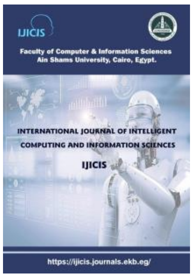
IJICIS, Vol.22, No.3, 14-38
DOI: 10.21608/ijicis.2022.130393.1174

International Journal of Intelligent Computing and Information Sciences

https://ijicis.journals.ekb.eg/


IJICIS
Faculty of Computer & Information Sciences Ain Shams University, Cairo, Egypt.
INTERNATIONAL JOURNAL OF INTELLIGENT COMPUTING AND INFORMATION SCIENCES
IJICIS
https://ijicis.journals.ekb.eg/

A Survey on Image Data Hiding Techniques

Mahmoud Magdy*
DMT Department, Future University in Egypt (FCIT)
Cairo, Egypt
Mahmoud.abdo@fue.edu.eg

Neveen I. Ghali
DMT Department, Future University in Egypt (FCIT)
Cairo, Egypt
Neveen.ghali@fue.edu.eg

Said Ghoniemy
Department of Computer systems (FCIS)
Ain Shams University
Cairo, Egypt
ghoniemy1@cis.asu.edu.eg

Received 2022-03-29; Revised 2022-04-17; Accepted 2022-04-19

Abstract: *Due to the observed growth in recent years of digital image communication, computer technologies, and image processing techniques image security has been an essential demand due to the different image attacks. Image security approaches are classified into cryptography and data hiding techniques, including digital watermarking and steganography. This study paper reviews existing picture data hiding techniques, their benefits and drawbacks, and future research directions. In addition to the survey, we included a brief explanation of several geometric and image processing attacks that impair picture transmission. General multimedia security ideas, primary requirements, and recent applications We addressed various approaches and their characteristics, types, requirements, and working mechanisms. We classify the techniques based on different domains. General concepts of data hiding approaches, their characteristics, recent applications used in, also recent research work for proposed techniques is discussed in the following sections, finally, a comparison between different methodologies has been presented in a table.*

Keywords**:** *Watermarking; Steganography; Attacks; Copyright; Spatial domain; Transform domain.*

***Corresponding Author**: Mahmoud Magdy
DMT Department, Future University in Egypt (FCIT), Cairo, Egypt
Email address: Mahmoud.abdo@fue.edu.eg

1 Introduction

The usage of the internet for sharing and transferring vast volumes of data has seen rapid advancements. Multimedia security has recently become one of the most crucial issues for all applications to protect data while it is stored and transmitted via the web. In the recent decade, multimedia communication is widely used, which is crucial in many fields such as entertainment, industrial, economics, eHealth, and military applications [1].

Multimedia data, has been transmitted rapidly and widely to destinations via the internet in various forms such as video, audio, text, and images. Digital data transmitted via the internet is attainable and detectable to all users. Data content can be freely eavesdropped, gathered, replicated, and distributed unlawfully due to the process of sending the data over the transmission medium, data repository, and data processing. The multimedia has unique features, requiring particular requirements of the encryption method [2]. Multiple techniques have been proposed to secure the images and prove ownership such as watermarking and steganography as shown in Figure 1.

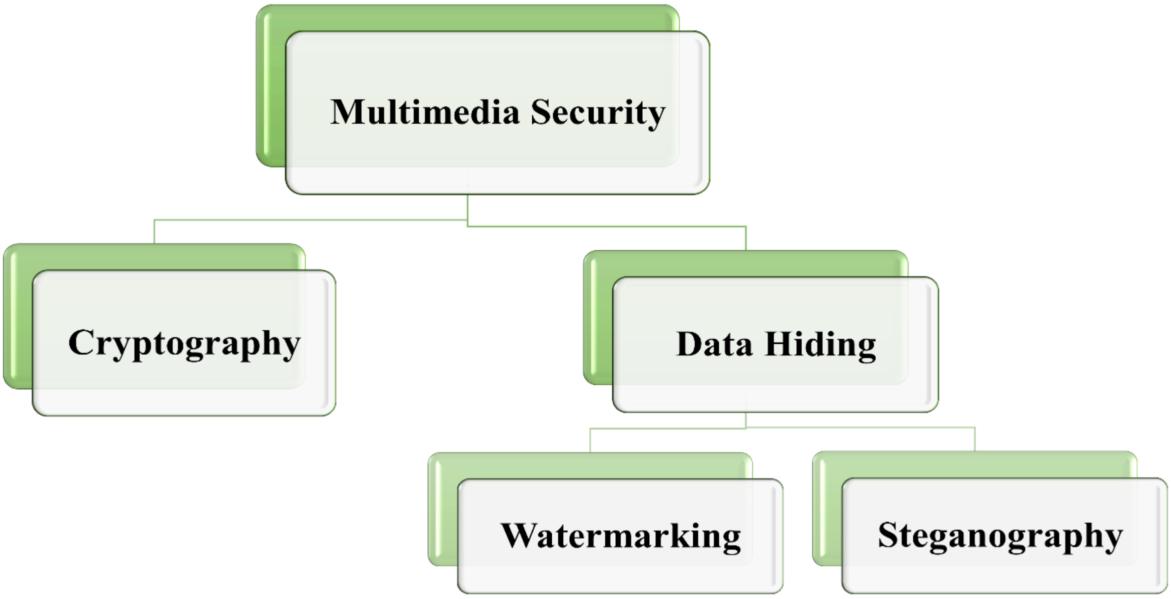
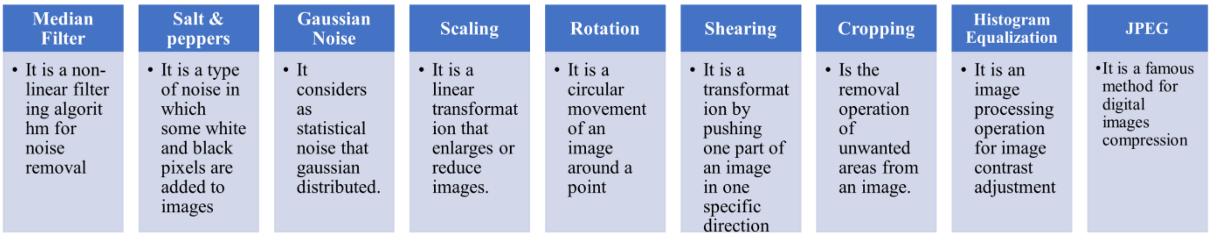


Figure. 1. Multimedia Security approaches

1.1 Attacks

As illustrated in Figures 2, many types of attacks can have an impact on images while they are being transmitted through multimedia networks. These attacks are classed as noise attacks (salt and pepper, Gaussian noise), geometric attacks (translation, scaling, and rotation), and other [3]. On the other side, image denoising like an average filter, median filter, and Sobel filter. Histogram equalization and adaptive histogram are an example of image processing attacks. Additionally, image compression attacks.



Median Filter	Salt & peppers	Gaussian Noise	Scaling	Rotation	Shearing	Cropping	Histogram Equalization	JPEG
• It is a non-linear filter ing algorit hm for noise removal	• It is a type of noise in which some white and black pixels are added to images	• It considers as statistical noise that gaussian distributed.	• It is a linear transformat ion that enlarges or reduce images.	• It is a circular movement of an image around a point	• It is a transformat ion by pushing one part of an image in one specific direction	• Is the removal operation of unwanted areas from an image.	• It is an image processing operation for image contrast adjustment	•It is a famous method for digital images compression

Figure 2. Examples of Image Attacks

2 Steganography

Steganography approach presnted to prevent eavesdropping on encrypted data transmissions. The idea behind steganography was to hide digital data. Steganography comes from the Greek terms stegano, which means "covered," and graphy, which means "written." As a result, the two words have become synonymous with "covered writing" [4]. Using the private key, it explores different methods for embedding . A secret message is the name given to the hidden content, while a cover file is the name given to the container in which the secrete file is kept. Any sort of multimedia element, including video, music, photos, and text, can be used as the cover [5].

