International Journal of Research

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 08 Issue 01
January 2021

A Watermarking Technique for Biomedical Images using SMQT, OTSU And Fuzzy C-Means

J.Anoohya[1], A.Sreevani[2], Dr. S.A. Sivakumar[3]
[1]P.G. Scholar, [2]Guide, Assisant Professor, [3]Head of the Department(ECE)
[1,2,3] Branch : Digital electronics and communication systems (DECS) department of Electronics and communication engineering (ECE)
[1,2,3] Dr.K.V. Subba Reddy College of engineering for women
Email: [1]jarubandeeanoohya487@gmail.com, [2]sreevanireddy.alluru@gmail.com

Abstract:
Digital watermarking is a process of giving security from unauthorized use. To protect the data from any kind of misuse while transferring, digital watermarking is the most popular authentication technique. This paper proposes a novel digital watermarking scheme for biomedical images. In the model, initially, the image is segmented using Fuzzy c-means. Afterwards, the watermark is embedded in the image using discrete wavelet transform (DWT) and inverse DWT (IDWT). Finally, the watermark is extracted from the biomedical image by executing the inverse operation of the embedding process. The main focus of this thesis is to provide good tradeoff between perceptual quality of the watermarked image and its robustness against different attacks. For this purpose, we have discussed two robust digital watermarking techniques in discrete wavelet (DWT) domain. One is fusion based watermarking, and other is spread spectrum based watermarking. Simulation results of various attacks are also presented to demonstrate the robustness of both the algorithms while maintaining robustness against different attacks by demonstrating a lower bit error rate (BER), and peak signal-to-noise ratio (PSNR).

Keywords: Digital watermarking; Biomedical image; Successive mean quantization transform; Fuzzy c-means cluster; confidentiality; robustness; imperceptibility

Introduction

The ongoing advances in technology and computer networks have drawn a significant change in the biomedical sector. Currently, multimedia data are treated as a source for transmitting biomedical information such as patients' reports, hospital information, diagnoses, and so on. This transition encompasses patients, doctors, hospitals, and clinic centers [1]. Among the various types of multimedia data, biomedical images have an immense usage in the biomedical zone. Due to the easy use of the multimedia data, the biomedical images can be easily manipulated during transmission. This initiates huge security issues such as copyright and authentication because the biomedical data are highly confidential. The digital watermarking technique has captured great attention for restricting various illegal hazards and ensuring security. Biometric fingerprints and signatures have been used as the watermarks [2,3]. Due to the sophistication of the medical images, digital watermarking has become more challenging. Although many research works focused on digital watermarking of medical images, there is no single model that adheres to all the security and privacy requirements. Therefore, it is crucial to develop watermarking models to fulfill all the required specifications.

Digital watermarking is a technique of inserting any kind of additional data into the source image. The additional data is known as the watermark. The key feature of watermarking is information hiding. Embedding sensitive data in the images facilitates data hiding and ensures maximum privacy. Watermarking medical images has two goals:

i. Controlling reliability and authentication.
ii. Hiding sensitive information of the patient.

In this paper, an image watermarking model for protecting biomedical images is proposed. A watermark is embedded into the image using discrete wavelet transform (DWT) and extracted using inverse DWT (IDWT). The image security is ensured by comparing the original watermark before embedding and the extracted watermark after transmission. The existence of these watermarks with in a multimedia signal goes unnoticed except when passed through an appropriate detector. Common types of signals to watermark are still images, audio, and digital video. As an example of the usefulness of watermarking, let us consider a simple scenario: Newspaper X publishes a photograph, for which it claims exclusive rights. Newspaper Y, also claiming to be the exclusive owner, publishes the same photograph after copying it from X. Without any special protection mechanism, X cannot prove that it is the rightful owner of the photograph. However, if X watermarks the photograph before publication (that is, X embeds a hidden message that identifies it as its legitimate owner), and is able to detect the watermark later in the illegally distributed copy, it will be able to supply proof of ownership in a court of law. On the other hand, to prevent detection of the watermark, Y may try to remove it from the picture by distorting the picture. That is, Y may attempt to attack the watermark so as to render it undetectable, without significantly degrading the quality of the image or affecting its commercial value. Careful design of the watermarking system can prevent this from happening.

