Literature Review on Multiple Watermarking for Images using Optimization Techniques

N. Mohananthini1*, G. Yamuna2, C. Ananth1, M. Karthikeyan3

Assistant Professor, Department of Electrical and Electronics Engineering, Muthayammal Engineering College, Tamilnadu, India1
Professor, Department of Electrical Engineering, Annamalai University, Tamilnadu, India2
Assistant Professor/Programmer, Annamalai University, Tamilnadu, India3,4

ABSTRACT: Multiple watermarks is to convey multiple sets of information, proposed to suit similar or differing objectives and also used to increase robustness with many different methods. This paper elaborates suitability of different transform based multiple watermarking techniques such as successive, segmented and composite watermarking. It also provides a comprehensive review of the existing literature available on image watermarking methods using optimization techniques.

KEYWORDS: Composite Watermarking, Multiple Watermarking, Optimization, Segmented Watermarking, Successive Watermarking.

I. INTRODUCTION

The recent advancements in digital information have made subtle changes in our society and life. The advantages of digital information also produced new challenges and opportunities. Innovations, supported with powerful software, new devices such as digital camera, camcorder and digital voice recorder, have reached the consumers, worldwide, use manipulate and experience the pleasure in the multimedia data. Internet and wireless communication networks give ubiquitous channels to send and exchange information.

Watermarks are identifying marks produced during the handmade paper making process and the watermarks first appeared in Fabriano (Italy) during the 13th century. In 1992, Andrew Tirkel and Charles Osborne first coined the term of digital watermark. Digital Watermarking is one of the important techniques in the area of information security. The information is embedded into cover image [1].

The medical safety application of the multiple watermarking techniques ensures that each doctor inserts his diagnosis in the medical image without degrading it. With any new diagnosis insertion, the image must always keep its clarity and its characteristics.

This paper is organized as follows; the overviews on watermarking techniques are discussed in section 2. The multiple watermarking techniques are discussed in section 3. The different attacks are discussed in section 4. The optimization techniques are discussed in section 5. Finally, the discussions and conclusion are given in section 6 and 7.

II. OVERVIEWS ON WATERMARKING

Watermarking has become an active and important area of research, development and commercialization of watermarking techniques is being deemed essential to help address some of the challenges faced by the rapid proliferation of digital content. The overview on watermarking is discussed as follows,

2.1. Types of Watermarking

According to the type of multimedia object, the watermarking techniques can be divided into four categories such as text, image, audio and video watermarking, but most of the time watermarking is applied to still images.
Text Watermarking: The process of embedding or hiding data in text can be termed as text watermarking. Ding Huang et al. [2] proposed a new approach in text watermarking where interword spaces of different text lines are slightly modified. Their experiments suggest space patterning of text documents can be a useful tool in digital watermarking.

Image Watermarking: The process of embedding or hiding information in image can be termed as image watermarking. Robust image watermarking algorithm using wavelet transform is presented in [3]. The performance of their proposed watermarking algorithm is robust to a variety of attacks.

Audio Watermarking: The process of embedding information into audio can be termed as audio watermarking. The audio watermarking along with its important properties is explained in [4]. Their also brings to view works done by various technique on digital audio watermarking.

Video Watermarking: The process of embedding information into video can be termed as video watermarking. Hamid Shojanazeri et al. [5] presented the state of the art in video watermarking techniques and provided a critical review on various available techniques. It addresses their main key performance indicators which include robustness, speed, capacity, fidelity, imperceptibility and computational complexity.

2.2. Watermark Types

Pseudo Random Number Sequence: Pseudo Random Number (PRN) sequence is generated by feeding the generator with a secret seed and the detector to check the presence or absence of watermark. Kesidis et al. [6] presented that embeds the watermark message in randomly chosen coefficients along a ring in the frequency domain using non maximal pseudorandom sequences. Experimental results show that their method is robust to a variety of image processing operations and geometric transformations.

Visual Watermark: The visual watermark is actually reconstructed and its visual quality is evaluated. A primary watermark in the form of a PN sequence is first embedded into an image (the secondary watermark) before being embedded into the host image. Two visual watermarks are embedded in the DWT domain through modification of both low and high frequency coefficients are explained in [7].

2.3. Watermarking Perception

Based on human perception, digital watermarks can be divided into visible and invisible perception.

Visible Watermark: In visible watermark the watermark appears, information is visible to a viewer in video or picture only on careful inspection [8]. For example a television channels, like BBC, whose logo is visibly superimposed on the corner of TV.