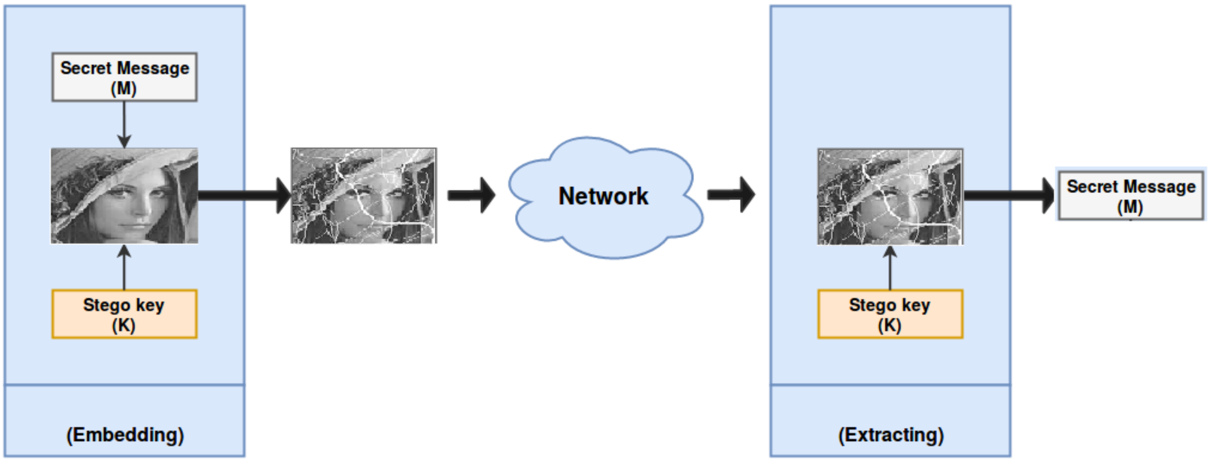


Figure. 3. Steganography Embedding and Extraction Phase

Steganography, as previously said, includes embedding crucial information within another multimedia file, as shown in Figure 3. As a result, steganography models must have a more expanded equivalent capability [4].

The authors demonstrate three key criteria for a good steganographic system in [5 and 6]. Security, imperceptibility, and payload capacity are all important considerations. Figure 5 depicts a fourth quality identified in their research [8]: robustness. As a result, any proposed algorithm should retain the majority of these qualities.

As shown in Figure 4, various steganography approaches can be classified as spatial, transform, adaptive domains, region-based, human vision, and machine learning. This classification will be described in greater depth in the next sections, along with some recent research [9].

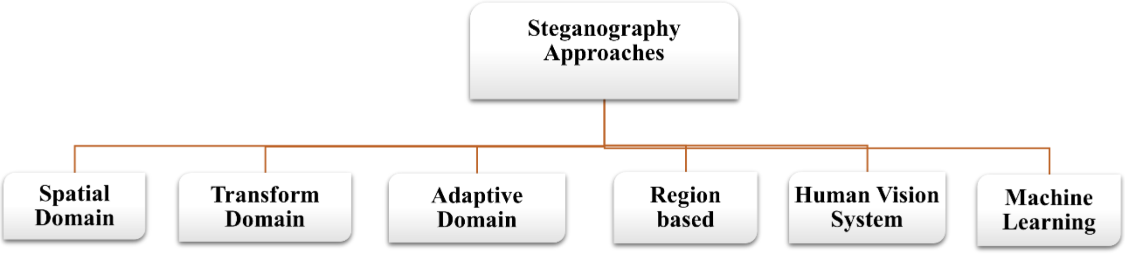


Figure 4. Steganography Approaches

2.1.1 Spatial Domain

The extraction and embedding processes in these techniques are simple. Some of the most common spatial domain techniques are covered further below. [10] explains some examples from research articles.

The secret information can be concealed using pixel value differencing (PVD) by matching the difference between two successive pixel values. During the embedding phase of the PVD technique [11], both the carrier picture and the secret information are chunked into blocks. Pixel value differencing outperforms least significant bit (LSB) techniques for extensive embedding.

Hussain et al. [12] proposed data hiding that uses adaptive PVD blocks that consider significant ones by applying pseudo-random number techniques for nominating the blocks [13]. The LSB is straightforward and considered a low computational methodology, so it is widely used. This method's main idea is that the secret information is embedded in the host image by modifying the least significant bit of elected pixels by a method that the naked eye cannot detect without affecting the original cover image quality. Unimportant information is usually represented in the least significant bits, and a slight modification in those bits is undetectable by the naked eye. Most LSB steganography techniques [14][15] focus only on designing the model to increase the embedding capacity of host image bits by maximizing the number of pixels in the cover image used in embedding operation. Steganalysis has become developed enough to violate steganographic systems. So now, most of the research issues are focused on developing more robust LSB mechanisms that can avoid such steganalysis attacks [16].

In the difference expansion-based system, secret information is embedded over different pixel pairs. The majority of these techniques are classified as reversible stegano systems because both secret data and host media can be extracted without any distortion. The sensitive information gets embedded over the expanded difference [17].

In [18], the carrier image's LSB bits are preserved to add to the system's reversibility feature. In the embedding stage, the LSB data bit is compressed. Coding is applied and hides these bits with secret information. Also, Jung et al. [19] proposed a different expansion-based steganographic algorithm called histogram shifting. The primary strategy of this method is histogram shifting of the host image. Firstly, determine the least and highest values in the host media and then embed it by changing the highest and lowest points [20][21]. This method's main characteristic is that reversibility also provides a higher capacity of payload and ensures imperceptibility.

Tai et al. [22] proposed a reversible technique based on histogram shifting that utilized a method for embedding the highest and lowest points in the carrier. The proposed technique makes a stego-image highly prone to intruder attacks, low payload capacity, and low imperceptibility. Nyeem [23] proposed an indirect embedding model by hybridizing each histogram shifting technique and a bit plane.

2.1.2 Transform Domain

The transform domain breaks down the image into frequency coefficients before integrating essential information. In terms of attack resistance, this technique has a lot of benefits. It is impervious to attacks that alter secret data. The transform domain techniques have some shortage, such as a low payload capacity and a high computational complexity. Some of the techniques employed include the IWT, DCT, DWT, and DFT.

DFT is a typical signal processing transform technique. DFT is commonly used in image processing methods. [24] mentions a revised Fourier transform technique based on steganography. Khashandarag et al. [25] suggested a stegano model based on DFT. The sensitive data is compressed using the LZW algorithm and encrypted by XORing these bits with pseudo-random integers. The author also used the DES algorithm on the blocks of data to increase security. The host media is transformed into DFT components, then encrypted secret bits over the elected DFT coefficient are embedded, and then inverse DFT is utilized to be transformed to the original image.

DCT is considered one of the most effective techniques for converting multimedia from the time domain to its transform domain. Basic steganography-based DCT is most commonly used in image security. the image is decomposed into corresponding low, middle, and high-frequency coefficients. [26]. Secret information bits compressed by JPEG compression technique before embedding in DCT coefficients is shown in the paper [27].

Savithri et al. [28] proposed two techniques, DCT combined with RSA, and others with chaotic. The secret information is encrypted before embedding into the DCT components. Saidi et al. [29] proposed a combination between the DCT approach and chaotic map. The method applies DCT on the host image to embed the sensitive data inside regions elected using a chaotic method. The DWT has become an alternative because it is flexible and adaptable to the human visual system (HVS). It covers the sensitive data in the regions with low sensitivity to the HVS. Using these techniques raises the robustness with high imperceptibility. DWT is performed in a vertical direction followed by a horizontal direction. As mentioned in [30], secret media are decomposed into HH, LL, LH, and HL to set the following coefficient values.

Nonetheless, DWT generates a floating-point value for the coefficients and casts them into an integer since the pixel's values are integers. Any truncation in this coefficient may destroy the embedded information according to Arunkumar et al. [31]. Xiong et al. [30] adopt an integer wavelet transform to overcome the floating-point problem, which can map an integer input to integer output to prevent the floating-point of wavelet filters. The IWT LL sub-band is similar to the original image to the DWT LL [32][33][34].

2.1.3 Adaptive Domain Image

Subhedar and Mankar [35] used the term "statistics-aware embedding" for adaptive domain steganography, which is also known as "Model-Based" [36]. Every transform and spatial strategy is included in an adaptive technique. This technique may choose random adaptive pixels for each block separately based on the cover image.

This work [37] describes a new frequency domain data concealing strategy based on adaptive wavelet transform and genetic algorithm. The encrypted information is incorporated in the resulting frequency coefficients once the cover images are transformed to frequency domain. The results of the simulation reveal that the suggested technique is resilient and unnoticeable, as measured by PSNR.

Hameed et al.[38] introduce a new image steganography technique based on PVD and LSB that does not take differing content in a cover image into account while hiding secret data. Using this characteristic in embedding diverse secret information in different edges to improve robustness based on the distribution of each pixel intensity. Extensive experiments demonstrated that the suggested method has a high embedding capacity when compared to various existing state-of-the-art schemes.

2.1.4 Human Vision System

HVS is regarded as a method for viewing, interpreting, and processing optical data. These methods are mostly centred on detecting the target region in order to conceal sensitive information using any of the transform or spatial domains.

Thahab et al. [39] presented a new video steganography approach that uses the lifted wavelet domain to disguise data. Using three secret keys, the secret data is embedded in the cover's coefficients via YCbCr colour space. The performance of the method is evaluated using Normalized Cross-Correlation (NCC) and peak signal to noise ratio, which indicate good imperceptibility and embedding capability.

