform domain images are represented by frequencies. In this technique, the transform coefficients are modified instead of directly changing the pixel values.

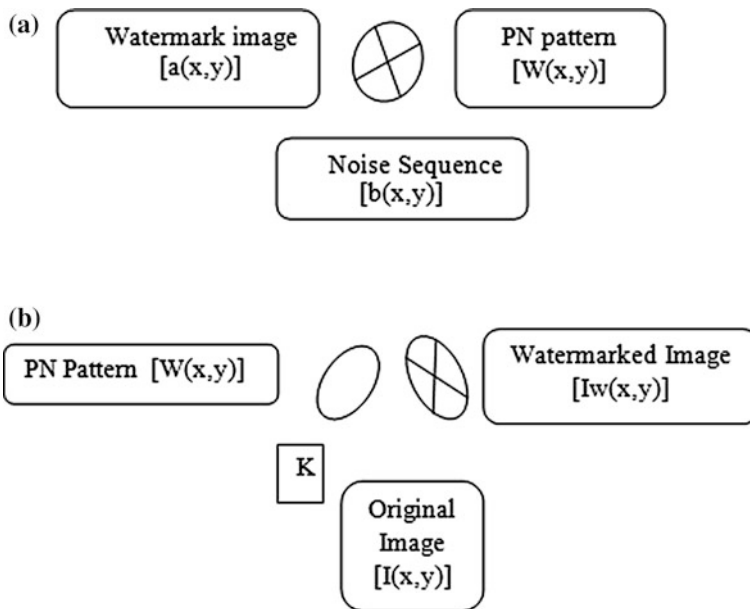


Fig. 5 Threshold-based embedding. **a** Generation of PN sequence and **b** watermarking the original image with PN sequence

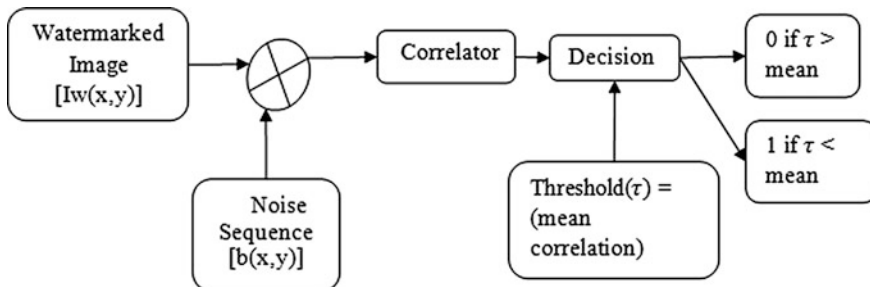


Fig. 6 Threshold-based extraction

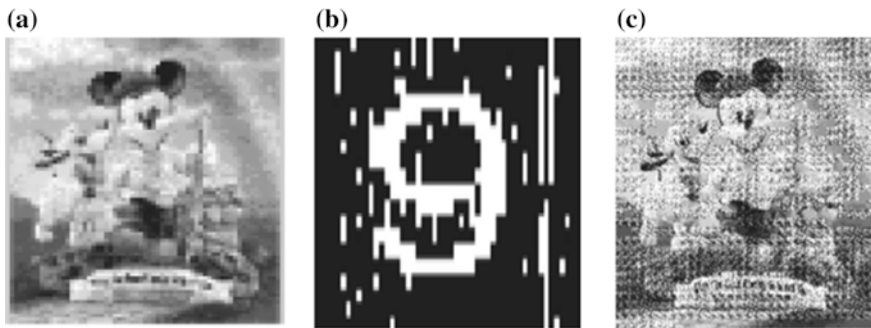


Fig. 7 Results. **a** Original, **b** watermark, and **c** watermarked images

First, the host image is converted into frequency domain using any of the transformation methods. The most commonly used transformation methods are DCT, DWT, and DFT.

A. DWT

DWT is a modern technique frequently used in digital image processing which has excellent multiresolution and spatial localization characteristics [15]. Its multiresolution characteristics hierarchically decompose an image [16]. DWT provides both the frequency and the spatial domain of an image; i.e., it captures both location information and frequency components. The original image is decomposed into four subimages: three high-frequency parts (HL, LH, and HH, named detail subimages) and one low-frequency part (LL, named approximate subimage). Edge information is present in detailed subimages. Compared to the detail subimages, approximate subimage is much more stable, since the majority of the image energy concentrates here. Therefore, the embedding is done in approximate subimages to have better robustness [16].

A.1. Watermark embedding and extraction using DWT

Alpha blending technique is a process of mixing two images to get the final image. It is accomplished in computer graphics by blending each pixel from first image and corresponding pixel in second image [17, 41]. It can be used to create partial or full transparency [16]. Formula of alpha blending technique used for watermark embedding and extraction is given as follows:

$$\text{Watermark Image} = A \times (\text{LL1}) + B \times (\text{WM1}) \quad (4)$$

$$\text{Recovered Image} = (\text{WM} - A \times \text{LL1}) \quad (5)$$

A and B represent scaling factors for cover and watermark image, respectively.

LL1 represents low-frequency approximation of cover image.

WM1 represents watermark image.

WM represents watermarked image.

Advantages of alpha blending technique are as follows:

- Insertion and extraction of watermark becomes simpler.
- This technique can be used to embed invisible watermark into salient features of the image [18].
- It provides high security.
- Image is resistant to several attacks [17].

Figures 8 and 9 represent DWT extraction and embedding.

Algorithm 3: DWT

Embedding

Input: Cover Image and Watermark.

Output: Watermarked Image.