Problem Statement

In general, the classification of an image's pixel belonging to one of the "objects" (i.e., classes) composing the image is based on some common feature(s), or resemblance to some pattern. In order to determine which are the features that can lead to a successful classification, some apriori knowledge or/and assumptions about the image are equally required. Classical, so-called "crisp" image clustering techniques, while effective for images containing well-defined structures such as edges, do not perform well in the presence of ill-defined data. In such circumstances, the processing of images that posses ambiguity is better performed using fuzzy clustering techniques, which are more adept at dealing with imprecise data. Fuzzy techniques may be broadly classified into five main categories:

1. Fuzzy clustering based image clustering
2. Fuzzy rule based image clustering
3. Fuzzy geometry based image clustering
4. Fuzzy thresholding based image clustering
5. Fuzzy integral based clustering techniques (Tizhoosh,1998).

Of all these methods mentioned, the most widely used are the fuzzy rule based and fuzzy clustering based clustering. The problem with fuzzy rule based image clustering techniques is that they are application dependent with the structure of the membership functions being predefined and in certain cases, the corresponding parameters being manually determined. Karmakar et al. [76] presented a contemporary review of fuzzy rule based image clustering techniques, and confirmed that despite being used in a wide range of applications, both the

structure of membership functions and derivation of their relevant parameters were still very much application domain and image dependent. Fuzzy c-means is an unsupervised technique that has been successfully applied to feature analysis, clustering, and classifier designs in fields such as astronomy, geology, medical imaging, target recognition, and image clustering [38],[39],[42],[43]. An image can be represented in various feature spaces, and the FCM algorithm classifies the image by grouping similar data points in the feature space into clusters. This clustering is achieved by iteratively minimizing a cost function that is dependent on the distance of the pixels to the cluster centers in the feature domain. Unfortunately, the greatest shortcoming of FCM is its over-sensitivity to noise, which is also a flaw of many other intensity based clustering methods. In recent years, many modification of the FCM algorithm have been reported to overcome the effect of noise. Most of these methods inevitably introduce computation issues. In almost all methods proposed recently, the objective function of the FCM is changed. As most equations are modified along with the modification of the objective function, these methods lose continuity from FCM, which is well-realized with many types of software, such as MATLAB.

Existing System

Fusion-Based Watermarking

We address the problem of embedding binary images, gray images robustly within the host signal. The method transforms both the host image and watermark into the discrete wavelet domain where their coefficients are fused according to a series combination rule that take into account contrast sensitivity characteristics of the HVS [36]. The watermark is restricted to be much smaller in dimension than the host signal. No randomly generated keys are required for security, but the host image is necessary for watermark extraction. The method repeatedly merges the watermark coefficients at the various resolution levels of the host signal which provides simultaneous spatial localization and frequency spread of the watermark to provide robustness against widely varying signal distortions including cropping and filtering. The watermarking process is adaptive and depends on the local host image characteristics at each resolution level. Moreover, the watermark is resilient to attack since it is embedded strongly in more salient components of the image.

We develop our approach to fulfill the following requirements of a successful robust watermarking scheme:

1. The data hiding technique is adaptive and takes into account the natural masking characteristics of the host signal to more strongly, and hence, reliably embed the watermark.
2. The embedded watermark is robust to a reasonable level of signal distortion. Since the host signal is available for watermark extraction, it is exploited to characterize any attacks.
3. The algorithm is portable to different applications and can hide different types of information robustly within a host signal.

Research into human perceptions indicates that the retina of the eye splits an image into several components which circulates from the eye to the cortex in differently tuned channels (frequency bands). These channels can only be excited by the component of a signal with similar characteristics. The processing of signals in different channels is independent. Studies have shown that each of these channels have a bandwidth of approximately one octave [33]. Similarly, in a multi-resolution decomposition, the image is separated into bands of approximately equal bandwidth on a logarithmic scale. It is therefore expected that use of the discrete wavelet transform will allow the independent processing of the resulting components

without significant perceptible interaction with them. For this reason, wavelet decomposition is attractive for the fusion of images. Image fusion refers to the processing and synergistic combinations of images from various knowledge sources and sensors to provide an overall result which contains the most relevant characteristics of its components. Since the process of image fusion is essentially a sensor-compressed information problem (i.e., it involves the combining of one or more images into a single fused result), it follows that wavelets are also useful for such merging. Some multi-resolution wavelet fusion methods make use of information about the HVS to determine the perceptually most significant information from each image to retain the composite [34]. It is then expected that such rules can be used to judiciously select the regions of the host image in which to embed the watermark.