Kadhim et al. [40] suggested an attempt to provide a novel strategy employing the Dual-Tree Complex Wavelet Transform (DT-CWT) approach to modify edge-based picture steganography, which gives imperceptibility and increased payload capacity. PSNR and SSIM are used to assess the algorithm. Experiment results reveal an improvement in security that prevents data hacking and outperforms the state-of-the-art.

2.1.5 Region-based steganography

As previously stated, steganography techniques is used to secure image in an unnoticed manner. In order to maximise usage of regions in host images [41].

The high-frequency pixels utilised in covering secured data by the LSBM revisited technique in [42] were chosen based on the threshold value. The author proposed ways for regulating the capacitance of concealment depending on image features in [43]. The "ant colony optimization" approach was employed by the researcher in [44] to choose cover picture pixels, and then LSB was utilised for the embedding procedure.

Laishram et al. [45] aim in their proposed model to address the shortcoming of the given method's spatial domain by constructing a Block-wise Edge Adaptive Steganography Scheme (BEASS) in which the region to embed is dynamically chosen to provide high payload with little distortion. The suggested approach was validated and compared to current algorithms, this method provides a high PSNR which is resistant to histogram assaults.

Naji et al. [46] suggested a method for selecting embedding regions based on the LSB approach. Aside from the upgraded RSA technique, the Elliptic Curve Equation is utilised to provide a second level of protection. Two datasets were used to test and assess the provided technique. The method is robust, secure, and produces high-quality images.

2.1.6 Machine Learning Techniques

AI and machine learning (ML) are now widely used in a wide range of advanced applications [47][48]; it was originally developed for optimization, object retrieval, and recognition [49].

Any steganographic technique is said to be efficient if the embedding process does not creates any minimal distortion in the stego-image while maintaining high embedding capacity and minimising retrieval mistakes. Many advanced machine learning algorithms have been developed to achieve this efficiency [50]. NN[51],SVM[52], GA [53][54] are some of the machine learning systems used, as shown in Figure 5. The following sections show some of the related research projects.

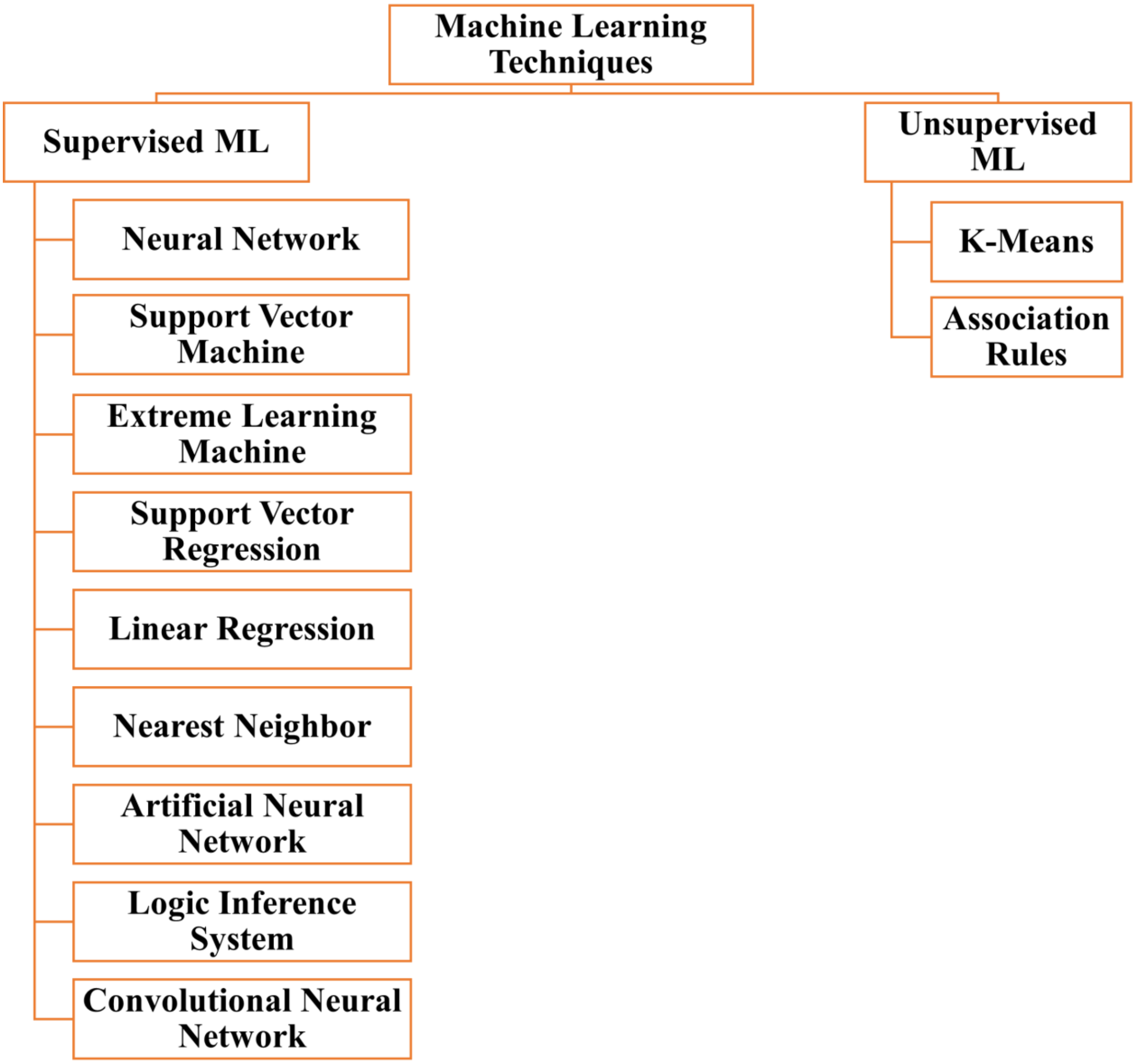


Figure 5. Machine learning Techniques

In [55], the authors utilized SVM for steganography-based techniques optimization by finding suitable embedding regions with high imperceptibility and security while keeping retrieval errors to a minimum, as soon as possible, with faster computing [56].

Chang et al. [57] described a methodology to enhance the payload's capacity by utilizing a 2-level quantization stage. In research [58], they developed a technique using a bitmap generation algorithm to enhance each embedding time and embedding capacity. Most neural network-based stegano models are concerned with the system's imperceptibility and robustness by analyzing the complete image details. Such techniques utilize a back-propagation approach to achieve optimum embedding locations. Lou et al. applied their model to study the features of the host media. Multiple characteristics like luminance, entropy, and frequency are used [59].

3 Watermarking

The development of image processing techniques made it easier to copy, alter, and share digital content at a low cost while maintaining high quality. Watermarking digital photographs is an alternative way for detecting tampering and proving ownership [60]. As seen in Figure 6, watermarking is a means of inserting a piece of information in image without changing its value in order to identify the data's original source.

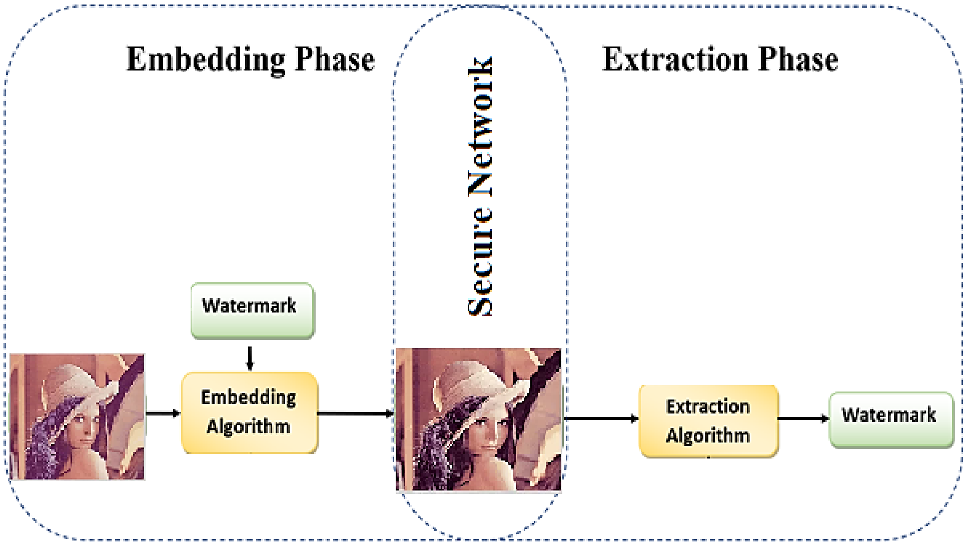


Figure 6: Digital Watermark System

Watermarking overcomes steganography's limitations by putting a watermark into the cover image, which prevents the watermark from being discovered [61]. The multiple requirements of the watermarking approach are depicted in Figure 7.

