COMPREHENSIVE SURVEY OF IMAGE WATERMARKING

Vaishali S. Jabade[1] and Sachin R. Gengaje[2]
[1]Department of Electronics Engineering, VIT, Pune University, Pune, India
[2]Department of Electronics Engineering, WIT, Solapur University, Solapur, India

ABSTRACT

Digital image watermarking is receiving widespread attention to protect applications of intellectual property rights. In image watermarking, information is embedded in cover image to prove ownership. This information must remain detectable even if image is manipulated. Applications of digital image watermarking include trusted cameras, journalistic photography, prevention of identity photo forgery, digital rights management systems, e-commerce, e-governance etc. It can also be used commercially for real time services such as broadcast monitoring and security in communication. Authenticating digital images with fair imperceptibility and high detection resolution is the challenge of today's research. Various image watermarking techniques have been proposed in the last few years. The purpose of this paper is to provide a comprehensive review of existing literature available on image watermarking. This paper is organized to discuss steps in image watermarking, its applications, attributes, possible attacks, performance metrics and various methods.

KEYWORDS: *Image Watermarking, Spatial and Transform Domain Watermarking, Watermarking Attacks*

I. INTRODUCTION

The unprecedented growth of digital networks and multimedia applications has resulted in significant growth digital media including images, audio and video. It is impossible to distinguish original from the copy as digital data has no difference in quality between the two. Digital media causes extensive opportunities for piracy of copyrighted material. The means are required to detect copyright violations and control access to these digital media. This has stimulated development of digital watermarking. While Internet has created opportunities for authors, musicians, photographers, artists and software engineers to market their works, it has also made copyright infringement easier than ever before. Image watermarking is one of the aspects of digital watermarking. Due to lack of security, images can be easily duplicated and distributed without owner's consent. Digital image watermarking is modification of the original image data by embedding a watermark containing key information such as authentication or copyright codes. A digital watermark is perceptible or imperceptible identification code that is permanently embedded in host image which uniquely identifies its ownership. The watermark embedded may be pseudo-random sequence, chaotic sequence, spread spectrum sequence or meaningful binary or gray scale image. It can also be used as a way to transport information secretly or to protect integrity of cover image. There is need to develop a method to embed readable watermark such as text or logo in images that can be easily identified upon extraction [1].
This paper is organized to discuss process of image watermarking in section II, its applications in section III, attributes in section IV, classification in section V, possible attacks in section VI, performance parameters in section VII, techniques in section VIII, Computation models in section IX followed by conclusion and future research direction.

II. PROCESS OF IMAGE WATERMARKING

Digital image watermarking process comprises of following 3 stages. Fig.2 describes generic model of watermarking [2-3].

2.1. Generation and Embedding of Watermark

Embedding process is combination of watermark signal and original image. The process is also known as tagging. In embedding phase, embedded data is usually hidden in image referred to as cover-image. This produces stego-image. A key (stego-key) is used to control hiding process, thus restricting detection and recovery of embedded data to parties who know it. This stego-key can be either a public key or a private key depending on scheme of watermarking.

2.2. Transmission and Possible Attacks

The transmission process can be seen as distribution of signal through the watermark channel. Possible attacks in the broadcast channel may be intentional or accidental.

2.3. Extraction and Detection of Watermark

Detection process allows the owner to be identified and provides information to intended recipient**.** In extraction phase, stego-object is used with the key to extract watermark and identifies watermark.

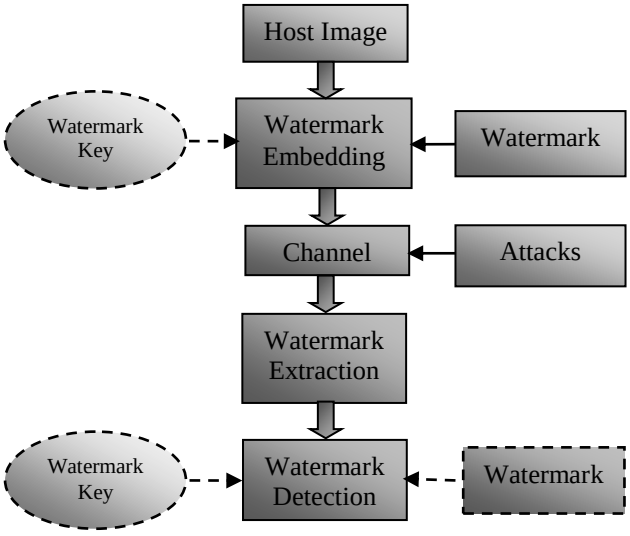

Figure 1. Stages in Image Watermarking

III. APPLICATIONS OF IMAGE WATERMARKING

3.1. Copyright Protection

When a new work is produced, copyright information can be inserted as a watermark. In case of dispute of ownership, watermark can provide evidence. It prevents third parties from claiming ownership. Image watermarking can be used for protecting redistribution of this copyright material over the un-trusted network like Internet or peer-to-peer networks.