- 1: In this first we take cover image(base image) and is decomposed into 4 components using 2D DWT.
- 2: The same procedure is applied on the watermark image which is to be embedded into cover image.
- 3: Apply DWT for both cover image and watermark image.
- 4: Now alpha blending technique is used for inserting a watermark.

Extraction

Input: Watermarked image.

Output: Cover image and watermark.

- 1: The watermarked image and cover image is first decomposed into sub images using DWT
- 2: Then alpha blending formula is applied to recover the watermarked image.

Fig. 8 DWT embedding

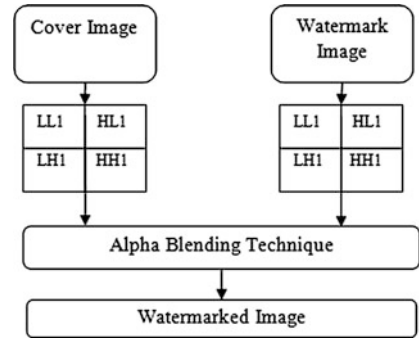
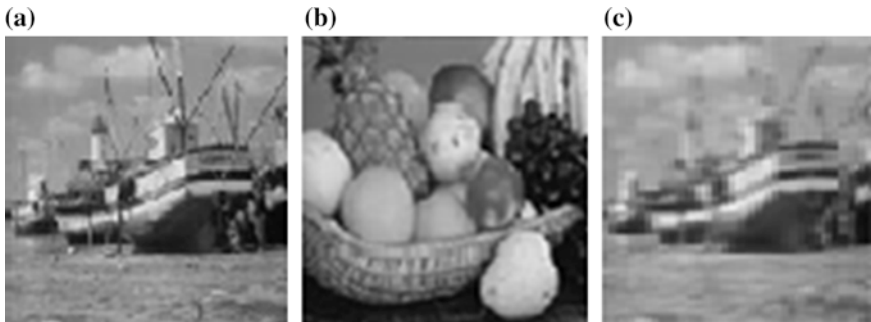
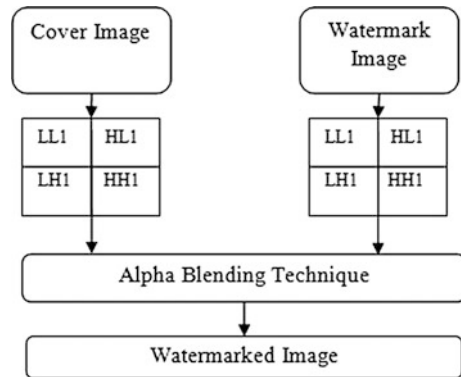


Fig. 9 DWT extraction**Fig. 10** DWT results. **a** Original, **b** watermark, and **c** watermarked images

A.2. Results of DWT

Figure 10 represents the original, the watermark, and the watermarked images. The figures are the experimental results obtained by Narang and Vashisth [16].

B. DFT

The DFT is a most popular technique used in signal analysis, signal study, and synthesis to define the effect of various factors on signal. The Fourier transform is used in transforming the signal from time domain to frequency domain or from frequency domain to time domain. This transformation is reversible and maintains the same energy [19]. The Fourier transform and the inverse Fourier transform are given in Eqs. 5 and 6 [19]:

$$F(\omega) = \int_{-\infty}^{\infty} f(t)e^{-j\omega t} dt \quad (6)$$

$$F(t) = \frac{1}{2\pi} \int_{-\infty}^{\infty} f(t) e^{j\omega t} d\omega \quad (7)$$

Performance parameters such as PSNR and normalized correlation (NC) are used in measuring the quality of watermarked image. PSNR and NC are described in the Eqs. 7 and 8 [19]:

$$\text{PSNR} = 10 \log_{10} XY \text{ map } p_{x,y}^2 / \sum (p_{x,y} - p_{x,y})^2 \quad (8)$$

$$\text{NC} = \sum p_{x,y} - p_{x,y} / \sum p_{x,y}^2 \quad (9)$$

B.1. Watermark embedding and extraction using DFT

Algorithm 4: DFT

Embedding

Input: Cover Image and Watermark.

Output: Watermarked Image.

- 1: Divide the original image, in which watermark is embedding, into the sub-blocks of 256*256.
- 2: Transform the all image blocks into 8*8 matrixes by using DFT transform.
- 3: Arnold Scrambling is used to change the binary watermark and generate two unrelated pseudo-random sequence.
- 4: Modify the corresponding value of amplitude spectrum.
- 5: Apply Discrete Fourier Transform to each image blocks to produce the image with watermark.

Extraction

Input: Watermarked Image.

Output: Cover Image and Watermark.

- 1: Apply image segmentation process to divide the image into 256*256 sub-blocks, which is embedded watermark.
- 2: Transform the all image blocks into 8*8 matrix by using DFT transform.
- 3: Produce the two unrelated pseudo-random sequence.
- 4: Compare the watermark's amplitude spectrum and the pseudo-random sequence and calculate the relativity between both of them and then produce watermark matrix with the help of embedding rules.
- 5: Use Arnold transform scrambling to watermark matrix.