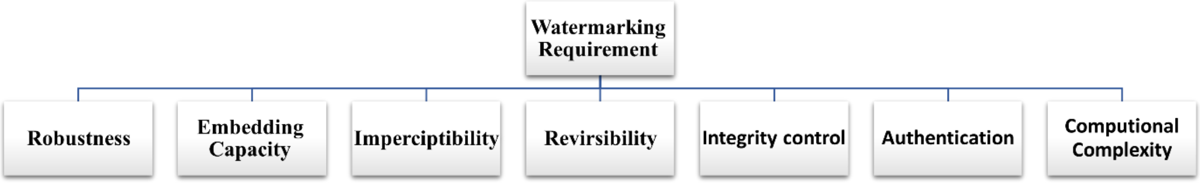


Figure 7: Digital Watermarking System Requirement

A digital watermarking system is divided into three stages: generating the watermark, embedding, and extraction. When a digital image's copyright is in issue, the extract the watermark to prove his copyrights.

3.1 Main watermarking scheme components.

(a) Phase I: Watermark Generation

The generated watermark is embedded in the cover image. Watermark may be a binary image or personal information which is unique to the user.

(b) Phase II: Watermark Embedding

The watermark is embedded in the image using various watermarking approaches such as

LSB replacement, histogram shifting, and so on [62].

(c) Phase III: Watermark Extraction

Is the process of extracting the watermark to verify the author's ownership, integrity, and authenticity.

In this subsection, a review of some recent research for image watermarking mechanisms is discussed.

3.2 Watermarking approaches

Figure 8. depicts a classification of watermarking approaches. Watermarking was classified into four types: human perception, domain-based, reversibility , and procedural type [63].

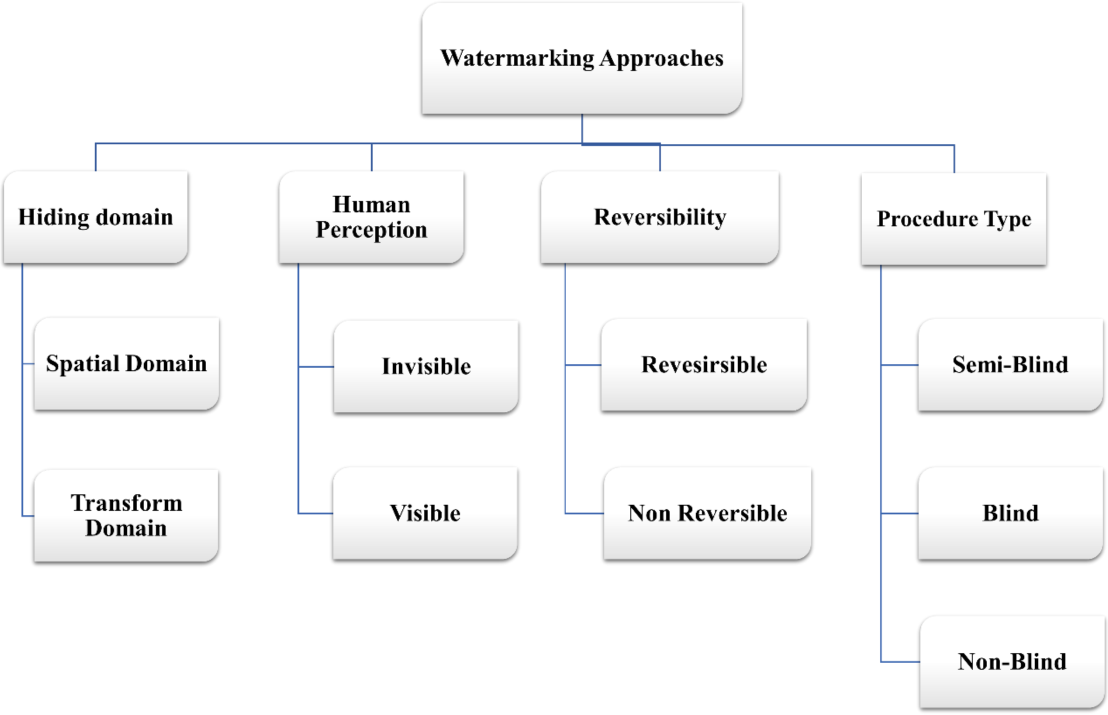


Figure 8. Watermarking Approaches

3.2.1 Hiding Domain

This paper provides an overview of watermarking techniques used in different applications. The sections that follow provide a brief overview of each technique.

1- Spatial Domain Techniques

The pixel values are explicitly adjusted in this domain to integrate the watermarked media. LSB, LBP, histogram equilization, and spread spectrum approaches are examples of methodologies. The watermark in LSB is embedded by replacing the rightmost bits of each pixel [64].

In LBP, the watermark is embedded by segmenting the original image into non-overlapped square blocks. Then, the embedding of the watermark bits is started. LBP-based methods are robust against contrast adjustment but cannot stand with blurring and filtering operations.

In the histogram, the modification watermark is hidden by shifting the histogram's maximum and minimum pixels. This technique has a limitation in the capacity as it is limited by the number of maximum pixels they represent. Patchwork is also one of the spatial domain techniques embedded by picking out the embedding positions using pseudo-random generated numbers as mentioned in [65]. The authors of [66] used the estimated error expansion method to cover secret data in the cover image's side segmented area. The image is divided into background regions, and the object region then calculates their histogram. The embedding process is concentrated on the background region rather than the object region to minimize image quality distortion.

The authors are looking forward to keeping the original image without distortion with high embedding capacity. In [67], the authors proposed a moment-based watermarking technique. The results proved that this method is very efficient under different attacks when compared to existing methods.

Hassan et al. proposed a robust watermarking method for secure storage and transmission of medical images. In [68], Aparna et al. also proposed a technique for health data security. The watermarks may be a patient report embedded in the selected part of the cover image. A suitable compression algorithm compressed the watermark to achieve more embedding capacity, and then the authors used pseudo-random numbers for the watermark embedding process.

The authors of [69] discuss a highly secure and numerically stable method in which the Arnold algorithm is applied and Quaternion Legendre-Fourier moments are computed from the host color image computed. Then the watermark is embedded.

In [70], the authors developed a reversible technique, in which the interpolation technique has been used to embed multiple watermarks inside pixels of the host image. The magic rectangle algorithm was applied for encryption before embedding. The results of the study on various images showed that the methodology was imperceptible, robust, and secure, with high payload capacity and good image quality.

2- Transform Domain

The host media coefficients are recreated following the embedding process in frequency domain mechanisms. DFT, DCT, RDWT, SVD, DWT, and other techniques are included in the methodology [71]. The spatial-domain approaches are still simpler in but low resistant to geometric attacks. For evaluating some attributes, the spatial and transform domain methodologies are compared. The next section discusses some preliminary research effort.

Hurrah et al. [72] propose an efficient watermarking scheme based on discrete cosine transform (DCT) domain and Discrete wavelet transform (DWT). The proposed scheme is secure to many kinds of geometric attacks and signal processing attacks which are measured using PSNR, NCC, BER.

Kishore et al. [73] proposed robust and blind discrete cosine transform-based watermarking scheme to achieve imperceptibility, robustness, blindness. The embedding process is accomplished by inserting the watermark in the DCT coefficients in two different locations to maintain the unambiguity. The algorithm is tested on eight different images. Experimental results demonstrate the imperceptibility, robustness in addition to low computational complexity.

In this paper [74] the authors present a color digital image watermarking scheme using the DWT-DCT and Arnold scrambling to improve the robustness and invisibility.

This paper [75], presents a watermarking algorithm based on the Generalized Gaussian Distribution (GGD) and the Neyman-Pearson (NP) criterion in which the image block is considered in the embedding process.

In this paper [76] a technique using concepts of DWT, SVD proposed to protect the copyright of the content. The experimental analysis using PSNR and NC shows that this scheme is robust.

3.2.2 Human Perception

The watermark is an effect inserted in an image that can be invisible or visible in order to identify who owns the data [77]. Digital watermarking has shown to be an effective approach for improving image copyright protection.

3.2.3 Zero watermarking

This section categorizes the zero watermarking approaches into traditional, and moment-based approaches.

- Traditional Techniques

Utami et al. [78] proposed a new hybrid zero watermarking algorithm based on discrete cosine transform (DCT), speeded-up robust features (SURF), singular value decomposition, and chaotic (Arnold's Cat Map) for medical images watermarking. The proposed algorithm was tested by applying various attacks. Experimental analysis for the results shows that SVD utilized in the proposed algorithm is robust against various attacks like signal processing, geometric attacks, JPEG compression attacks, and noise addition than the other state-of-the-art techniques.

Xiyao Liu et al. [79] addressed a multi-slice feature zero-watermarking scheme to improve robustness and distinguishability for medical imaging based on ring statistics and logistic-logistic system based chaotic map to guarantee distinguishability, robustness, and security the scheme results demonstrate that the proposed scheme satisfies the lossless quality requirement and robust against different attacks.