3.2. Broadcast Monitoring

This application uses watermark to identify when and where works are broadcast by recognizing watermarks. It can be used to monitor unauthorized broadcast station or works broadcasted by pirate station. This has major application in commercial advertisement broadcasting to monitor whether their advertisement was actually broadcasted at the right time and for right duration.

3.3. Tamper Detection

Digital content can be used for tamper detection by embedding fragile watermarks. If fragile watermark is destroyed or degraded, it indicates presence of tampering and hence the digital content cannot be trusted. Tamper detection is very important for applications involving highly sensitive data like satellite imagery, medical imagery or as a forensic tool.

3.4. Content Authentication and Integrity Verification

Content authentication is able to detect any change in digital content. This can be achieved by using either fragile or semi-fragile watermark which has low robustness for modification. For some works, content is very important and original copy is not available. Under such circumstances, signature information can be embedded and later on checked to verify whether it has been changed or not. It is also used to authenticate snapshots of digital camera so that any changes in still image will be reflected in watermark.

3.5. Fingerprinting

Fingerprints are unique to the owner of digital content. Someone obtains content legally but illegally redistributes it. This can be prevented by tracking the whole transaction by issuing unique watermark to every recipient. Hence a single digital object can have different fingerprints because they belong to different users. Thus, one can tell who did it and when illegal copy appeared.

3.6. Copy and Usage Control

In this application, hardware like recording equipment reads watermark and act accordingly. It is desirable in systems to have copy and usage control mechanism using watermark to prevent illegal copying of the content or limit the number of times it is copied.

3.7. Content Archiving

Watermark can be used to insert digital object identifier or serial number to help archive digital contents. It can also be used for classifying and organizing digital contents. Normally digital contents are identified by their file names. However, this is a very fragile technique as file names can be easily changed. Hence embedding an object identifier within the object itself reduces possibility of tampering.

3.8. Content Description

Watermark can contain some detailed information of the host image such as label and caption. For this kind of application, capacity of the watermarking should be relatively large and there should not be strict requirement for robustness.

3.9. Covert Communication

It includes exchange of messages secretly embedded within images. Hidden data should not raise any suspicion that a secret message is being communicated. The basic requirement for such applications is ability to secretly convey fairly large amount of data [4-5].

IV. ATTRIBUTES OF IMAGE WATERMARKING

The attributes of image watermarking are its characteristics, properties or requirements. Different applications demand different attributes. The following basic attributes need to be considered [6].

4.1 Imperceptibility, Transparency or Fidelity

One of the most important attribute is perceptual transparency of watermark which can also be called as image fidelity. It refers to similarity of the un-watermarked and watermarked works. From this perspective, watermark system exploits limitation of human eyes. Cox et al. define transparency or fidelity as 'perceptual similarity between original and watermarked versions of the cover work'. Watermark should not introduce visible distortions because it reduces commercial value of the image.

4.2 Robustness

Robustness indicates survival of watermark in the image. It is defined as ability to detect watermark after common signal processing operations. Watermark should not be removed intentionally or unintentionally by simple image processing operations or geometric manipulations. Robust watermarks are designed to resist these normal operations. On the other hand, fragile watermarks are designed to detect any attempt by an unauthorized person to change digital contents.

4.3 Capacity or Data Payload

This is the maximum amount of information that can be hidden without degrading image quality. It describes how much data should be embedded as watermark so that it is successfully detected. Watermark should be able to carry enough information to represent uniqueness of an image.

4.4 Security

Secret key can be used for embedding and detection process. Hackers should not be able to remove watermark with anti-reverse engineering research algorithm. There are three types of keys used in image watermarking: private-key, detection-key and public-key. Private-key is available only to author. The public-key can be extracted by other users.

4.5 Computational Complexity

Computational complexity depends on the amount of time needed for execution of watermarking algorithm. More computations ensure security and real time applications need speed and efficiency.

V. CLASSIFICATION OF IMAGE WATERMARKING

Image watermarking techniques can be classified from five perspectives as shown in Fig. 2.