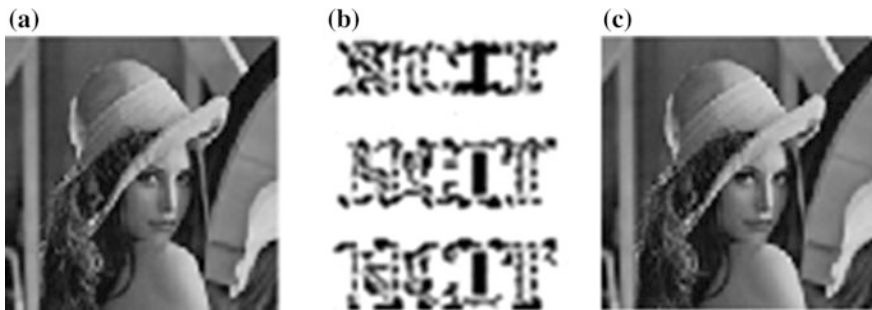


Fig. 11 DFT results. **a** Original, **b** watermark, and **c** watermarked images

B.2. Results of DFT

Figure 11 represents the original, the watermark, and the watermarked images. The figures are the experimental results obtained by Kaushik et al. [19].

C. DCT

DCT is a popular image transformation method which is used in many image processing applications. This transformation allows each transform coefficient to be encoded independently without losing compression efficiency [20]. Due to its good performance, it has been used in JPEG standard for image compression. DCT has been applied in many fields such as data compression, pattern recognition, and image processing [20].

Performance parameters such as PSNR are used in measuring the quality of watermarked image [20]. PSNR is described in Eq. 7:

$$\text{PSNR} = 10 \log_{10} 225^2 / \frac{1}{N \times N} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} (x_{ij} - x)^2 \quad (10)$$

C.1. Watermark embedding and extraction using DCT

Figures 12 and 13 represent watermark embedding and extraction using DCT.

Algorithm 5: DCT

Embedding

Input: Cover Image and Watermark.

Output: Watermarked Image.

- 1: Extract every 8 bit data from the watermark bit stream.
- 2: Using pseudo random system generate the random number, which points to one of n blocks of host image.
- 3: Embed extracted the 8-bit watermarking data into the 8 lower-band coefficients in the block pointed by previous step.
- 4: Repeat step 1 to step 3, until the watermark bit stream is run out.
- 5: The proposed employee replace bit to embedded watermark bit stream, and it was hidden at position bit 3 in the selected 8-bit coefficient. If the watermark bit is "1" then bit 3 to "1" otherwise "0".

Extraction

Input: Watermarked Image.

Output: Cover Image and Watermark.

- 1: Transform the watermarked image to frequency domain by DCT.
- 2: Use the same set of random numbers, which is applied in the embedding process.
- 3: Apply the random number to find the exact location of the DCT block in the watermarked image
- 4: Extract 8-bit watermark data from each DCT block by means of the inverse embedded. The watermark bit is "1" when bit 3 is "1" of selected DCT-block coefficient otherwise the watermark bit is "0".
- 5: Rearrange the 8-bit data into watermark image.

C.2. Results of DCT

Figure 14 represents the original, the watermark, and the watermarked images using DCT. The figures are the experimental results obtained by Marjuni et al. [20].

2.2 Audio Watermarking

Recently, audio watermarking is used as one of the most popular approaches for providing copyright protection. Digital audio watermarking is different from digital image watermarking. An effective audio watermarking scheme must have the following properties: (1) imperceptibility, (2) robustness, (3) payload, and (4) security [21].

Fig. 12 DCT embedding

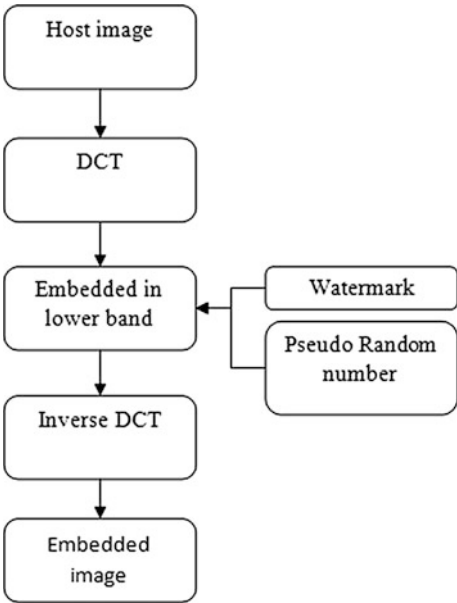
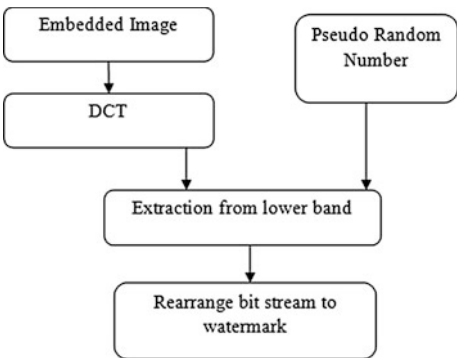


Fig. 13 DCT embedding



1. Imperceptibility refers to the maintaining of audio quality after adding the watermark.
2. Robustness refers to the ability to extract a watermark from a watermarked audio signal after various intentional and unintentional attacks.
3. Payload refers to the amount of data that can be embedded into the host audio signal.
4. Security refers to the watermark that can only be detected by the authorized person.