Qin et al. [80] proposed a new zero-watermarking methodology for medical image security. Firstly, the feature vector is constructed based on extracted features using Curvelet-DCT; then, the watermark is encrypted using a pseudo-random sequence. The proposed algorithm does not perform well on Gaussian noise attacks and cropping attacks but is robust against traditional attacks. The ownership share is constructed using the extracted features and the binary watermark.

- Moment-based Techniques

Ma et al. [81] proposed a new zero-watermarking scheme for protecting medical images. The essential features are extracted using the Gaussian numerical integration (GNI) method and chaotic mapping. Then, by using and ternary number theory, and APCET the feature vector was constructed. The experimental results show the robustness against common and geometric attacks.

In this paper [82], the authors proposed a new robust moment-based zero watermarking technique for color stereoscopic images based on Continuous orthogonal moments (COMs). Firstly, the color components of the images are coded and provide a good image descriptor. Experimental analysis shows that the proposed algorithm is stable and robust against various image processing attacks.

Xia et al. [83] proposed a Zero-watermarking scheme to resist desynchronization attacks, such as translation and cropping based on local feature regions (LFRs) and quaternion polar harmonic Fourier moments (QPHFMs). The stable features are extracted from the original medical image using SURF. Then the QPHFMs of the LFRs were calculated to generate multiple zero-watermarks. The experimental results indicate that the proposed scheme can resist standard image processing and geometric attacks compared with the state-of-the-art LFR zero-watermarking schemes.

4 Performance Measurement Metrics

The presented techniques can be evaluated in terms of computation complexity, robustness , excusio time, and image quality. Figure 11 summarises these metrics. Some of these measures are addressed in the following lines.

4.1 Image Quality Measurement

1- Peak Signal to Noise Ratio (PSNR) [84] is used to measure the imperceptibility of the original and watermarked image calculated using the following equation

$$\mathbf{PSNR = 10_{log}\frac{(255)^2}{MSE}}$$

2- Mean Square Error (MSE) [84]
is used to measure the similarity between two images, measured using this equation,

where M&N are the image dimensions, I: is the original imag, W is the watermarked image.

$$\mathbf{MSE} = \frac{\mathbf{1}}{\mathbf{M\ x\ N}} \sum_{\mathbf{i=1}}^{\mathbf{M}} \sum_{\mathbf{j=1}}^{\mathbf{M}} (\mathbf{I_{ij}} - \mathbf{W_{ij}})^{\mathbf{2}}$$

3- Normalized Correlation (NC) [84]

This criteria also used for similarity measurement NC=1 is the ideal value. where I: is the original imag, W is the watermarked image.

$$\mathbf{NC} = \frac{\sum_{\mathbf{I=1}}^{\mathbf{M}} \sum_{\mathbf{J=1}}^{\mathbf{N}} \left(\mathbf{I_{orgij}\ x\ W_{recij}}\right)}{\sum_{\mathbf{i=1}}^{\mathbf{M}} \sum_{\mathbf{j=1}}^{\mathbf{N}} \left(\mathbf{I_{org-ij^2}}\ \right)}$$

4- Number of Pixels Changes Rate (NPCR) [85]

Values ranged from 0 to 100, 100 is the ideal value

$$\mathbf{NPCR}: \mathbf{N}(\mathbf{C^1}, \mathbf{C^2}) = \sum_{\mathbf{I,J}} \frac{\mathbf{D}(\mathbf{i}, \mathbf{j})}{\boldsymbol{WxH}}$$

5- The bit error rate (BER) [86]

$$\mathbf{BER} = \frac{\textbf{number of incorrectly decoded bits}}{\textbf{Total number of bits}}$$

6- Unified Average Change Intensity (UACI) [87]. Let us assume two ciphered images C^1 and C^2 whose corresponding plain images have only one-pixel difference and where W and H are the width and height

$$\mathbf{UACI}: \mathbf{U}(\mathbf{C^1}, \mathbf{C^2}) = \sum_{\mathbf{I,J}} \frac{|\mathbf{C^1}(\mathbf{i}, \mathbf{j}), \mathbf{C^2}(\mathbf{i}, \mathbf{j})|}{\boldsymbol{WxH}}$$

5 Discussion

5.1 Statistical Analysis

This part included a statistical depiction in Figure 12 of some major published research work in well-known indexed journals over the last five years in the subject of image security. It is determined that image security is expanding and has considered a significant concern due to its importance.

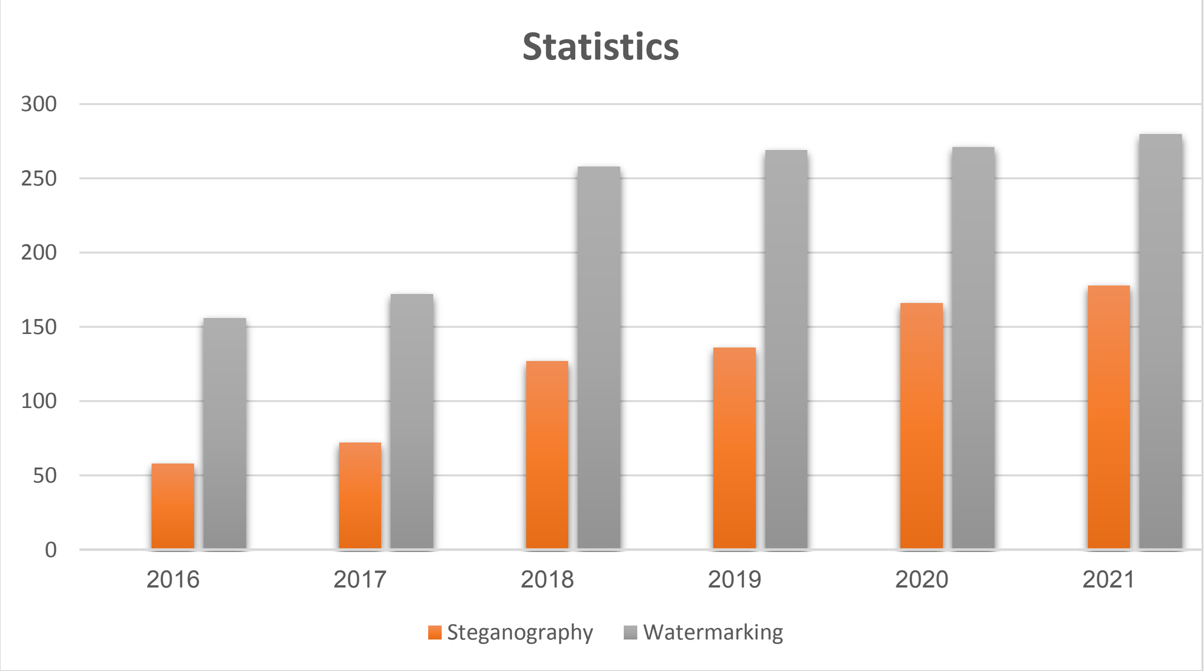


Figure 9. The statistics of published studies in the last five years.

Various technologies, such as steganography and watermarking, are proposed for image copyright protection and tamper detection. Nothing has proven that any of these ways is the best for image security, so we can say that deciding to use any one of these approaches is based on application type and data sensitivity Table 1, Table 2 presents the most current state of art in image security approaches.

6 Points of future research

After the increasing of image transmission over the internet and the development of image processing techniques, so the images can be easily modified, the copyright attacked. The data hiding approach including steganography and watermarking considered a good approach for image copyright protection and attack proving. So, this approach is still a hot topic of research and enhancement in various applications and especially in healthcare applications. Our survey considers a good guide for the researchers to understand this concept and other researchers' contributions. As mentioned, it can be applied in the medical environment which needs to be secured as any modification may lead to a disaster, but the traditional techniques need more enhancement to be applicable for this region. Furthermore, we need more robust feature extraction techniques which can resist the geometric and image processing attacks also need algorithms that do not affect the quality of the transmitted image or lead to any degradation, and also to be fast to appropriate for real-time applications, Deep learning-based data hiding maybe has a good effect in this domain.