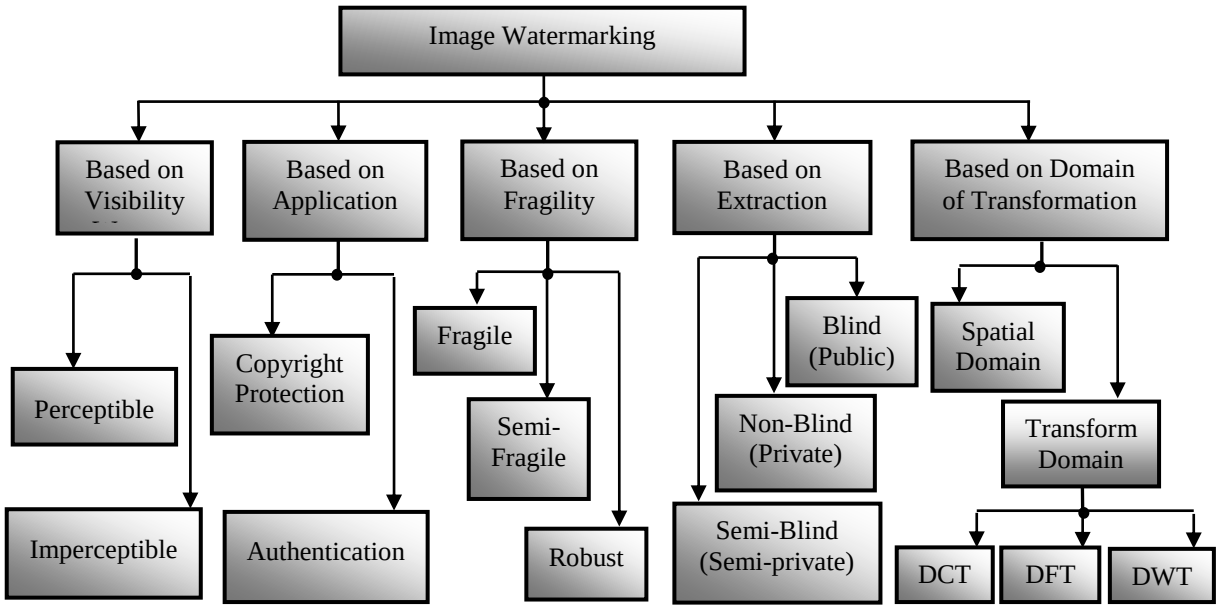

Figure 2. Classification of Image Watermarking

5.1. Based on Visibility

Watermarks may be visible (perceptible) or invisible (imperceptible). A visible watermark is easily detected by observation while an invisible watermark is designed to be transparent to observer and detected using signal processing techniques. Invisible or transparent marks use properties of the human visual system to minimize perceptual distortion in watermarked image.

5.2. Based on Application

The watermarking techniques are classified based on application such as copyright protection or authentication. Copyright protection is useful for ownership verification. Image authentication systems have applicability in law, commerce, defence and journalism. Common examples include marking of images in a database to detect tampering, in commercial applications, so a buyer can be assured that the images bought are authentic upon receipt. Other situations include images used in courtroom evidence or images involved in journalistic photography.

5.3. Based on Fragility (Ability to Resist Attack)

Based on fragility, watermarking schemes are classified as fragile, semi fragile or robust. This classification indicates survival of watermark in watermarked image. A fragile watermark is designed to detect slight changes to watermarked image with high probability. Fragile watermarking is used for content authentication and tamper detection. Semi-fragile watermarking schemes are used to discriminate between malicious manipulations, such as addition or removal of significant element of image and global operations preserving semantic content of the image. Semi-fragile watermark can also serve purpose of quality measurement. Robust watermark indicates survival of watermark in an image in case of image degradation. A robust watermark is designed to resist attacks that attempt to remove or destroy watermark. This is required in copyright protection applications.

5.4. Based on Extraction

Based on extraction method, image watermarking is classified as blind (public or oblivious), semi-blind (semi-private) or non-blind (private or non-oblivious). In blind watermarking, watermark is extracted without original image thus reducing storage requirements. However, this kind of watermarking increases possibility of malicious access. Blind watermarking remains most challenging problem as it does not require either original image or embedded watermark. There is also asymmetric blind watermarking (public key watermarking). It has property that any user can read watermark without being able to remove it. Semi-blind watermarking does not use original image for detection but answers the question in positive or negative form. Non-blind watermarking systems require original image for extraction. This kind of scheme is more robust than others since it requires access to secret material. Non-blind watermarking is suitable for automatic Internet search applications. The host image availability greatly facilitates detection. The original image can be used to register watermarked image in order to compensate for geometric distortions.

5.5. Based on Domain of Transformation

In spatial domain methods, watermark information is embedded directly into image pixels. The images are manipulated by altering one or more number of bits that make up pixels of the image. In frequency domain methods, watermark information is embedded in the transform domain. There is mapping of image to be watermarked into transform domain using either Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT). The other transforms include Arnold Transform, Hadmard Transform, Bandelet Transform etc. Frequency domain watermarking techniques are often used to achieve robustness, imperceptibility and security.