Robustness and imperceptibility are the most important requirements for digital audio watermarking. A watermark embedding should be imperceptible by the user;

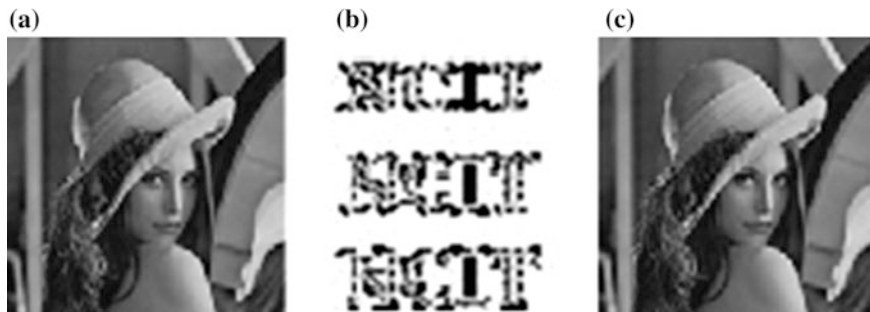


Fig. 14 DCT results. **a** Original, **b** watermark, and **c** watermarked images

that is, it should be highly transparent or invisible to prevent unauthorized detection and removal. On the other hand, watermark should be resistant to several attacks such as noise addition, cropping, resampling, requantization, MP3 compression, shifting, time scale modification (TSM), and pitch scale modification (PSM) [22, 23].

In general, audio watermarking is classified into 2 types: time domain and transform domain [21]. Time domain watermarking schemes are very easy to implement, and they also require less computing resources compared to transform domain watermarking methods. On the other hand, time domain watermarking systems are usually weaker against various attacks. The widely used transform domains for audio watermarking are DCT, DWT, and FFT.

Audio watermarking applications are as follows:

- Copyright protection—the copyright owner will be having knowledge of secret key to read the embedded watermark.
- Vendor identification—copyright notice can be embedded in the audio signal and can determine vendor of the copyrighted audio.
- Evidence of proprietorship—the original owner can prove his proprietorship by extracting watermark from watermarked image.
- Validation of genuineness—the copyright audio can be proved easily by adding watermark.
- Fingerprinting—information about authenticated customers can be embedded as secret watermarks right before the secure delivery of the data [24].

2.3 Video Watermarking

Video watermarking is a rapidly evolving field in the area of multimedia. Many watermarking techniques have been proposed for video watermarking. Video watermarking scheme should have the following properties: (1) imperceptibility, (2) robustness, (3) payload, and (4) security. An effective and efficient video

watermarking should be resistant to several attacks such as JPEG coding, gaussian noise addition, histogram equalization, gamma correction, lossy compression, frame averaging, frame swapping, rotation, and rescaling.

Based on the domain, video watermarking can be broadly classified into two domains. The first one is the spatial domain watermarking where embedding and detection of watermark are performed by manipulating the pixel values of the frame. The second category is the transform domain techniques in which the watermark is embedded by changing its frequency components. The commonly used transform domain techniques are DFT, DCT, and DFT and also principle component analysis (PCA) transform. The transform domain watermarking schemes are relatively more robust than the spatial domain watermarking schemes, particularly in pixel removal, noise addition, rescaling, rotation, and cropping.

Video watermarking applications are as follows [25]:

- Copy control—it prevents copying from unauthorized persons.
- Broadcast monitoring—it monitors the video contents that are broadcasted.
- Fingerprinting—it traces the unauthorized or malicious uses.
- Enhanced video coding—it includes additional information.
- Copyright protection—it proves the authenticity of the owner.

2.4 Text Watermarking

Authentication and copyright protection are the two main applications of digital watermarking. In addition to image, audio and video text is also an important medium. Textual contents over the Internet include newspapers, e-books, and messages. Hence, text has to be protected from intentional and unintentional attacks such as random insertion, deletion or, reordering of words or sentences to and from the text [14, 40]. Text watermarking techniques help to protect the text from illegal copying, forgery, and redistribution. It also helps to prevent copyright violations [26]. Text watermarking developed so far use either image or textual watermark. Watermarking which makes use of both text and image is more secured and provides better robustness to various attacks [27]. Compared to other watermarking techniques, less research works are proposed for text. Text watermarking algorithms can be broadly classified into 4 types:

- Image-based methods,
- Syntactic methods,
- Semantic methods, and
- Structural methods [26, 28].

In the next section, we discuss in detail steganography, its classification, and the algorithms used.

3 Steganography

Steganography refers to the technique of hiding secret messages into media such as text, audio, image, and video, while steganalysis is the art and science of detecting the presence of steganography. There are two main categories of image steganography techniques, which are based on embedding position, spatial domain, and transform domain.

3.1 Image Steganography

In this section, we present spatial and transform domain image steganography methods.

3.1.1 Spatial Domain

A. LSB

In spatial domain, LSB is most commonly used technique and very easy to implement, but it is less robust compared to other techniques. It embeds the secret into least significant bits of pixel value of the base image (cover image) [29].

Performance parameters such as PSNR are used to measure the quality of stego-image. The formula is given as follows [39]:

$$\text{PSNR} = 10 \log C_{\max}^2 / \text{MSE} \quad (11)$$

$$\text{MSE} = \text{mean} - \text{square} - \text{error} \quad (12)$$

$$\text{MSE} = \frac{1}{MN((S - C)^2)} \quad (13)$$

$$C_{\max} = 255. \quad (14)$$

where M and N are the dimensions of the image, S is the resultant stego-image, and C is the cover image.

A.1. Data embedding and extraction using LSB

Figures 15 and 16 represent the watermark embedding and extraction using LSB

Algorithm 6: LSB method

Embedding

Inputs: Cover image, stego-key and the text file

Output: stego image

- 1: Extract the pixels of the cover image.
- 2: Extract the characters of the text file.
- 3: Extract the characters from the Stego key.
- 4: Choose first pixel and pick characters of the stego key and place it in first component of the pixel.
- 5: Place some terminating symbol to indicate end of the key.
- 6: Insert characters of text file in each first component of next pixels by replacing it.
- 7: Repeat step 6 till all the characters has been embedded.
- 8: Again place some terminating symbol to indicate end of data.
- 9: Obtained stego image.[16].