Table 1 . Comparison of Various Image Watermarking Techniques

Ref	Technique	Result				Cover Image/Watermark Size	Comments
		PSNR	NC	BER	UACI		
[88]	Discrete Wavelet Transform (DWT), Discrete Wavelet Transforms (DCT), singular value decomposition (SVD)	28.51 dB	1.0	NA	NA	512x512/512x512	Simple robust watermarking technique for various attacks
[89]	DWT	44.05	NA	6.287	NA	512x512/-	Robust for different image attacks
[90]	Redundant Discrete Wavelet Transform (RDWT) &SVD	>35	>0.7	NA	>0.32	512x512/128x128	Semi-blind secure watermarking for image security
[91]	Transform & arnold	52.34dB	0.9785	NA	NA	1024x1024/128x128	Bline watermarking technique for copyright protection
[92]	DWT,DCT,SVD &arnold	43.88 dB	0.9861	0	NA	512x512/256x256	Imperceptible and robust watermarking for patient identity protection
[93]	DWT & SVD	NA	NA	0	NA	1024x1024/32x32	Robust, blind watermarking algorithm for 3D objects
[94]	DWT	38.0358	0.9613	NA	NA	256x256/64x64	Imperceptible watermarking technique for different attacks
[95]	DWT,DCT,SVD	34.68dB	0.9973	NA	NA	512x512 / 256x256	Robust and secure
[96]	Guided dynamic particle swarm optimization (GDPSO) &DWT &SVD	36.87dB	NA	NA	NA	512x512 / 512x512	Non-blind, robust watermarking approach

Table 2. Comparison of Various Image Steganography Techniques

Ref	Used Technique	Result (PSNR)	Payload Capacity	Comments
[97]	lifting wavelet transform （LWT） & Artificial Neural Network (ANN)	43.8dB	512 bits	High robustness against noise with the good visual quality
[98]	Integerwavelet transform （IWT）	50dB	Up to 60%	High visual quality with enhanced security
[99]	Least Signeficant Bit (LSB) & Genetic Algorithm (GA)	53.11 dB	NA	Not robust against geometric attacks
[100]	DCT	32.2dB	NA	High Payload capacity and imperceptibility
[101]	DWT & ANN	36.26dB	Limited	Robust to various noise with the acceptable visual quality
[102]	LSB & IWT	55.52 dB	Good	High security and high invisibility
[103]	Alpha bending & Arnold	55.0702	Good	High robustness, good PSNR for extracted and stego image
[104]	Flipping Distortion measurement (FDM) & Edge Adaptive Grid (EAG) & Connectivity Preserving Criteria (CPC)	49.01	Average	Worse image quality
[105]	RSA 2D-DCT	Above 20	Good	Good performance of algorithms for large images

7 Conclusion

This paper has presented a brief discuss on on image security approaches as steganography, and watermarking have been illustrated. The concept, kinds, characteristics, and requirements, for each approach have been discussed also their potential issues to support further research in this area.

This discussion include the deep illustration for the watermark embedd ng and process, also the steps of the steganography approach have been discussed. Finally, the performance comparisons for different research papers of the discussed techniques are presented in the above tables. Researchers can propose new techniques to secure the images used in different applications with the help of this survey.

Thus we can conclude that choosing between these approaches is depending on different aspects as the sensitivity of secured data and application.

8 Acknowledgments

This is to acknowledge the effort of Prof Dr. Khaled Hosny for advising the research point and for his helpful comments and suggestions.

Reference

[1] X. Wang, A. Akgul, S. Kacar, and V. T. Pham, “Multimedia Security Application o f a Ten-Term Chaotic System without Equilibrium”, Complexity, vol., pp. 1–11, 2017.

[2] Y. Tan, J. Qin, L. Tan, H. Tang, and X. Xiang, ”A survey on the new development of medical image security algorithms”, In International Conference on Cloud Computing and Security, pp. 458-467, 2018.

[3] G. S. Chandel, V. Sharma, and U. P. Singh, “Different Image Encryption Techniques-Survey and Overview”, International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, pp. 434–437, 2016.

[4] S. Atawneh, A. Almomani, H. Al Bazar, P. Sumari, and B. Gupta, “Secure and imperceptible digital image steganographic algorithm based on diamond encoding in DWT domain”, Multimedia tools and applications,vol. 76, pp. 18451–18472, 2017.

[5] J. Kadhim, P. Premaratne, and P. J. Vial, “High capacity adaptive image steganography with cover region selection using dual-tree complex wavelet transform”, Cognitive Systems Research, vol. 60, pp. 20–32, 2020.

[6] C. Warfare, “Cyber Warfare: Steganography vs. Steganalysis”, vol. 47, pp. 76–82, 2004.

[7] M. Bachrach and F. Y. Shih, “Survey of image steganography and steganalysis,” M ultimedia Security, vol. 2, pp. 201–214, 2017.

[8] A. A. J. Altaay, S. Bin Sahib, and M. Zamani, “An introduction to image steganogra phy techniques”, International Conference on Advanced Computer Science Applications and Technologies (ACSAT) pp. 122–126, 2012.

[9] Laishram, Debina, and Themrichon Tuithung, “A survey on digital image steganography: current trends and challenges”, In proceedings of 3rd international conference on internet of things and connected technologies (ICIoTCT), (pp. 26-27), 2018.

[10] J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, “Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research”, Neurocomputing, vol. 335, pp. 299–326, 2019.

[11] F. Pan, J. Li, and X. Yang, “Image steganography method based on PVD and modulus function” , In 2011 International Conference on Electronics, Communications and Control (ICECC), pp. 282–284, 2011.

[12] M. Hussain, A. W. Abdul Wahab, A. T. S. Ho, N. Javed, and K. H. Jung, “A data hid ing scheme using parity-bit pixel value differencing and improved rightmost digit replac ement”,Signal Processing: Image Communication, vol. 50, pp. 44–57, 2017.

[13] O. Hosam and N. Ben Halima, “Adaptive block-based pixel value differencing steganography”, Security and Communication Networks, vol. 9, no.18, pp. 5036–5050, 2016.

[14] R. Chandramouli and N. Memon, “Analysis of LSB based image steganography techniques”, In Proceedings international conference on image processing (Cat. No. 01CH37205), IEEE., vol. 3, pp. 1019–1022, 2001.

[15] M. S. Sutaone and M. V. Khandare, “Image based steganography using LSB insertion”, IET International Conference on Wireless, Mobile and Multimedia Networks, pp. 146–151, 2008.

[16] X. Zhou, W. Gong, W. Fu, and L. Jin, “An improved method for LSB based color image steganography combined with cryptography”,In IEEE/ACIS 15th international conference on computer and information science (ICIS), pp. 4–7, 2016.

[17] C. F. Lee, H. L. Chen, and H. K. Tso, “Embedding capacity raising in reversible data hiding based on prediction of difference expansion”, Journal of Systems and Software, vol. 83, no.10, pp. 1864–1872, 2010.

[18] C. C. Chang, Y. H. Huang, and T. C. Lu, “A difference expansion based reversible information hiding scheme with high stego image visual quality” Multimedia Tools Applications, vol. 76, no.10, pp. 12659–12681, 2017.

[19] K. H. Jung, “High-capacity reversible data hiding method using block expansion in digital images”, Journal of Real-Time Image Processing, vol. 14, no. 1, pp. 159–170, 2018.

[20] C. Qin, C. C. Chang, Y. H. Huang, and L. T. Liao, “An inpainting-assisted reversible steganographic scheme using a histogram shifting mechanism”, IEEE transactions on circuits and systems for video technology, vol. 23, no.7, pp. 1109–1118, 2013.

[21] C. L. Liu and H. H. Liu, “Reliable detection of histogram shift-based steganography using payload invariant features”, In Applied Mechanics and Materials, vol. 284, no.287, pp. 3517–3521, 2013.

[22] J. Der Lee, Y. H. Chiou, and J. M. Guo, “Reversible data hiding based on histogram modification of SMVQ indices”, IEEE Transactions on Information Forensics and Security, vol. 5, no.4, pp. 638–648, 2010.

[23] H. Nyeem, “Reversible data hiding with image bit-plane slicing”, In 20th International Conference of Computer and Information Technology (ICCIT), pp. 1–6, 2018.

[24] A. Soni, J. Jain, and R. Roshan, “Image steganography using discrete fractional Fourier transform” A. Soni, J. Jain, and R. Roshan, “Image steganography using discrete fractional Fourier transform,” 2013 Int. Conf. Intell. Syst. Signal Process. ISSP, pp. 97–100, 2013.

[25] A. S. Khashandarag, A. H. Navin, M. K. Mirnia, and H. H. Agha Mohammadi, “An optimized color image steganography using LFSR and DFT techniques”, In International Conference on Computer Education, Simulation and Modeling, vol. 176 no. PART 2, pp. 247–253, 2011.

[26] H. Dadgostar and F. Afsari, “Image steganography based on interval-valued intuitionistic fuzzy edge detection and modified LSB”, Journal of information security and

applications, vol. 30, pp. 94–104, 2016.

[27] M. S. Subhedar and V. H. Mankar, "Current status and key issues in image steganography: A survey", Computer science review, vol. 13–14, pp. 95–113, 2014.

[28] G. Savithri, Vinupriya, S. Mane, and J. Saira Banu, "Parallel implementation of RSA 2D-DCT steganography and chaotic 2D-DCT steganography", In Proceedings of International Conference on Computer Vision and Image Processing ,vol. 459, pp. 593–605, 2017.