The technique is comprised of the 3 main stages is summarized in Figure 1. First, the image and watermark both are decomposed using the DWT. In the second stage, the watermark is selectively and repeatedly merged using a model of human contrast sensitivity to determine the most salient localized host image components. Last, the inverse DWT is applied to form the watermarked image. The following is the more detailed and analytic description of the procedure.

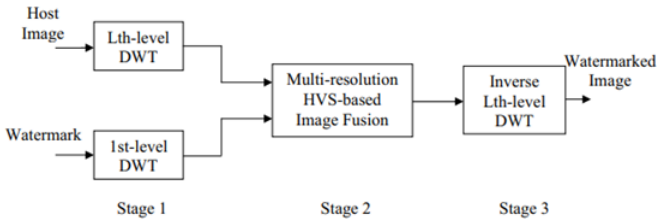

Figure 3.1: The Fusion-Based Watermark Embedding Method

Algorithm

Throughout our discussion, we use X (m,n) to denote the host image and) w(m,n the watermark. The watermark, assumed to be a two dimensional array of real elements. The watermark is visually recognizable binary or gray scale image. The size of the watermark is N×N. It is required that the size of the watermark in relation to the host image be "small". We assume, without loss of generality, that the watermark is smaller than the host by a factor of 2^M, where M is an integer greater or equal to 1.

Proposed System

Digital Watermarking

In this thesis, work has been carried out on digital watermarking. Throughout the rest of the report, watermarking refers to digital watermarking. To avoid the unauthorized distribution of images or other multimedia property, various solutions has been proposed. Most of them make unobservable modifications to images that can be detected afterwards. Such image changes are called watermarks. Watermarking is defined as adding (embedding) a watermark signal to the host signal. The watermark can be detected or extracted later to make an assertion about the object. A general scheme for digital watermarking is given in Figure 2. The watermark message can be a logo picture, sometimes a visually recognizable binary picture or it can be binary bit stream. A watermark is embedded to the host data by using a secret key at the embedder.

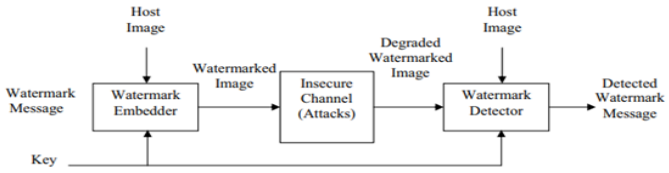

Fig. 2 A Digital Watermarking System

The information embedding routine imposes small signal changes, determined by the key and watermark, to generate the watermarked signal. Only the owner of the data knows the key and it is not possible to remove the message from the data without the knowledge of the key. Then, the watermarked image passes through the transmission channel. The transmission channel includes the possible attacks, such as lossy compression, geometric distortions, any common signal processing operation and digital-analog and analog to digital conversion, etc. After the watermarked image passes through these possible operations, the message is tried to be extracted at the watermark detector. The decoding process can itself performed in two different ways. In one process the presence of the original unwatermarked data is required and other blind decoding is possible. The extracted watermark is compared with the original watermark (i.e. the watermark that was initially embedded) by a comparator function and binary output decision is generated. The comparator is basically a correlator.

ALGORITHM

Watermark Embedding Method: The watermark embedding technique is comprised of the 3 main stage discussed below. First, the image is decomposed using the DWT. In the second stage, the watermark bits are adaptively embedded through a PN-sequence using a model of human contrast sensitivity. Last, the inverse DWT is applied to form the watermarked image. The following is the more detailed and analytic description of the procedure.

Stage 1:

The host image is transformed into the wavelet domain. We perform the 1st-level discrete wavelet decomposition of the original image, and we got 3 detail images, corresponding to the horizontal, vertical, diagonal details, and 1 gross approximation image. We denote the th k detail image component of the host by $X_{k,1}$ (m,n) , where k = 3,2,1 represents the frequency orientation corresponding to the horizontal, vertical and diagonal image details, and 1 represents the first resolution level and (m,n) particular pair spatial location index. The gross approximation is represented by $X_{4,1}$(m,n) where the subscript "4" is used instead of k to denote the gross approximation image. In order to avoid serious image degradation and survive lossy compression, we will embed the watermark in the middle frequency band that is $X_{1,1}$ (m,n) and $X_{2,1}$ (m,n). We split $X_{1,1}$ (m,n) and $X_{2,1}$ (m,n) sub-band into non-overlapping 8×8 blocks respectively, suppose that the original image is of M × M , then $X_{1,1}$ (m,n) and $X_{2,1}$ (m,n) will be of size M/2 × M/2 . After splitting there will be M/16 × M/16 blocks respectively in $X_{1,1}$ (m,n) and $X_{2,1}$ (m,n) sub-band.