Invisible Watermark: The invisible watermark is completely imperceptible. The invisible-robust watermark is embedded in such a way that alterations made to the pixel value are perceptually not noticeable and can be recovered only with the appropriate decoding mechanism [9]. The invisible-fragile watermark is embedded in such a way that any manipulation or modification of the image would alter or destroy the watermark.

Dual Watermark: The dual watermark is a combination of a visible and an invisible watermark [10]. Their work first insert the visual watermark in the original image and then an invisible watermark is added to the already visual watermarked image. The final watermarked image is the dual watermarked image.

2.4. Watermarking Domains

Watermarks can be embedded either in the spatial or the transform domain as discussed below.

Spatial Domain: The spatial-domain techniques directly modify the intensity values of some selected pixels. A new spatial domain probability based watermarking scheme for color Images is proposed in [11]. Their method proved to be robust to various image processing operations.

Transform Domain: The watermarking scheme based on the transform domains can be further classified into the Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) domain methods.
Discrete Fourier Transform: The discrete Fourier transform (DFT) converts a finite list of equally spaced samples of a function into the list of coefficients of a finite combination of complex sinusoids, ordered by their frequencies, that has those same sample values. Solachidis et al. [12] presented an algorithm for rotation and scale invariant watermarking of digital images. Their experimental results are robust to compression, filtering, cropping, translation and rotation.

Discrete Cosine Transform: A discrete cosine transform (DCT) expresses a finite sequence of data points in terms of a sum of cosine functions oscillating at different frequencies. A spread-spectrum-like discrete cosine transform domain watermarking technique for copyright protection of still digital images is analyzed in [13]. The DCT is applied in blocks of 8 × 8 pixels as in the JPEG algorithm.

Discrete Wavelet Transform: The wavelet transform is based on small waves. The heart of wavelet analysis is multi-resolution analysis. In two-dimensional DWT, each level of decomposition produces four bands of data, one corresponding to the low pass band (LL), and three other corresponding to horizontal (HL), vertical (LH), and diagonal (HH) sub-bands. A DWT based image watermarking technique is proposed in [14]. Simulation results vividly illustrated that their proposed technique performed well in terms of robustness against attacks and imperceptibility.

Hybrid Domain: The Hybrid domain technique is intermediate between spatial and transform domain, it is a combination of both spatial and frequency domain. Dharm Singh et al. [15] studied watermarking based scheme on Least Significant Bit (LSB) and the DCT under spatial and frequency domain. Their experimental results demonstrated the improved performance of the DCT in terms of imperceptibility and robustness as compared to the LSB domain.

2.5 Watermarking Techniques

Watermarking techniques can be classified in several ways. According to the need of the original image for watermark extraction or detection, watermarking is classified to blind, non-blind and semi-blind watermarking.

Blind Watermarking: In blind watermarking need only the secret key for extraction. The blind watermarking is more insecure than non-blind techniques. Blind watermarking is referred as public watermarking. Sahraee et al. [16] proposed a robust blind watermarking algorithm based on quantization of distance among wavelet coefficients for copyright protection. Experimental results show that their proposed method is quite robust against attacks.

Non-Blind Watermarking: In non-blind watermarking require the original image and secret key for watermark detection process. Non-blind watermarking is referred as private watermarking. DWT-SVD based non-blind watermarking scheme for color images in RGB space is proposed in [17]. The combinations of DWT and SVD increase the security, robustness and imperceptibility of their scheme.

Semi-Blind Watermarking: Finally semi-blind watermarking require the secret key and watermark bit sequence for extraction process. Semi-blind watermarking is referred as semi-private watermarking. C-C-Chang et al. [18] proposed a robust semi-blind watermarking scheme based on DWT to hide a gray scale watermark in a digital image for image authentication. Their proposed scheme is robust to various attacks.

2.6 Watermarking Embedding Methods

Embedding method is an important one in a watermarking scheme. The different embedding methods are additive, multiplicative, hybrid and quantization watermarking. Most of the early watermarking techniques were based on an additive embedding method.