[29] M. Saidi, H. Hermassi, R. Rhouma, and S. Belghith, "A new adaptive image stegan ography scheme based on DCT and chaotic map," Multimedia Tools Applications, vol. 76, no.11, pp. 13493–13510, 2017.

[30] D. Bucerzan and C. Raţiu, "Testing methods for the efficiency of modern steganography solutions for mobile platforms", In 2016 6th International Conference on Computers Communications and Control (ICCCC), pp. 30–36, 2016.

[31] S. Arunkumar, V. Subramaniyaswamy, V. Vijayakumar, N. Chilamkurti, and R. Lo gesh, "SVD-based robust image steganographic scheme using RIWT and DCT for secur e transmission of medical images", Measurement, vol. 139, pp. 426–437, 2019.

[32] F. Gu and J. Lu, "A new composite implicit iterative process for a finite family of n onexpansive mappings in Banach spaces," Fixed Point Theory Applications, pp. 1–11, 2006.

[33] C. T. Kavitha and C. Chellamuthu, "Multimodal medical image fusion based on int eger wavelet transform and neuro-fuzzy", International Conference on Signal and Image Processing. IEEE, pp. 296–300, 2010.

[34] R. O. El Safy, H. H. Zayed, and A. El Dessouki, "An adaptive steganogr aphic technique based on integer wavelet transform", International Conference on Networking and Media Convergence. IEEE, pp. 111–117, 2009.

[35] Yu, X., Chen, K., Wang, Y., Li, W., Zhang, W., & Yu, N. ”Robust adapti ve steganography based on generalized dither modulation and expanded embedding domain", Signal Processing, vol.168, 107343, 2020.

[36] P. Sallee, "Model-Based Steganography", In International workshop on digital watermarking, pp. 154–167, 2003.

[37] Miri, A., & Faez, K. "Adaptive image steganography based on transform domain via genetic algorithm", Optik, vol.145, pp.158-168, 2017.

[38] Hameed, M. A., Hassaballah, M., Aly, S., & Awad, A. I, ”An adaptive image steganography method based on histogram of oriented gradient and PVD-LSB techniques", IEEE Access, vol.7, pp.185189-185204.

[39] Thahab, A,”A novel secure video steganography technique using temporal lifted w avelet transform and human vision properties", International Arab Journal Information. Technology, vol.17, no.2, 147-153, 2020.

[40] Kadhim, I. J., Premaratne, P., & Vial, P. J. “High-capacity adaptive image steganography with cover region selection using dual-tree complex wavelet transform”, Cognitive Systems Research, vol.60, 20-32, 2020.

[41] N. Hamid, A. Yahya, R. B. Ahmad, and O. Al-Qershi, “Characteristic region based image steganography using Speeded-Up Robust Features technique”, In 2012 International Conference on Future Communication Networks, pp. 141–146, 2012.

[42] S. Mungmode, R. R. Sedamkar, and N. Kulkarni, “A Modified High Frequency Ad aptive Security Approach using Steganography for Region Selection based on Threshold Value”, Procedia Computer Science, vol. 79, pp. 912–921, 2016.

[43] O. M. Al-Qershi and B. E. Khoo, “Controlling hiding capacity using image characteristics with a 2D-DE data hiding scheme,” AEU-International Journal of Electronics and Communications, vol. 68, no.4, pp. 346–350, 2014.

[44] S. Khan, “Ant colony optimization (ACO) based data hiding in image complex regi on”, International Journal of Electrical and Computer Engineering (IJECE), vol. 8, no.1, pp. 379–389, 2018.

[45] Laishram, D., & Tuithung, T,“ A novel minimal distortion-based edge adaptive im age steganography scheme using local complexity. Multimedia Tools and Applications, vol.80, no.1, pp.831-854, 2021.

[46] Naji, S. A., Mohaisen, H. N., Alsaffar, Q. S., & Jalab, H. A. Automatic region selection method to enhance image-based steganography. Periodicals of Engineering and Natural Sciences (PEN), vol.8, no.1, p.p67-78, 2020.

[47] J. X. Du, D. S. Huang, G. J. Zhang, and Z. F. Wang, “A novel full structure optimiza tion algorithm for radial basis probabilistic neural networks”, Neurocomputing, vol. 70, pp. 592–596, 2006.

[48] D. S. Huang and J. X. Du, “A constructive hybrid structure optimization methodolo gy for radial basis probabilistic neural networks”, IEEE Transactions on neural networks, vol. 19, no.12, pp. 2099–2115, 2008.

[49] W. Wei, J. A. Gulla, and Z. Fu, “Advanced Intelligent Computing Theories and Applications”, springer heidelberg, vol. 621, pp. 490-498, 2010.

[50] V. Pomponiu, D. Cavagnino, and M. Botta, “Data Hiding in the Wild: Where Computational Intelligence Meets Digital Forensics”, In Surveillance in Action, pp. 301-331. 2018.

[51] A. Shahzad, T. Ahmad, and M. N. Doja, “A novel edge based chaotic steganograph y method using neural network”, In proceedings of the 5th international conference on frontiers in intelligent computing: theory and applications, vol. 516, pp. 467–475, 2017.

[52] H. H. Tsai and D. W. Sun, “Color image watermark extraction based on support vec tor machines”, Information Sciences, vol. 177, no.2, pp. 550–569, 2007.

[53] A. Miri and K. Faez, “Adaptive image steganography based on transform domain via genetic algorithm”, Optik (Stuttg)., vol. 145, pp. 158–168, 2017.

[54] S. Uma Maheswari and D. Jude Hemanth, “Performance enhanced image s teganography systems using transforms and optimization techniques”, Multimedia Tools Applications, vol. 76, pp. 415–436, 2017.

[55] R. Tanwar and S. Malhotrab, “Scope of Support Vector Machine in Steganography

", In IOP Conference Series: Materials Science and Engineering, vol. 225, no.1, pp. 012077, 2017.

[56] A. Rai and H. V. Singh, "SVM based robust watermarking for enhanced medical im age security", Multimedia Tools Applications, vol. 76, no.18, pp. 18605–18618, 2017.

[57] C. C. Chang, Y. H. Yu, and Y. C. Hu, "Hiding secret data into an AMBTC-compressed image using genetic Algorithm", In 2008 Second International Conference on Future Generation Communication and Networking Symposia , vol. 3, pp. 154–157, 2008.

[58] C. C. Chang, Y. H. Chen, and C. C. Lin, "A data embedding scheme for color image s based on genetic algorithm and absolute moment block truncation coding," Soft Comp uting, vol. 13, no.4, pp. 321–331, 2009.

[59] H. A. Ghaleb AlJbara, L. B. Mat Kiah, and H. A. Jalab, "Increased capacity of imag e based steganography using artificial neural network" In AIP Conference Proceedings, vol. 1482, pp. 20–25, 2012.

[60] M. Begum and M. S. Uddin, "Digital image watermarking techniques: A review," Information., vol. 11, no.2, 2020.

[61] R. Thanki and A. Kothari, "Multi-level security of medical images based on encryption and watermarking for telemedicine applications," Multimedia. Tools Applications, vol.80, no.3, pp. 4307-4325, 2020.

[62] S. Banerjee, S. Chakraborty, N. Dey, A. Kumar Pal, and R. Ray, "High Payload Wat ermarking using Residue Number System", International Journal of Image, Graphics and Signal Processing, vol. 3, pp. 1–8, 2015.

[63] A. M. S. Kamalraj, G. K. D. P. Venkatesan, and R. V Ravi, "Digital watermarking te chniques for image security : a review", Journal of Ambient Intelligence and Humanized Computing, vol. 11, no.8, pp. 3221–3229, 2020.

[64] A. Anand and A. K. Singh, "Watermarking techniques for medical data authentication : a survey", Multimedia Tools and Applications, vol.80, no.20, pp. 30165-30197, 2020.

[65] K. M. Hosny and M. M. Darwish, "Resilient color image watermarking using accur ate quaternion radial substituted chebyshev moments", ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM) , vol. 15, no.2, pp. 1-25, 2019.

[66] H. Y. Lee, "Adaptive reversible watermarking for authentication and privacy prote ction of medical records", Multimedia Tools Applications, vol. 78, no.14, pp. 19663–19680, 2019.

[67] B. Hassan, R. Ahmed, B. Li, and O. Hassan, "An Imperceptible Medical Image Wat ermarking Framework for Automated Diagnosis of Retinal Pathologies in an eHealth Arr angement", IEEE Access, vol. 7, pp. 69758–69775, 2019.

[68] P. Aparna and P. V. V. Kishore, "Biometricbased efficient medical image watermar king in E-healthcare application," IET Image Processing, vol. 13, no.3, pp. 421–428, 2019.