Extraction

Inputs: Stego-image file, stego-key

Output: Secret text message.

- 1: Extract the pixels of the stego image.
- 2: Now, start from first pixel and extract stego key characters from first component of the pixels. Follow Step3 up to terminating symbol, otherwise follow step 4.
- 3: If this extracted key matches with the key entered by the receiver, then follow Step 5, otherwise terminate the program.
- 4: If the key is correct, then go to next pixels and extract secret message characters from first component of next pixels. Follow Step 5 till up to terminating symbol, otherwise follow step 6.
- 5: Image extraction algorithm.
- 6: Extract secret message[16].

Fig. 15 LSB embedding

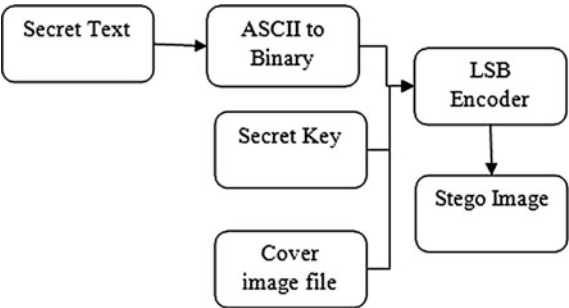


Fig. 16 LSB extraction

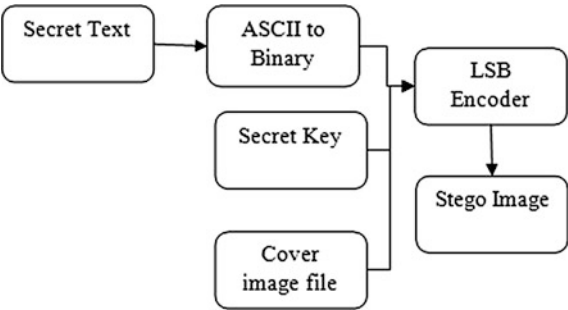


Fig. 17 LSB results. **a** Original image and **b** stego-image

A.2. Results of LSB

Figure 17 represents the original image and stego-image. The figures are the experimental results obtained by Devi [39].

3.1.2 Transform Domain

A. DWT

DWT divides the image into low- and high-frequency components. The original image is embedded in approximate coefficients which are low-frequency components. And additional information about the image is embedded in detailed coefficients which are high-frequency components [31].

A.1. Data embedding and extraction using DWT

Algorithm 7: DWT

Embedding

Input: An $m \times n$ carrier image and a secret message/image.

Output: An $m \times n$ stego-image.

- 1: Read the cover image (I_c)
- 2: Calculate the size of I_c
- 3: Read the secret image (I_m)
- 4: Prepare I_m as message vector
- 5: Decompose the I_c by using Haar wavelet transform
- 6: Generate pseudo-random number (P_n)
- 7: Modify detailed coefficients like horizontal and vertical coefficients of wavelet decomposition by adding P_n when message bit = 0.
- 8: Apply inverse DWT
- 9: Prepare stego image to display.

Extraction

Input: An $m \times n$ carrier image and an $m \times n$ stego-image.

Output: Secret message/image.

- 1: Read the cover image (I_c)
- 2: Read the stego image (I_s)
- 3: Decompose the I_c and I_s by using Haar wavelet transform
- 4: Generate message vector of all ones
- 5: Find the correlation between the original and modified coefficients
- 6: Turn the message vector bit to 0 if the correlation value is greater than mean correlation value
- 7: Prepare message vector to display secret image.

A.2. Results of DWT

Figure 18 represents the original image and stego-image. The figures are the experimental results obtained by Banik [30].

B. DFT

It is used to get the frequency component for each pixel. The DFT of spatial value $f(x, y)$ for the image size $M * N$ is given by [32]

$$F(u, v) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) e^{-j2\pi(\frac{ux}{M} + \frac{vy}{N})} \quad (15)$$

$$F(u, v) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} F(u, v) e^{-j2\pi(\frac{ux}{M} + \frac{vy}{N})} \quad (16)$$

where $u = 0$ to $M - 1$ and $v = 0$ to $N - 1$.



Fig. 18 DWT results. **a** Original image and **b** stego-image

B.1. Data embedding and extraction using DFT

Algorithm 8: DFT

Extraction

Inputs: Source image, Secret Image

Output: Stego image

- 1: Read the source image.
- 2: Read the image.
- 3: Apply DFT. Embedded the image in the real part of transform domain excluding 1st pixel.
- 4: Insert the image bit one by one.
- 5: Apply Inverse DFT.
- 6: Repeat steps 3 to 5 for the whole embedding process.
- 7: Stop.

Extraction

Inputs: Stego Image

Output: Source image and Secret image

- 1: Read the noisy embedded image.
- 2: Apply DFT.
- 3: Extract the image from real part of transform domain.
- 4: Repeat steps 2 to 3 for complete decoding of as per image size.
- 5: Apply Inverse DFT.
- 6: Stop

C. DCT

DCT provides high-energy compaction compared to DFT for natural images [33]. DCT is a general 8×8 transform for digital image processing and signal processing [34]. Two-dimensional DCT can be defined as follows:

$$f(x, y) = C(u)C(v) \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} F(u, v) \cos \left[\frac{(2x+1)u\pi}{2N} \right] \cos \left[\frac{(2x+1)v\pi}{2N} \right] \quad (17)$$

$$F(u, v) = \frac{2}{N} C(u)C(v) \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} f(x, y) \cos \left[\frac{(2x+1)u\pi}{2N} \right] \cos \left[\frac{(2x+1)v\pi}{2N} \right] \quad (18)$$

where $F(u, v)$ is cosine transform coefficient, and u and v is generally frequency variables. For $x, y = 0, 1, 2 \dots N-1$. N is horizontal and vertical pixel number of pixel block.