The watermark image is converted into an array of bits. If the watermark is 32×32, the number of bits is 1024. The number of watermark bits used should be less than total number of blocks in $X_{1,1}$ (m,n) and $X_{2,1}$ (m,n) sub-band.

Stage 2:

The salience S (which is a numerical measure of perceptual importance) of each of these localized segments is computed using information about the contrast sensitivity characteristics of the IDWT. The value of the salience determines the strength of the

watermark to embed in the particular 8 8× coefficient image block. Mathematically, contrast sensitivity is defined as the reciprocal of the contrast necessary for a given spatial frequency to be perceived. Again for convenience the resulting contrast sensitivity for a particular pair of spatial frequencies is given by:

$$C(u,v) = 5.05e^{-0.178(u+v)}(e^{0.1(u+v)} - 1)$$

where C(u, v) is the contrast sensitivity matrix and u and v are the spatial frequencies. The salience of each block is defined as:

$$S(X^i_{k,1}(m,n)) = \sum C(u,v)\left|F_{k,1}(u,v)\right|^2$$

In order to keep secret of watermark embedding position, we generate pseudo random number to be used as the allocation of the watermarking position of the blocks in $X_{1,1}$ (m,n) and $X_{2,1}$ (m,n) sub-band. In generating the pseudo random number, a 'key' is used as a seed number. To fit the random number to the number of blocks in $X_{1,1}$ (m,n) and $X_{2,1}$ (m,n), it is scaled to the block numbers in $X_{1,1}$ (m,n) and $X_{2,1}$ (m,n) sub-band. Watermark is embedded in chosen blocks in $X_{1,1}$ (m,n) and $X_{2,1}$ (m,n) only. We use another different key to generate an 8 x 8 random sequence having distribution of N (0,1) to embed a watermark bit in each chosen block. The same watermark bit is embedded in the chosen blocks, which have the same location in $X_{1,1}$ (m,n) and $X_{2,1}$ (m,n) sub-band. Watermark bit embedding procedure can be represented as follows:

$$\beta^i_{k,1} = \sqrt{\frac{S(X^i_{k,l}(m,n))}{\max S(X^i_{k,l}(m,n))}}$$

If *watermark bit=1*

$$X^{w,ci}_{k,l}(m,n) = X^{ci}_{k,l}(m,n) + \alpha^{ci}_{k,l}\beta^{ci}_{k,l}PN\_one(m,n)$$

else

$$X^{w,ci}_{k,l}(m,n) = X^{ci}_{k,l}(m,n) - \alpha^{ci}_{k,l}\beta^{ci}_{k,l}PN\_one(m,n)$$

Stage 3: Perform one-level IDWT to obtain watermarked image.

Watermark Extracting Method:

The extraction process of watermark is rather similar to the embedding process, first we compute DWT of the watermarked image and spilt $X_{1,1}$ (m,n) and $X_{2,1}$ (m,n) sub-band into nonoverlapping 8 x 8 blocks and then use the same key to generate the same random number by which to find the watermark embedding position, and also use the same key to generate random sequence which have the distribution of N(0,1). Then we compute the correlation between PN_one and the coefficients of selected block that embed the same watermark bit both in $X_{1,1}$ (m,n) and $X_{2,1}$ (m,n) sub-band and calculate the average correlation. Watermark bit value can be decided as follows:

If correlation > 0

Watermark bit =1 else

Watermark bit =0

Watermark extraction is oblivious (blind), with no reference to the original image and thus is more practical than non-oblivious one. The normalized correlation coefficient r was used to measure the robustness of the extracted watermark against different attacks.