VI. ATTACKS ON WATERMARKED IMAGE

Watermarked image is transmitted through watermark channel. This channel includes possible attacks or distortions on watermarks [16]. It includes signal processing or geometric attacks. These attacks may be intentional (malicious) or un-intentional (accidental). These include cryptanalysis, stega-analysis, image processing techniques or other attempts to remove existing watermarks or confuse the reader challenging authenticity of watermark.

6.1 Signal Processing Attacks

These attacks are also called as Image Processing Attacks or Non geometric Attacks. Some common signal processing attacks include Gaussian noise, salt and paper noise, compression etc.

6.2. Geometric Attacks

Geometric attacks attempt to destroy synchronization of detection. It makes detection process difficult and sometimes even impossible. Geometrical distortions are classified basically into two types. Global geometric attack affects all the pixels of the image in similar manner. Local geometric attack affects different portions of an image in different ways. Geometric attacks include rotation, cropping, scaling, translation etc.

VII. PERFORMANCE PARAMETERS

The performance analysis for watermarked image and extracted watermark is done using different statistical measures. The watermark robustness depends directly on the embedding strength, which in turn influences visual degradation of the image. For benchmarking and performance evaluation, visual degradation due to embedding is important.

7.1. Watermark Imperceptibility Analysis

The imperceptibility of watermarked image is qualitatively decided by visual artefacts in the watermarked image. Different literatures have reported different metrics. As a quantitative measure, following metrics are used. The various notations used are listed below.
$X(i,j)$: Original image,
$X'(i,j)$: Watermarked image, and
Nt : Size of image

7.1.1. Mean Square Error (MSE)

Mean Square Error between original image and watermarked image is calculated as follows:

$$MSE = \frac{1}{Nt}\sum_{i,j}(X(i,j) - X'(i,j))^2 \quad (1)$$

7.1.2. Normalized Mean Square Error (NMSE)

Mean square error is normalized by original image energy and is calculated as follows:

$$NMSE = \frac{\sum_{i,j}(X(i,j) - X'(i,j))^2}{(X(i,j))^2} \quad (2)$$

7.1.3. Peak Signal to Noise Ratio (PSNR)

Peak signal to noise ratio is an image quality metric and is defined in decibels as follows:

$$\mathrm{PSNR(dB)} = \mathrm{l0log}_{10}\frac{255 \times 255}{\mathrm{MSE}} \quad (3)$$

PSNR is calculated between the original and watermarked image. It is measured in units of dB. The larger the PSNR value, more similar is the watermarked image to original image. If the PSNR value is greater than 30dB then the perceptual quality is acceptable, i.e. watermark is almost invisible to human eyes.

7.1.4. Image Fidelity (IF)

Image fidelity is a measure of imperceptibility or transparency of watermarked image and is calculated as follows:

$$IF = 1 - \frac{\sum_{i,j}(X(i,j) - X'(i,j))^2}{\sum_{i,j}(X(i,j))^2} \quad (4)$$

7.2. Watermark Robustness Analysis

The robustness of watermarked image is qualitatively decided by visual artefacts in the extracted watermark in case of visually meaningful logo watermark. As a qualitative analysis, extracted and embedded watermark images or text logos can be compared visually. As a quantitative measure, following metrics are used in case of logo or binary sequence watermark. These indicate reliability and readability of extracted watermark. The notations used are listed below.
$W(i,j)$: Original Watermark and
$W'(i,j)$: Extracted Watermark

7.2.1. Correlation Coefficient (CRC)

This metric is used to analyze compatibility of original watermark and extracted watermark. The value ranges from 0 to 1. CRC is calculated as follows:

$$CRC = \frac{\sum_i \sum_j W(i,j)W'(i,j)}{\sqrt{\sum_i \sum_j W(i,j)^2 \times \sum_i \sum_j W(i,j)^2}} \quad (5)$$

7.2.2. Similarity Measure (SIM)

A similarity measure also called as similarity coefficient (SC) between the extracted watermark and embedded watermark is used for objective judgment of the extraction fidelity. This parameter is used to quantify the difference between original and extracted watermark. The metric is compared with predefined threshold to decide whether watermark signal exists or not. It is used to judge the existence of watermark and is defined as

$$SIM(W,W') = \frac{\sum_i \sum_j W(i,j)W'(i,j)}{\sum_i \sum_j W'(i,j)^2} \quad (6)$$

7.2.3. Distortion Ratio (DR)

To obtain a quantitative measure of the distortion, the distortion ratio between the extracted watermark and original watermark is defined as

$$DR = \frac{\sum_i \sum_j |W'(i,j) - W(i,j)|}{N_t} \times 100\% \quad (7)$$

The minimum value of DR indicates reliable extraction of watermark.