C.1. Data embedding and extraction using DCT

Figures 19 and 20 represent DCT embedding and extraction.

Algorithm 9: DCT

Embedding

Input: Cover Image I, Secret Message

Input Parameters: Quantization Matrix (Q)

Output: Stego Image S

- 1: Begin
- 2: Read the cover image, I .
- 3: Divide the cover image, I into blocks of size 8×8 .
- 4: Find the DCT of I .
- 5: Obtain the Quantized DCT blocks by dividing the DCT of I by the quantization matrix.
- 6: Hide the secret message in the Quantized DCT.
- 7: Obtain the dequantized matrix and inverse DCT.
- 8: Restructure the 8×8 blocks into a single array.
- 9: Stego image is formed.
- 10: End

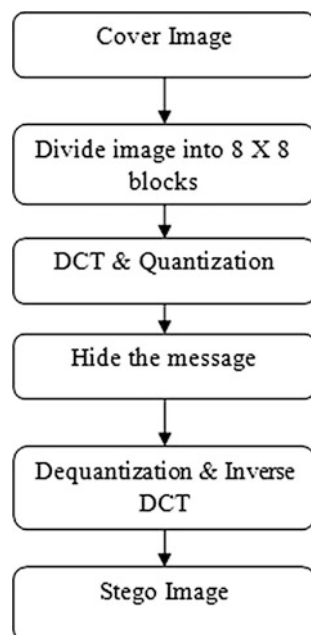
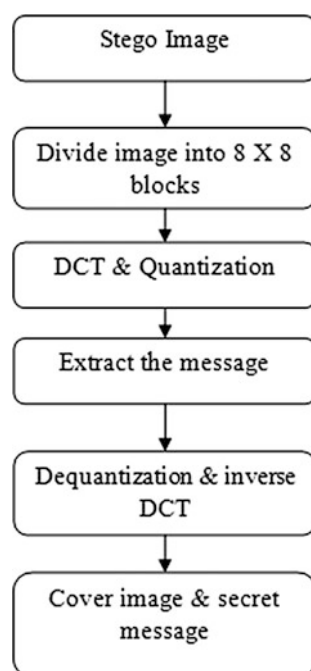
Extraction

Input: Stego Image S

Input Parameters: Quantization Matrix (Q)

Output: Cover Image I, Secret Message

- 1: Begin
- 2: Read the stego image, S .
- 3: Divide the stego image, S into blocks of size 8×8 .
- 4: Find the DCT of S .
- 5: Obtain the Quantized DCT blocks by dividing the DCT of S by the quantization matrix.
- 6: Extract the secret message from the quantized DCT blocks and concatenate DCT LSB to secret message.
- 7: Obtain the dequantized matrix and inverse DCT.
- 8: Restructure the 8×8 blocks into a single array.
- 9: Cover image and secret message are obtained[13].
- 10: End

Fig. 19 DCT embedding**Fig. 20** DCT extraction

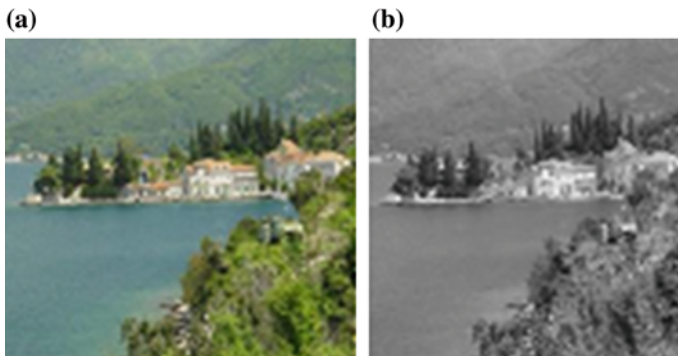


Fig. 21 DCT results. **a** Original image and **b** stego-image

C.2. Results of DCT

Figure 21 represents the original image and stego-image. The figures are the experimental results obtained by Bansal and Chhikar [33].

In this section, we discuss briefly on cryptography, its classification, purposes, and algorithms used.

4 Cryptography

Cryptography is a technique used to scramble confidential data to make it unreadable for unauthorized persons [35]. Many security system use cryptography for providing security because it consists of different encryption algorithms that makes encrypted data to be unreadable [35]. It is not only used to provide security for data but can also be used for user authentication.

A. Purpose of cryptography

- Confidentiality—confidential means private or secret. It ensures that only the sender and authorized person have access to the message [35].
- Authentication—origin of the message is authenticated [35, 36].
- Integrity—it makes sure that the contents of the message are not modified during transmission [37].
- Non-repudiation—it ensures that the sender of the message does not claim of not sending the message to the authorized person [36].
- Access control—it ensures that the only person has access to the message [37].

Cryptography can be classified into symmetric and asymmetric cryptography [35]. In symmetric cryptography, only one key is used for encryption and decryption. In asymmetric cryptography, 2 keys are used: one for encryption and another for decryption.

4.1 DES

DES stands for data encryption standard, and it was the first standard recommended by National Institute of Standard and Technology [36]. It is a block cipher that uses secret key for both encryption and decryption [35]. It takes fixed length of plain text and transforms into same length of cipher text. In DES, each block size is of 64 bits and uses 56 bits key. The decryption can only be done using the key which was used to encrypt the message [38].