Additive Watermarking: In additive watermarking, the watermark is multiplied with a global embedding strength and added to the wavelet image coefficients. Mairgiotis et al. [19] proposed a new family of watermark detectors for additive watermarks in digital images. These detectors are based on a recently proposed 2 image model, which was found to be beneficial for image recovery problems. Their numerical experiments demonstrate that these new detectors can lead to superior performance to several state-of-the-art detectors. The additive embedding equation is given by

\[ I_w(i,j) = I(i,j) + \alpha \times W(i,j) \]  

(1)

Where, \( I_w \) = watermarked image, \( W \) = watermark, \( I \) = cover Image and \( \alpha \) = scaling factor

The additive extraction equation is given by
Multiplicative Watermarking: More current watermarking techniques apply a multiplicative embedding method. In multiplicative watermarking, the watermark embedded into the wavelet coefficients are locally modulated proportional to the strength of the coefficients. Antonis Mairgiotis et al. [20] proposed the application of a hierarchical prior for the multiplicative image watermarking problem. Their method investigated the detector’s performance compared with known state of the art methods and the robustness of the proposed detectors against watermark attacks. The multiplicative embedding equation is given by

\[ W(i, j) = I_w(i, j) - I(i, j) \]

Multiplicative extraction equation is given by

\[ W(i, j) = I_w(i, j) - I(i, j) \]

Hybrid Watermarking: In hybrid watermarking, combine the additive and multiplicative watermark embedding methods. Seigo Ikeda et al. [21] presented a hybrid method of two basic embedding schemes, additive and multiplicative schemes, which embeds a watermark by both rules so that the degradation of image quality caused by one embedding is decreased by the other. They experimentally confirmed that the optimum detection scheme for the proposed hybrid scheme shows a better performance than both additive and multiplicative ones in the DWT domain.

The hybrid embedding equation is given by

\[ I_w(i, j) = I(i, j) + (\alpha \times W(i, j)) \]

Here \( \beta \) is watermark strength to improve the correlation of watermark extraction. The hybrid extraction equation is given by

\[ W(i, j) = I_w(i, j) - I(i, j) \]

2.7. Watermarking properties

The digital watermarking properties [23] are discussed bellow.

**Effectiveness:** When input to a detector results in a positive detection. With this definition of watermarked Works, the effectiveness of a watermarking system is the probability that the output of the embedder will be watermarked. In other words, the effectiveness is the probability of detection immediately after embedding.

**Fidelity:** The fidelity of a watermarking system refers to the perceptual similarity between the original and watermarked versions of the cover Work. The fidelity of a watermarking system as the perceptual similarity between the unwatermarked and watermarked Works at the point at which they are presented to a consumer.

**Data Payload:** Data payload refers to the number of bits a watermark encodes within a unit of time or within a Work. For a photograph, the data payload would refer to the number of bits encoded within the image. A watermark that encodes N bits is referred to as an N-bit watermark. Such a system can be used to embed any one of 2^N different messages. Different applications may require very different data payloads.

**Robustness:** Robustness refers to the ability to detect the watermark after common signal processing operations. Not all watermarking applications require robustness to all possible signal processing operations. Rather, a watermark need only survive the common signal processing operations likely to occur between the time of embedding and the time of detection.

**Security:** The security of a watermark refers to its ability to resist hostile attacks. A hostile attack is any process specifically intended to thwart the watermark’s purpose.
Cost: The two principal issues of concern are the speed with which embedding and detection must be performed and the number of embedders and detectors that must be deployed. Other issues include whether the detectors and embedders are to be implemented as special-purpose hardware devices or as software applications or plugins.

III. MULTIPLE WATERMARKING TECHNIQUES

In multiple watermarking techniques multiple watermarks are embedded into the original image. The works in the literature related to multiple image watermarking techniques are discussed below.

A wavelet-based watermarking scheme to embed multiple watermarks in medical images is proposed in [25]. Their scheme offers medical confidentiality and record integrity, the quality of watermarked images to achieve higher PSNR values. A wavelet based watermarking algorithm the watermarks are embedded in different sub-bands with variable scaling factor [26]. The scaling factor is high for the LL sub-band and it is low for other three sub-bands. A multiple watermarking technique by adopting integer wavelet transform is presented in [27]. Their method is robust to a wide variety of attacks. Maha Sharkas et al. [28] tested a novel image watermarking technique in the wavelet domain. Their method achieves more security and robustness. A multiple watermarking techniques for color images in spatial domain are proposed in [29]. A novel multiple watermarking algorithm which embedded two watermarks into original image is modelled in different frequency by using bandelet transform is proposed in [29]. Their watermarking algorithm has a good performance in invisibility and robustness. An image watermarking technique is proposed in [31], to embed multiple binary watermarks into original images based on the concept of Visual Cryptography.