7.2.4. Accuracy Ratio (AR)

It is used to evaluate similarity between the original watermark and extracted one. It is defined as ratio of number of correct bits between original watermark and extracted watermark and number of original watermark bits and is given by following equation.

$$AR = \frac{CB}{NB} \quad (8)$$

Where,
CB =No. of correct bits & NB =Total no. of bits
AR value closer to 1 indicates more similarity between original watermark and extracted watermark.

VIII. TECHNIQUES OF IMAGE WATERMARKING

8.1 Spatial Domain

Spatial domain watermarking techniques modify the intensity or gray levels of original image. The earlier work of digital image watermarking schemes embed watermark in least significant bits (LSB) of the pixels. Pixels of image are represented by an 8-bit sequence. Watermark is embedded in the last (i.e., least significant) bit, of selected pixels of the image. This kind of watermarking is simple and has less computing complexity, because no transform of original image is required. However, there must be trade-off between imperceptibility and robustness.
These techniques are easier to implement and does not generate serious distortions in the image. However, these techniques are not very robust against attacks. For instance, an attacker could simply randomize all LSBs which effectively destroy the hidden information. Also, these techniques suffer from low information hiding capacity [7].

8.2 Transform Domain

Transform domain schemes involve insertion of watermark in the transform coefficients unlike spatial domain watermarking. This approach shows better robustness and hiding capacity for watermarking. In transform domain watermarking, watermark is inserted into transform coefficients of image. This approach is more robust as embedded information can be spread out over entire image.

8.2.1 Discrete Fourier Transform (DFT)

DFT domain has been explored by researches because it offers robustness against geometric attacks. There are two different kinds of DFT based watermark embedding techniques. One in which watermark is directly embedded and another which is template based embedding. In direct embedding watermark is embedded by modifying phase information in DFT. A template is a structure which is embedded in DFT domain to estimate transformation factor. Once the image undergoes a transformation this template is searched to resynchronize image, and then use detector to extract embedded watermark. Wei Wang Aidong and Men Xiaobo Chen present robust digital image watermarking scheme based on phase features in DFT domain and generalized Radon transformations. The scheme selects phase information in DFT domain as feature of image, and uses generalized Radon transformations to indentify geometric transformations. Kang Xiao and Jun Dong present watermarking algorithm based on image segmentation and DFT, in order to improve security and robustness against some attacks [8-10].

8.2.2 Discrete Cosine Transform (DCT)

I.J. Cox et al. proposed a secure and robust watermark for multimedia. Based on hyper-chaos and DCT algorithm, combined with the Arnold scrambling method, a novel digital image watermarking algorithm is presented. Based on HVS, original image is split into blocks and encrypted watermark is embedded into low frequency coefficients with different strength. A. Piva et al. developed a DCT-Based watermark recovering without restoring to the uncorrupted original image and Chien Chang Chen et al. developed a DCT based reversible image watermarking approach that works on quantized DCT coefficients. Chip-Hong Chang et al. describe a DCT transform domain digital watermarking scheme that uses visually meaningful binary watermark. The method embeds watermark adaptively with localized embedding strength according to noise sensitivity level of host image. Fuzzy adaptive resonance theory (Fuzzy-ART) classification is used to identify appropriate locations for watermark insertion [11].

8.2.3 Discrete Wavelet Transform (DWT)

Wavelet transform is a mathematical tool for hierarchically decomposing an image. Wavelets allow image to be described in terms of a coarse overall shape and details that range from broad to narrow because of multi-resolution approach. Single stage decomposition divides an image into four sub-bands, a lower resolution approximation image (LL) a horizontal (HL), a vertical (LH) and a diagonal (HH) detail bands. This is achieved by using a pair of high pass and low pass filters. Each of these filters decomposes image into several frequencies. The process can then be repeated to compute multiple scale wavelet decompositions. Watermark is embedded in different frequency DWT components of sub-bands. Wavelets reflect anisotropic properties of HVS more precisely as compared to FFT or DCT. This allows higher energy watermarks in regions where HVS is less sensitive. Embedding watermark in these regions allow us to increase robustness of watermark, without much degradation of image quality. Another advantage is that image compression standard JPEG 2000 is uses wavelet transform. Victor et al. have developed an algorithm that relies upon adaptive image watermarking in high resolution sub-bands of DWT. Zhao Dawei et al. suggested a chaos-based robust wavelet-domain watermarking algorithm. N. Kaewkamnerd and K.R. Rao developed wavelet based image adaptive watermarking scheme. The embedding is performed in higher level sub-bands of wavelet transform, even though this can clearly change image fidelity. In order to avoid perceptual degradation of image, watermark insertion should be carefully performed while using HVS. Literature has reported use of various wavelet filters like Haar Wavelet, Daubechies wavelet, orthogonal wavelet, bi-orthogonal wavelet, balanced multi-wavelet, hyperbolic wavelet, fractional wavelet and wavelet packets to transform the image [12-18].