4.2 TDES

TDES stands for triple DES. It is the enhancement of DES but uses 3 keys each of 56 bits key size. TDES provides key of larger size, hence increasing the computational complexity [38]. Encryption method is same as DES, but it is applied 3 times to increase the encryption level [35]. TDES algorithm which uses three keys requires 2^{168} possible combinations, and the algorithm which uses two keys requires 2^{112} combinations. Hence, TDES is said to be the most strongest encryption algorithm, but one disadvantage is that it is very time-consuming [35].

4.3 AES

It is a block cipher and a symmetric key algorithm means which uses same key for both encryption and decryption [36]. AES works on the principle known as substitution and permutation which makes it faster and more efficient algorithm [38]. AES has fixed block size of 128 bits, and a key size of 128, 192, or 256 bits [35].

4.4 RSA

RSA stands for Ron Rivest, Adi Shamir, and Leonard Adleman, who first publicly described the algorithm in 1977 [36]. It is an asymmetric algorithm and is widely used for secure data transmission.

Two different keys are used for encryption and decryption: (i) public key and (ii) private key. The former one is used for encryption, and the latter one is used to for decryption [35].

In the next section, a comparative study is made on different encryption techniques used so far.

Table 2 Comparative study

Criteria	Watermarking	Steganography	Cryptography
Carrier	Any multimedia data	Any multimedia data	Text files
Visibility	Visible or invisible	Not visible	Visible
Robustness	High	Moderate	Less
Capacity	Depends on the size of hidden data	Usually low	High
Objective	To protect copyright information	To prevent discovery of secret message	To prevent unauthorized access
Failure	Removed	Detected	Deciphered

5 Comparative Study

Watermarking, steganography, and cryptography are well-known security techniques and are widely used to provide security for highly confidential data. All three techniques are useful for real-time encryption and are suitable for different applications. A comparative study on these security techniques is given in Table 2.

6 Conclusions and Future Scope

In the digital world nowadays, the security of digital images become more and more important since the communications of digital products over open network occur more and more frequently. In this chapter, we have surveyed existing work on image encryption

It also presents a background discussion on major techniques of steganography and watermarking. Some important techniques used in steganography and watermarking and few encryption algorithms used in cryptography are discussed. Both steganography and watermarking are divided into spatial domain and transform domain. In spatial domain, LSB is the most important technique used for image encryption. In transform domain, DCT, DWT, and DFT are the commonly used techniques for image encryption. Spatial domain techniques are said to be less robust compared to transform domain techniques. Watermarking is robust to most of the signal processing techniques and geometric distortions compared to steganography and cryptography. PSNR is the most commonly used parameter to measure the quality of encrypted data. Lena and boat images are the most commonly used testing images. Few algorithms on image watermarking and steganography are reviewed and are robust against different kinds of attacks. General description on text, audio, and video is also given.

Nowadays, many companies have already been active in digital watermarking. For example, Microsoft has developed a system that limits unauthorized playback

which helps music industry for copyright protection. Future development of multimedia systems in the Internet is conditioned by the development of efficient methods to protect data owner from copyright violations. But many encryption systems do not solve this problem. Hence, different encryption systems must be proposed in order to give copyright protections.

References

1. Dey N, Das P, Roy AB, Das A, Chaudhuri SS (2012) DWT-DCT-SVD based intravascular ultrasound video watermarking. In: 2012 World congress on information and communication technologies (WICT). IEEE, pp 224–229
2. Dey N, Mukhopadhyay S, Das A, Chaudhuri SS (2012) Analysis of P-QRS-T components modified by blind watermarking technique within the electrocardiogram signal for authentication in wireless telecardiology using DWT. *Int J Image Graph Signal Process* 4(7):33
3. Dey N, Maji P, Das P, Biswas S, Das A, Chaudhuri SS (2013) An edge based blind watermarking technique of medical images without devalorizing diagnostic parameters. In: 2013 International conference on advances in technology and engineering (ICATE), IEEE, pp 1–5
4. Dey N, Biswas S, Roy AB, Das A, Chowdhuri SS (2013) Analysis of photoplethysmographic signals modified by reversible watermarking technique using prediction-error in wireless telecardiology. International conference on intelligent infrastructure the 47th annual national convention at Computer Society of India
5. Chakraborty S, Samanta S, Biswas D, Dey N, Chaudhuri SS (2013) Particle swarm optimization based parameter optimization technique in medical information hiding. In: 2013 IEEE International conference on computational intelligence and computing research (ICCIC). IEEE, pp 1–6
6. Dey N, Das P, Chaudhuri SS, Das A (2012) Feature analysis for the blind-watermarked electroencephalogram signal in wireless telemonitoring using Alattar's method. In: Proceedings of the fifth international conference on security of information and networks. ACM, pp 87–94
7. Dey N, Biswas S, Das P, Das A, Chaudhuri SS (2012) Feature analysis for the reversible watermarked electrooculography signal using low distortion prediction-error expansion. In: 2012 International conference on communications, devices and intelligent systems (CODIS). IEEE, pp 624–627
8. Dey N, Biswas S, Das P, Das A, Chaudhuri SS (2012) Feature analysis for the reversible watermarked electrooculography signal using low distortion prediction-error expansion. In: 2012 International conference on communications, devices and intelligent systems (CODIS). IEEE, pp 624–627
9. Chakraborty S, Maji P, Pal AK, Biswas D, Dey N (2014) Reversible color image watermarking using trigonometric functions. In: 2014 International conference on electronic systems, signal processing and computing technologies (ICESC). IEEE, pp 105–110
10. Chen WY, Huang SY (2000) Digital watermarking using DCT transformation. Department of Electronic Engineering, National ChinYi Institute of Technology, Taichung
11. Chopra D, Gupta P, Sanjay G, Gupta A (2012) LSB based digital image watermarking for gray scale image. *IOSR J Comput Eng (IOSRJCE)*. ISSN:2278-0661
12. Kaur G, Kaur K (2013) Implementing LSB on Image Watermarking using text and image. *Int J Adv Res Comput Commun Eng*. ISSN:2319-5940
13. Sharma PK (2012) Rajni, "Information security through Image watermarking using Least Significant Bit Algorithm,". *Comput Sci Inf Technol* 2(2):61–67
14. Gajriya LR, Tiwari M, Singh J (2011) "Correlation based watermarking technique-threshold based extraction,". *Int J Emerg Technol* 2(2):80–83