Secure Watermarking: In this case, mainly dealing with copyright protection, ownership verification or any other security-oriented application, the watermark must survive both no-malicious as well as malicious manipulations. In secure watermarking, the loss of the hidden data should be obtainable only at the expense of a significant degradation of the quality of the

host signal. When considering malicious manipulation it has to be assumed that attackers known the watermarking algorithm and thereby they can conceive ad-hoc watermark removal strategies. The security must lie on the choice of key. The watermarking algorithm has truly secure if knowing the exact algorithms for embedding and extracting the watermark does not help unauthorized party to detect the presence of the watermark. As to non- malicious manipulations, they include a huge variety of digital and analog processing tools, including lossy compression, linear and non-linear filtering, cropping editing, scaling, D/A and A/D conversions, analog duplications, noise addition, and many others that apply only to particular type. Thus in the image case, we must considering zooming and shrinking, rotation, contrast, enhancement histogram manipulation, row/ column removal or exchange, in the case of video we must taken into account frame removal, frame exchange, temporal filtering, temporal re-sampling, finally robustness of an audio watermark, may imply robustness against echo addition, multi-rate processing, and pitch scaling. It is though important to point out that even the most secure system does not need to perfect the contrary, it is only needed that a high enough degree of security is reached. In other words, watermark breaking does not need to be impossible (which probably will never be the case), but only difficult enough.

Robust watermarking:

In this case it is required that the watermark be resistant only against non-malicious manipulations. Robust watermarking is less demanding than secure watermarking. Application fields in robust watermarking include all the situations in which it is unlikely that someone purposely manipulates the host data with the intention to remove the watermark. The application scenario is such that the normal use of data comprise of several kinds of manipulations, which must not damage the hidden data. Even in copyright protection applications, the adoption of robust watermarking instead of secure watermarking may be allowed due to the use of a copyright protection protocol in which all the involved actors are not interested in removing the watermark.

Capacity

The capacity requirement of the watermarking scheme refers to be able to verify and distinguish between different watermarks with a low probability of error as the number of differently watermarked versions of an image increases [7]. The requirements listed above are all related to each other. The mutual dependencies between the basic requirements are shown in Fig. 3. For instance, a very robust watermark can

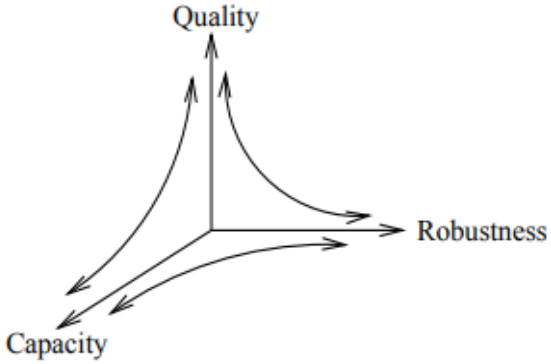

Fig. 3 Mutual dependencies between the basic requirements

be obtained by making many large modifications to the host data for each bit of the watermark. Large modifications in the host data will be noticeable, however, and many modifications per watermark bit will limit the maximum amount of watermark bits that can be stored in a data object. The robustness of the watermarking method increases, the capacity also increases where the imperceptibility decreases. The security of a watermark influences

the robustness enormously. If a watermark is not secure, it cannot be a very robust. Hence, a tradeoff should be considered between the different requirements so that an optimal watermark for each application can be developed.

WATERMARKING ATTACKS AND PERFORMANCE MEASUREMENTS

To win each campaign, a general needs to know about both his opponents as well as his own troops. Attacks aim at weakening the watermarking algorithm. The purpose of any watermark embedding algorithm is to provide some degree of security and the purpose of any attack is to negate that purpose. Hence the compilation of a report on watermarking is incomplete without a mention of watermarking attacks. Study of watermarking algorithm enable to:

- Identify weakness of the watermarking algorithm
- Propose improvement of the watermarking algorithm
- Study effects of current technology on watermark

In watermarking terminology, an attack is any processing that may impair detection of the watermark or communication of the information conveyed by the watermark. The processed watermarked data is then called attacked data. Watermarking is treated as a communication problem, in which the owner attempts to communicate over a hostile channel, where the non-intentional and the intentional attacks from the channel. The owner tries to communicate as much watermark information as possible while maintaining a sufficient high data quality, contrary, and an attacker tries to impair watermark communication while impairing the data quality as little as possible. Therefore, digital watermarking scenarios can be considered as a game between the owner and attacker. Continuing with the analogy of watermarking as a communication system, some researchers have chosen to work on modeling and resisting attacks on the watermark. They work on the philosophy that the more specific the information known about the possible attacks, the better we can design systems to resist it.