IX. COMPUTATIONAL MODELS OF IMAGE WATERMARKING

In recent years, watermarking techniques are being improved using computational models. This includes following models discussed.

9.1 Singular Value Decomposition (SVD)

SVD is one of the most powerful numerical analysis tools used to analyze matrices. In SVD transformation, a matrix can be decomposed into three matrices that are of the same size as original matrix. SVD transformation preserves both one-way and non-symmetric properties, usually not obtainable in DCT and DFT transformations. Using SVD in digital image processing has advantages like the size of matrices from SVD transformation is not fixed and can be a square or a rectangle. Singular values in a digital image are less affected if general image processing is performed and singular values contain intrinsic algebraic image properties. The singular values of the host image are modified to embed the watermark image by employing multiple singular functions [19-22].

9.2 Independent Component Analysis (ICA)

Independent component analysis is recently developed technique. ICA is applied to compute some statistically independent transform coefficients where watermark is embedded. The main advantage of this approach is that each user can define its own ICA-based transformation. These transformations behave as private-keys. On the other hand, some of these transform coefficients have white noise-like spectral properties. An orthogonal watermark is developed to blindly detect it with a simple matched filter. ICA consists of projecting a set of components onto another statistically independent set. These approaches assume a multiple-input multiple-output model and have been successfully applied to image watermarking. When applied to watermarking, ICA presumes the watermarked image as a mixture of original image and watermark. The mixture image can be separated to estimate this watermark [23-24].

9.3 Artificial Neural Network (ANN)

An artificial neural network (ANN), usually called neural network, is a mathematical model or computational model that is inspired by the structural and functional aspects of biological neural networks. A neural network consists of an interconnected group of artificial neurons, and it processes information using a connectionist approach to computation. In most cases ANN is an adaptive system that changes its structure based on external or internal information that flows through the network during learning phase. Modern neural networks are non-linear statistical data modelling tools. They are usually used to model complex relationships between inputs and outputs or to find patterns in data. Chuan-Yu Chang introduced copyright authentication for images with a full counter-propagation neural network (FCNN). Most attacks do not degrade the quality of detected watermark image as FCNN has storage and fault tolerance. Chen Yongqiang devised an optimal image watermarking algorithm using synergetic neural network. Quan Liu et.al. designed and realized meaningful digital watermarking algorithm based on Radial Basis Function neural network. It is used to simulate human visual system to determine watermark embedding intensity [25-26].

9.4 Support Vector Machine (SVM)

SVM is a novel machine learning method. SVM-based classifier is built to minimize structural misclassification risk, whereas conventional classification techniques often apply minimization of empirical risk. SVM based classification is better because its efficiency does not directly depend on dimension of classified entities. It is a technique for universal data classification. In recent years, SVMs have been used for digital watermarking. The idea of SVM is to construct a mapping model from input data to output data which are also defined as features for input data and targets for output data. There are two data sets in classification as training data and testing data. Each training data contains several features and one target [27- 28].

9.5 Genetic Algorithm (GA)

Genetic algorithm belonging to class of evolutionary algorithms is a search heuristic used to generate useful solutions to optimization and search problems. It generates solutions to optimization problems

using techniques inspired by natural evolution, such as inheritance, mutation, selection, and crossover. In genetic algorithm, population of strings encode candidate solutions to an optimization problem. The evolution usually starts from a population of randomly generated individuals and happens in generations. In each generation, the fitness of every individual in the population is evaluated, multiple individuals are stochastically selected from the current population (based on their fitness) and modified (recombined and possibly randomly mutated) to form a new population. The new population is then used in next iteration of algorithm. Algorithm terminates when either a maximum number of generations has been produced or a satisfactory fitness level has been reached for population. In case of watermarking, singular values of host image are modified by multiple scaling factors to embed watermark in an image. Modifications are optimised to obtain highest possible robustness without losing transparency [29-30].

9.6 Fuzzy Logic (FL)

Fuzzy logic is a multi-valued logic which relates to classes of objects with un-sharp boundaries in which membership is a matter of degree. The basic concept underlying fuzzy logic is that variable values are words or linguistic variables, rather than numbers. Although words are inherently less precise than numbers, their use is closer to human intuition. Computing with words exploits tolerance for imprecision and thereby lowers cost of solution. Thus it is a form of logic in which predicates can have fractional values. Lou and Yin suggsted an adaptive digital watermarking using fuzzy clustering technique. The watermark is adaptively embedded in significant DWT coefficients that are selected in higher level sub bands. Nizar Sakr et. al. used dynamic fuzzy logic approach to adaptive HVS based watermarking. Santi P. Maity and Seba Maity developed a multistage spread spectrum watermark detection technique using fuzzy logic. Ming Shing Hsieh developed image watermarking based on fuzzy inference filter [31-32].