[69] K. M. Hosny and M. M. Darwish, "Robust color image watermarking using invaria nt quaternion Legendre-Fourier moments," Multimedia Tools Applications, vol.77, no.19, pp. 24727–24750, 2018.

[70] S. A. Parah et al., ”Secure and reversible data hiding scheme for healthcare system using magic rectangle and a new interpolation technique”, In Healthcare Data Analytics and Management, pp. 267-309, 2019.

[71] Shaik, A., & Masilamani, V. ”A novel digital watermarking scheme using dragonfl y optimizer in transform domain”, Computers & Electrical Engineering, vol. 90, pp.106923., 2021.

[72] Hurrah, N. N., Loan, N. A., Parah, S. A., & Sheikh, J. A.,” A transform domain base d robust color image watermarking scheme for single and dual attacks. In Fourth Internat ional Conference on Image Information Processing (ICIIP) (pp. 1-5), 2017.

[73] Kishore, R. R,” A Novel and Efficient Blind Image Watermarking In Transform D omain”, Procedia Computer Science, vol. 167, pp.1505-1514., 2020.

[74] L. Xiaomin and Z. Fengyuan, "Double-color digital image watermarking technolo gy based on double transform domain”, IEEE International Conference on Artificial Intel ligence and Computer Applications (ICAICA), pp. 52-55, 2020.

[75] J. Liu, "An Image Watermarking Algorithm Based on Energy Scheme in the Wavel et Transform Domain”, IEEE 3rd International Conference on Image, Vision and Compu ting (ICIVC), pp. 668-672, 2018.

[76] Garg, P., & Rama Kishore, R.” Secured and multi optimized image watermarking u sing SVD and entropy and prearranged embedding locations in transform domain. Journ al of Discrete Mathematical Sciences and Cryptography, vol.23, no.1, pp.73-82, 2020.

[77] S. Gupta, R. Baraskar, and S. Agrawal, “A survey on Reversible Watermarking Tec hniques for Image Security”, pp. 826–836, 2019.

[78] Utami, N. S., Novamizanti, L., Saidah, S., & Ramatryana, I. N. A, ” SVD on a Robust Medical Image Watermarking based on SURF and DCT”, In IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT), pp. 32-38, 2021.

[79] Liu, X., Sun, Y., Wang, J., Yang, C., Zhang, Y., Wang, L., ... & Fang, H, “ A novel zero-watermarking scheme with enhanced distinguishability and robustness for volumetric medical imaging”, Signal Processing: Image Communication, vol 92, pp.116124, 2021.

[80] Qin, F., Li, J., Li, H., Liu, J., Nawaz, S. A., & Liu, Y, “A robust zero-watermarking algorithm for medical images using curvelet-dct and RSA pseudo-random sequences”, In International Conference on Artificial Intelligence and Security, pp. 179-190, 2020.

[81] Ma, B., Chang, L., Wang, C. et al. “Double Medical Images Zero-Watermarking Algorithm Based on the Chaotic System and Ternary Accurate Polar Complex Exponential Transform”, Journal of Mathematical Imaging and Vision vol .63, no.9, 2021.

[82] Wang, C., Hao, Q., Ma, B., Wu, X., Li, J., Xia, Z., & Gao, H, “Octonion continuous orthogonal moments and their applications in color stereoscopic image reconstruction and zero-watermarking”, Engineering Applications of Artificial Intelligence, vol.106, pp.104450, 2021.

[83] Xia, Z., Wang, X., Wang, C., Ma, B., Wang, M., & Shi, Y. Q, "Local quaternion polar harmonic Fourier moments-based multiple zero-watermarking scheme for color medical images", Knowledge-Based Systems, vol.216, pp.106568.

[84] L. Novamizanti, "A Robust Medical Images Watermarking Using FDCuT-DCT-S VD,", International Journal of Intelligent Engineering and Systems, vol. 13, no.6, 2020.

[85] A. Roček, M. Javorník, K. Slavíček, and O. Dostál, "Zero Watermarking : Critical Analysis of Its Role in Current Medical Imaging," Journal of digital imaging, vol.34, no.1, pp. 204–211, 2021.

[86] Petitcolas FAP, Anderson RJ, Kuhn MG "Information hiding-a survey". Proceedin gs of the IEEE, vol.87, no.7, pp. 1062-1078, 1999.

[87] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI Randomness Tests for Imag e Encryption", Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT) vol.1, no.2, 2011.

[88] P. Selvam, S. Balachandran, S. Pitchai Iyer, and R. Jayabal, "Hybrid transform-bas ed reversible watermarking technique for medical images in telemedicine applications", Optik (Stuttg), vol. 145, pp. 655–671, 2017.

[89] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding - a survey, " Proc. IEEE, vol. 87, pp. 1062–1078, 1999.

[90] Singh AK "Improved Hybrid Algorithm for Robust and Imperceptible Multiple W atermarking using Digital Images", Multimedia Tools Applications, vol. 76, no.6, pp.8881–8900, 2017.

[91] Mathon B, Cayre F, Bas P "Optimal Transport for Secure Spread – SpectrumWatermarking for Still Images", IEEE Transactions on Image Processing, vol. 23, no.4, pp.1694–1705, 2014.

[92] Thakur S, Singh AK, Ghrera SP, Mohan A ," Chaotic based secure watermarking a pproach for medical images". Multimed Tools Applications, vol.79, no.7, 4263-4276, 2020.

[93] Singh D, Singh SK "DWTSVD and DCT based Robust and Blind Watermarking S cheme for Copyright Protection". Multimedia Tools andApplications, vol. 76, no.11, pp.13001–13024, 2017.

[94] Zear A, Singh AK, Kumar P "A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine". Multimedia Tools Applicati ons, vol. 77, no.4, pp.4863–4882, 2018.

[95] Thakkar FN, Srivastava VK " A blind medical image watermarking: DWT-SVD ba sed rob st and sec re approach for telemedicine applications", Multimedia Tools and Applications, vol. 76, no.3, pp.3669–3697, 2017.

[96] Ali M, Ahn CW (2018) An optimal image watermarking approach thro gh c ckoo se arch algorithm in wavelet domain", International Journal of System Assurance Engineering and Management, vol 9, no.3, pp.602–611, 2018.

[97] Kumar C, Singh AK, K mar P "Improved wavelet-based image watermarking thro gh SPIHT", M ltimedia Tools and Applications, vol. 79, no.15, pp.11069-11082.

[98] Zheng Z, Saxena N, Mishra KK, Sangaiah AK, ” G ided Dynamic Particle Swarm Optimization for Optimizing Digital Image Watermarking in Industry Applications”, vol.88, pp.92–106, 2018.

[99] M. Islam, A. Roy, R.H. Laskar, ”Neural network based robust image watermarking techniq e in LWT domain”, Journal of Intelligent & Fuzzy Systems, vol. 34, pp. 1691–1700, 2018.

[100] I. Shafi, M. Noman, M. Gohar, A. Ahmad, M. Khan, S. Din, S.H. Ahmad, J. Ahmad, ”An adaptive hybrid f zzy-wavelet approach for image steganography using bit reduction and pixel adjustment”, Soft Computing, vol. 22, no.5, pp.1555–1567, 2018.

[101] P.D. Shah, R.S. Bichkar, A Sec re Spatial Domain Image Steganography using Genetic Algorithm and Linear Congruential Generator, In International conference on intelligent computing and applications, pp.119-129, 2018.

[102] T. Rabie, I. Kamel, ”High-capacity steganography: a global-adaptive-region discrete cosine transform approach”, Multimedia Tools and Applications, vol. 76, pp. 6473–6493., 2017.

[103] A. Zear, A.K. Singh, P. K mar, Rob st watermarking techniq e sing back propagation ne ral network: a sec rity protection mechanism for social applications, International journal of information and computer security, vol.9, pp. 20–35, 2017.

[104] Emad, E., Safey, A., Refaat, A., Osama, Z., Sayed, E., & Mohamed, E. ”A secure image steganography algorithm based on least significant bit and integer wavelet transform”, Journal of Systems Engineering and Electronics, vol.29, no.3, pp.639–649, 2018.

[105] Sharma, V. K., Srivastava, D. K., & Math r, P. ”Efficient image steganography using graph signal processing”. IET Image Processing, vol.12, no.6, pp.1065–1071, 2018.

[106] Lu, W., He, L., Ye ng, Y., X e, Y., Li , H., & Feng, B, ”Secure binary image steganography based on fused distortion measurement” IEEE Transactions on Circuits and Systems for Video Technology, vol.29, no.11, pp. 3341-3355, 2019.

[107] Savithri, G., Mane, S., & Ban , J. S. “Parallel implementation of RSA 2D-DCT steganography and chaotic 2D-DCT steganography”. In Proceedings of International Conference on Computer Vision and Image Processing, pp. 593-605, 2017.