Vijendra Rai et al. [32] presented a multiple image watermarking based on dither quantization. Their algorithm is superior in terms of embedding capacity and attacks. A multiple robust digital watermarking system for still images is proposed in [33]. Their method shows the results are resistant to different types of attacks. A review of multiple watermarking for text documents is presented [34]. Their multiple watermarking approach increases the security and robustness.

The multiple watermarking techniques are discussed as follows,

3.1. Successive watermarking

In successive watermarking technique, the multiple watermarks are embedded one after the other, from the watermarked images the multiple watermarks are extracted from one after other. This approach is also called Re-watermarking technique. The three main categories of multiple watermarking techniques are distinguished in [35]. The use of classical single watermarking scheme in a multiple re-watermarking scenario is discussed in [36]. Comparison of blind and non-blind algorithms is focused in their method.

3.2. Segmented watermarking

In segmented watermarking technique, the original image is separated into different segments and each watermark is embedded into its specific share. Wheeler et al. [37] proposed weighted segmented watermarking of still images in which segments are formed by dividing the image into square blocks, each of which contains one contributor’s watermark. Nantha Priya et al. [38] proposed the segmented image is modeled as mixture generalized Gaussian distribution and their model is the basis of mathematical analysis of various aspects of the watermarking process such as probability of error and embedding strength adjustment.

3.3. Composite watermarking

In composite watermarking, multiple watermarks are combined into a single watermark which is subsequently embedded in one single embedding step. Mina Deng et al [39] proposed a buyer seller watermarking protocol based on composite signal representation in the encrypted domain. Their proposed composite embedding can be performed in the encrypted domain by simply using an additively homomorphic cryptosystem.
IV. ATTACKS

To prove the robustness the images are tested for selected attacks. Attacks on watermark need to identify weakness, propose improvement and study effects of current technology on watermark. The four classes of attacks are removal attacks, geometric attacks, cryptographic and protocol attacks [40, 41]. The removal attacks intend to remove the watermark data from the watermarked object. Such attacks exploit the fact that the watermark is usually an additive noise signal present in the host signal. The interference attacks are those which add additional noise to the watermarked object (including lossy compression, collusion, denoising, quantization, remodulation and averaging). The geometric attacks are specific to images and videos [42]. The geometric attacks do not actually remove the watermark, but manipulate the watermarked object in such a way that the detector cannot find the watermark data (include rotation, translation, scaling, Warping, line/column removal and cropping) [43]. The removal and geometric attacks do not breach the security of the watermarking algorithm, but the cryptographic attacks deal with the cracking of the security. The protocol attacks exploit the loopholes in the watermarking concept. A fake original object is created that produces the same results through the detector as that of real original object. Review of image watermarking against attacks is presented below.

Gui Xie et al. [44] designed a novel wavelet-based watermarking scheme resilient to geometrical attacks using a rotation-invariant log-polar mapping to eliminate all the effects of the geometrical operations in the input image before computing its discrete wavelet transform. Experimental results demonstrate the advantages of their scheme, particularly its robustness against geometrical attacks. The families of watermark attacks (geometric, signal processing attacks) are studied in [45]. Martin Kutter et al. [46] proposed a new attack for digitally watermarked images. Their experiments showed that the attack is very effective in copying a watermark from one image to a different image.

V. OPTIMIZATION TECHNIQUES

The optimization techniques are to maximize the performance of imperceptibility and robustness. Optimization is to make as perfect, effective and functional as possible. The optimization technically use of systems as fully as possible within the parameters. The optimization techniques are neural network, fuzzy systems, genetic algorithm and particle swarm optimization.

5.1. Neural Network

An artificial neural network is a mathematical function conceived as a simple model of a biological neural network. The function is determined by network structure, connection strengths, and the processing performed at computing elements or nodes. The basic elements in neural networks are weights, thresholds and activation function. The learning methods in neural networks are classified into three basic types such as supervised learning, unsupervised learning and reinforced learning. The Neural Network Architecture is connection between the neurons such as single layer feed-forward, multi layer feed-forward, fully recurrent network, competitive network, Jordan network, simple recurrent network.

Review of image watermarking based on neural network is presented below.