X. CONCLUSION

Image watermarking is a challenging field that involves principles and techniques from a range of diverse disciplines like signal processing, image processing, steganography and encryption. Research in image watermarking is progressing very fast. Various researchers from different fields are focusing on development of robust watermarking scheme. Many new research directions arise in image watermarking methods and the area is still in its stages of development. In this paper, we have been concerned with description and categorization of all possible watermarking application scenarios. A comprehensive survey of significant methods for watermarking has been presented. The aim of this overview is to assist budding researchers in the field of digital image watermarking to understand existing methods and to aid their research further.

XI. FUTURE RESEARCH DIRECTION

It is envisioned to develop effective watermarking technique by using multiple watermarks, combination of pseudo random binary sequence, barcode and logo watermarks. The protection can be enhanced by incorporating biometric data such as fingerprint, iris, audio clip or any such other human identity. The watermarking techniques further can be extended for 3-D images and multimedia data. It will find effective applications in distance learning, digital libraries, digital TVs, e-commerce and e-governance.

REFERENCES

[1]. Thi Hoang Ngan Le, Kim Hung Nguyen, Hoai Bac Le, "Literature Survey on Image Watermarking Tools, Watermark Attacks, and Benchmarking Tools", *Second IEEE International Conferences on Advances in Multimedia, 2010,*pp.67-73.

[2]. Vidyasagar M. Potdar, Song Han, Elizabeth Chang, "A Survey of Digital Image Watermarking Techniques", *3rd IEEE International Conference on Industrial Informatics (INDIN), 20*05, pp.709-713.

[3]. M.F. Fahmy and G. Fahmy, "A Quasi Blind Watermark Extraction of watermarked Natural Preserve Transform Images", *IEEE Ineternational Conference on Image Processing*,2009, pp.3665-3668.

[4]. Dr. M.A. Dorairangaswamy, B. Padmavathi, "An Effective Blind Watermarking Scheme for Protecting Rightful Ownership of Digital Images", *IEEE, TENCON*, 2009, pp. 1-6.

[5]. Jun Sang and Mohammad S. Alam, "Fragility and Robustness of Binary-Phase-Only-Filter-Based Fragile/Semi fragile Digital Image Watermarking," *IEEE Transactions on Instrumentation And Measurement, Vol. 57, No. 3, March 2008,* pp.595-606.

[6]. Dong Zheng, Sha Wang, and Jiying Zhao, "RST Invariant Image Watermarking Algorithm With Mathematical Modeling and Analysis of the Watermarking Processes," IEEE *Transactions on Image Processing, Vol. 18, No. 5, May 2009,* pp.1055-1068.

[7]. K.Aboutammam, A. Tamtaoui & D. Aboutajdine, "A New Spatial Decomposition Scheme For Image Content-Based Watermarking" *IEEE, 2009* pp.539-542.

[8]. Wei Wang Aidong Men Xiaobo Chen, "Robust Image Watermarking Scheme Based on Phase Features in DFT Domain and Generalized Radon Transformations", *2nd IEEE International Congress on Image and Signal Processing CISP '09*, 2009, pp.1-5.

[9]. Kang Xiao and Jun Dong Li Jun, "A Digital Watermarking Algorithm Based on Image Segmentation and DFT",*1st IEEE International Conference on Information Science and Engineering,* 2009, pp.1511-1514.

[10]. Xiao Jun Kang Li Jun Dong, "Study of the Robustness of Watermarking Based on Image Segmentation and DFT", *IEEE International Conference on Information Engineering and Computer Science, ICIECS,* 2009, pp1-4.

[11]. Liu Yuejun, "Research on Information Hiding System based on DCT Domain", *Second IEEE International Conference on Computer Modeling and Simulation,* 2010, pp.11- 14.

[12]. Ming-Xiang Zang, Na Zang, Jian-guo Jiang, "An Adaptive Digital Watermarking Algorithm Based on Balanced Multi-wavelet", *Fifth international Conference on Information Assuirance and Security,* 2009, pp. 243-246.

[13]. Yuanhai Shao, Wei Chen, Chan Liu,"Multiwavelet-based Digital Watermarking with Support Vector Machinr Technique", *IEEE Conference CCDC,*2008, pp.4557-4561.

[14]. Yusnita Yusof, Othman O. Khalifa, "Imperceptibility and Robustness Analysis of DWT based Digital Image Watermarking", *Proceedings of the International Conference on Computer and Communication Engineering,*2008, pp. 1325-1330.

[15]. Zhao Dawei, Chen Guanrong, Liu Wenbo, "A Chaos-based Robust Wavelet-domain Watermarking Algorithm", *IEEE International Conference on Multimedia and Expo (ICME),* 2004.