15. Awasthi M, Lodhi H (2013) Robust image watermarking based on discrete wavelet transform, discrete cosine transform & singular value decomposition. *Adv Electr Electron Eng* 3(8):971–976
16. Narang M, Vashisth S (2013) Digital watermarking using discrete wavelet transform. *Int J Comput Appl* 74(20)
17. Singh AP, Mishra A (2011) Wavelet based watermarking on digital image. *Indian J Comput Sci Eng* 1(2), 86–91
18. Kashyap N, Sinha GR (2012) Image watermarking using 2-level DWT. *Adv Comput Res* 4(1):42–45
19. Kaushik AK (2012) A novel approach for digital watermarking of an image using DFT. *Int J Electron Comput Sci Eng* 1(1):35–41
20. Marjuni A, Fauzi MFA, Logeswaran R, Heng SH (2013) An improved DCT-based image watermarking scheme using fast Walsh Hadamard transform. *Int J Comput Electr Eng* 5(3):271
21. Dhar PK, Kim JM (2011) Digital watermarking scheme based on fast Fourier transformation for audio copyright protection. *Int J Secur Appl* 5(2):33–48
22. Dhar PK, Khan MI, Jong-Myon K (2010) A new audio watermarking system using discrete fourier transform for copyright protection. *Int J Comput Sci Netw Secur* 6:35–40
23. Lei B, Soon Y, Zhou F, Li Z, Lei H (2012) A robust audio watermarking scheme based on lifting wavelet transform and singular value decomposition. *Sig Process* 92(9):1985–2001
24. Arnold M (2000) Audio watermarking: features, applications, and algorithms. In: *IEEE international conference on multimedia and expo (II)*, pp 1013–1016
25. Doerr G, Dugelay JL (2003) A guide tour of video watermarking. *Signal Process Image Commun* 18(4):263–282
26. Jaseena KU, John A (2011) Text watermarking using combined image and text for authentication and protection. *Int J Comput Appl* 20(4):8–13
27. Jaseena KU, John A (2011) An invisible zero watermarking algorithm using combined image and text for protecting text documents. *Int J Comput Sci Eng* 3(6):2265–2272
28. Jalil Z, Jaffar MA, Mirza AM (2011) A novel text watermarking algorithm using image watermark. *Int J Innov Comput Inf Control* 7(3)
29. Gupta S, Gujral G, Aggarwal N (2012) Enhanced least significant bit algorithm for image steganography. *IJCEM Int J Comput Eng Manag* 15(4):40–42
30. Banik B (2013) A DWT Method for image steganography. *Int J Adv Res Comput Sci Softw Eng* 3(6):983–989
31. Nag A, Biswas S, Sarkar D, Sarkar PP (2011) A novel technique for image steganography based on DWT and Huffman encoding. *Int J Comput Sci Secur* 4(6):497–610
32. Ghoshal N, Mandal JK (2012) Image authentication technique in frequency domain based on discrete Fourier transformation (IATFDDFT). [arXiv:1212.3371](https://arxiv.org/abs/1212.3371)
33. Bansal D, Chhikara R (2014) An improved DCT based steganography technique. *Int J Comput Appl* 102(14)
34. Kaur B, Kaur A, Singh J (2011) Steganographic approach for hiding image in DCT domain. *Int J Adv Eng Technol* 1(3):72
35. Patel BK, Pathak M (2014) Survey on cryptography algorithms. *Int J Innov Technol* 4(7)
36. Elminaam DSA, Kader HMA, Hadhoud MM (2008) Performance evaluation of symmetric encryption algorithms. *IJCSNS Int J Comput Sci Netw Secur* 8(12):280286
37. Patel KD, Belani S (2011) Image encryption using different techniques: a review. *Int J Emerg Technol Adv Eng* 1(1):30–34
38. Mitali VK, Sharma A (2014) A survey on various cryptography techniques. *Int J Emerg Trends Technol Comput Sci* 3(4):6
39. Devi KJ (2013) A secure image steganography using LSB technique and pseudo random encoding technique. Doctoral dissertation. National Institute of Technology-Rourkela
40. Kaur M, Mahajan K (2015) An existential review on text watermarking techniques. *Int J Comput Appl* 120(18)
41. Dey N, Roy AB, Dey S (2012) A novel approach of color image hiding using RGB color planes and DWT. [arXiv:1208.0803](https://arxiv.org/abs/1208.0803)

Intelligent Techniques in Signal Processing for
Multimedia Security

Dey, N.; Santhi, V. (Eds.)

2017, IX, 485 p. 226 illus., 96 illus. in color., Hardcover

ISBN: 978-3-319-44789-6