An efficient blind digital watermarking algorithm based on neural networks in the wavelet domain is presented in [47]. The experimental results proved the validity of their approach. Qianhui Yi et al. [48] proposed a novel digital watermarking scheme improved back propagation neural network for colour image. The results demonstrated that their algorithm has good visual effect and high robustness. A new digital watermarking algorithm based on BPN neural network is proposed in [49]. The neural network processing the learning capability from given trained patterns; their method can recover the watermark from watermarked image. The results show that their watermarking algorithm has a good prefference.

Fan Zhang et al. [50] presented a blind watermarking algorithm using Hopfield neural network and analyze watermarking capacity based on neural network. Their results show that the attraction basin of associative memory decides watermarking capacity. A robust image adaptive watermarking scheme has been presented in [51]. Their scheme is enhanced with the aid of MLF neural networks. Their experimental results show that the neural networks can satisfactorily maximizing the watermark strength with properly trainings, which is adaptive based on the knowledge of the local block features.
5.2. Fuzzy systems

Fuzzy systems include fuzzy logic and fuzzy set theory. The fuzzy logic is the logic underlying approximate, modes of reasoning as an extension of multi valued logic including truth, is a matter of degree. The fuzzy sets have been introduced in 1965 by Lotfi A. Zadeh as an extension of the classical notion of set. The fuzzy system elements are fuzzification, fuzzy rule base, membership function, fuzzy inferencing and defuzzification.

Review of image watermarking based on fuzzy systems is presented below.

In [52], a fuzzy logic approach is introduced to embed the encrypted watermark in the wavelet domain. Their fuzzy logic approach is used to estimate the optimal gain with a proper scaling factor, the watermark is imperceptible. Nizar Sakr et al [53] proposed adaptive wavelet based watermarking algorithm based on the model of HVS and fuzzy inference system. Their proposed algorithm computed the watermark weighting function that enables the maximum energy and imperceptible watermark. Ming-Shing Hsieh [54] proposed a wavelet based watermarking approach for embedding visually recognizable watermark in images. Their method deals with a fuzzy inference filter to choose the larger entropy of coefficients to embed watermark. Their watermarking approach is very robust to image compression and image operations. Ming-Shing Hsieh et al. [55] proposed a novel subband image coder with fuzzy inference filter and adaptive quantization. Their approach can achieve an excellent performance on the combination application of image compression and watermarking.

5.3. Genetic algorithm

The Genetic Algorithm (GA) was introduced in the mid 1970s by John Holland. Genetic algorithms are a technique to solve problems which need optimization. Genetic algorithms are a subclass of evolutionary computing and random search algorithms. Genetic algorithms are based on Darwin’s theory of evolution. The genetic algorithm is a probabilistic search algorithm that iteratively transforms a set (called a population) of mathematical, each with an associated fitness value, into a new population of offspring objects using the Darwinian principle of natural selection and using operations that are patterned after naturally occurring genetic operations, such as crossover and mutation.

Evaluate the fitness function is based on the peak signal to noise ratio and normalized correlation as follows,

\[ \text{Fitness Function} = \text{PSNR} + 100 \times \text{NC} \]

\[ \text{Fitness Function} = \text{NC} + 100 \times \text{PSNR} \]

Review of image watermarking based on genetic algorithm is presented below.

A modified image watermarking scheme based on singular value decomposition, edge detection and genetic algorithm is proposed in [56]. Their method based on quantization step size optimization using the genetic algorithm to improve the quality of watermarked image and robustness of the watermark. Cauvery [57] demonstrated the utility of genetic algorithm in the area of improving the fidelity and robustness of digital watermarking. A novel DWT domain gray image watermarking scheme using genetic algorithm is proposed in [58]. The experimental results prove their method is feasibility and validity. Sachin Goyal et al [59] proposed the conceptual background of technique based on genetic algorithm. Their method helps to optimize the fidelity and robustness of watermarking.

VI. DISCUSSION

Most watermarking techniques support single watermark embedding, but there are great limitations when single watermarking techniques are tried into practical applications in few rare situation, like when multiple users share the copyright, it is need to support multiple users to embed their watermarks synchronously. This highlights the need for multiple watermarking. Based on this review multiple watermarks are embedded into the image to achieve security, Imperceptibility, embedding capacity and robustness to large range of image processing operations in various methods.
VII. CONCLUSION

The various researchers from different fields are focusing multiple watermarking techniques to develop imperceptibility and robust watermarking. This paper emphasizes multiple watermarking for various domains, techniques, application and analysis for the various attacks. The review of optimization technique in image watermarking algorithm are also discussed which will be useful for the researchers to implement effective multiple image watermarking techniques.

REFERENCES