[16]. Miang Zuang Zang, Na Zang and Jian Guo Jiang, "An Adaptive Digital Watermarking Algorithm Based on Balanced Multi-wavelet", *Proceedings, Fifth IEEE International Conference on Information Assurance ans Security,*2009, pp. 243-246.

[17]. Daxing Zhang, Zhigeng Pan and Haihua Li, "A Contour-based Semi-fragile Image Watermarking Algorithm in DWT Domain", *Second IEEE International Workshop on Education Technology and Computer Science,* 2010, pp. 228-231.

[18]. Lin Zhuang "Multipurpose Digital Watermarking Algorithm Based on Morphological Wavelet Transform", *IEEE International Conference on Communications and Mobile Computing,* 2009, pp. 396-400.

[19]. B.Jagadeesh, S.Srinivas Kumar, K.Raja Rajeswari, "Image Watermarking Scheme Using Singular Value Decomposition, Quantization and Genetic Algorithm", *IEEE International Conference on Signal Acquisition and Processing, 2010,*pp 120-124.

[20]. Feng Wen-ge, Liu Lei, "SVD and DWT Zero-bit Watermarking Algorithm", *2nd IEEE International Asia Conference on Informatics in Control, Automation and Robotics,* 2010, pp. 361-364.

[21]. Vijay R Ayangar, S. N. Talbar, "A Novel DWT-SVD Based Watermarking Scheme", MCIT, 2010, pp. 105-108.

[22]. Chin-Chen Chang a, Piyu Tsai b, Chia-Chen Lin, "SVD-based Digital Image Watermarking scheme", *Pattern Recognition Letters 26, Elsevier, 2005,* pp.1577–1586.

[23]. Shao-min Zhu, Jian-ming Liu, "Adaptive Image Watermarking Scheme in Contourlet Transform Using Singular Value Decomposition", *IEEE, ICACT 2009,*pp. 1216-1219.

[24]. Thang Viet Nguyen, Jagdish Chandra Patra, "A simple ICA-based digital image watermarking scheme", *Elsevier Digital Signal Processing 18, 2008,* pp. 762–776

[25]. Song Huang, Wei Zhang, " Digital Watermarking Based on Neural Network and Image Features" *Second IEEE International Conference on Information and Computing Science, 2009*,pp.238-240.

[26]. Quan Liu, Xuemei Jiang, "Design and Realization of a Meaningful Digital Watermarking Algorithm Based on RBF Neural Network" *IEEE, 2005* pp. 214-218.

[27]. Xiang-Yang Wang Hong-Ying Yang, Chang-Ying Cui, "An SVM-based robust digital image watermarking against desynchronization attacks", *Elsevier Signal Processing 88,2008,*pp. 2193– 2205.

[28]. Yuanhai Shao, wei Chen, Chan Liu, "Multiwavelet based Digital Watermarking with Support Vector Machine Technique", *IEEE, 2008*, pp. 4557-4561.

[29]. Changjiang Zhang and Min Hu, "Curvelet Image Watermarking Using Genetic Algorithms", *IEEE Congress on Image and Signal Processing, 2008,*pp. 486-490.

[30]. Chen Yongqiang, Peng Lihua, "Optimal Image Watermark Using Genetic Algorithm and Synergetic Neural Network," *Second IEEE International Conference on Intelligent Computation Teclmology and Automation, 2009,* pp. 209-212.

[31]. Chip Hong Chang and Mingyan Zhang, "Fuzzy-Art based adaptive digital watermarking scheme", *IEEE Transactions on Circuits and Systems for Video Technology, Vol. 15 no. 1,* 2005, pp. 65-81.

[32]. Ming-shing Hsieh, "Image Watermarking based on Fuzzy Inference Filter", *IEEE Proceedings of the International Conference on Machine Learning and Cybernetics, Baoding,* 2009, pp.3058-3063.

AUTHORS

Vaishali S. Jabade is presently Assistant Professor in Electronics Engineering Department at Vishwakarma Institute of Technology, Pune, India. She completed master's degree in Electronics Engineering from University of Pune. She has been Branch Counsellor for IEEE Student Chapter, VIT, Pune. She has also worked as secretary of Indian Society for Technical Education, VIT, Pune, Chapter. Her research interests include Image steganography and image watermarking.

Sachin R. Gengaje is Professor and Head of Electronics Engineering Department in Walchand Institute of Technology, Solapur, India. He is a Senate Member, Solapur University, Research & Review committee member and Chairman Board of Studies, Electronics engineering, Solapur University. His research interest includes image processing, artificial neural network and fuzzy logic. Several research publications are to his credit. He has more than twenty years of teaching experience