CLASSIFICATION OF ATTACKS

Attacks can be broadly classified as non-malicious (unintentional) such as compression of a legally obtained, watermarked image or video files and malicious such as an attempt by a multimedia pirate to destroy the embedded information and prevent tracing of illegal copies of watermarked digital video. Watermarking systems utilized in copy protection or data authentication schemes are especially susceptible to malicious attacks. Non-malicious attacks usually come from common signal processing operations done by legitimate users of the watermarked materials.

Malicious attacks

An attack is said to be malicious if its main goal is to remove or make the watermark unrecoverable. Malicious attacks can be further classified into two different classes. Blind: A malicious attack is said to be blind if it tries to remove or make the watermark unrecoverable without exploiting knowledge of the particular algorithm that was used for watermarking the asset. For example, copy attack that estimates the watermark signal with aim of adding it to another asset. Informed: A malicious attack is said to be informed if it attempts to remove or make the watermark unrecoverable by exploiting knowledge of the particular algorithm that was used for watermarking the asset. Such an attack first extracts some secrete information about the algorithm from publicly available data and then based on this information nullifies the effectiveness of the watermarking system. Examples of malicious attacks:

- Printing and Rescanning
- Watermarking of watermarked image (re-watermarking)

- Collusion: A number of authorized recipients of the image should not be able to come together (collude) and like the differently watermarked copies to generate an unwatermarked copy of the image (by averaging all the watermarked images).
- Forgery: A number of authorized recipients of the image should not be able to collude to form a copy of watermarked image with the valid embedded watermark of a person not in the group with an intention of framing a 3rd party.
- IBM attack [9]: It should not be possible to produce a fake original that also performs as well as the original and also results in the extraction of the watermark as claimed by the holder of the fake original.

Non-Malicious attacks

An attack is said to be non-malicious if it results from the normal operations that watermarked data or any data for that matter has to undergoes, like storage, transmission or fruition. The nature and strength of these attacks are strongly dependent on the application for which the watermarking system is devised.

Examples of non-malicious attacks:

- Lossy Compression: This is generally an unintentional attack which appears very often in multimedia applications. Practically all the audio, video and images that are currently being distributed via Internet have been compressed. If the watermark is required to resist different levels of compression, it is usually advisable to perform the watermark insertion task in the same domain where the compression takes place. Many compression schemes like JPEG and MPEG can potentially degrade the data's quality through irretrievable loss of data.
- Geometric Distortions: Geometric distortions are specific to images videos and include such operations as rotation, translation, scaling and cropping.
- Common Signal Processing Operations: Common signal processing operation includes such operations such as linear filtering such as high pass and low pass filtering, non linear filtering such as median filtering, D/A Conversion, A/D conversion, re-sampling, requantization, dithering distortion, addition of a constant offset to the pixel values, addition of Gaussian and Non Gaussian noise, local exchange of pixels.

The existing attacks can be categorized into four classes of attacks [10]: removal attacks, geometric attacks, cryptographic attacks, and protocol attacks.

Removal attacks

Removal attacks aim at the complete removal of the watermark information from the watermarked data without cracking the security of the watermarking algorithm, e.g., without the key used for watermark embedding. That is, no processing, even prohibitively complex, can recover the watermark information from the attacked data. This category includes denoising, quantization (e.g., for compression), re-modulation, and collusion attacks. Not all of these methods always come close to their goal of complete watermark removal, but they may nevertheless damage the watermark information significantly. Sophisticated removal attacks try to optimize operations like de-noising or quantization to impair the embedded watermark as much as possible while keeping the quality of the attacked document high enough. Usually, statistical models for the watermark and the original data are exploited within the optimization process. Collusion attacks are applicable when many copies of a given data set, each signed with a key or different watermark, can be obtained by an attacker or a group of attackers. In such a case, a successful attack can be achieved by averaging all

copies or taking only small parts from each different copy. Recent results show that a small number of different copies, e.g., about 10, in the hand of one attacker can lead to successful watermark removal.

Geometric attacks

In contrast to removal attacks, geometric attacks do not actually remove the embedded watermark itself, but intend to distort the watermark detector synchronization with the embedded information. The detector could recover the embedded watermark information when perfect synchronization is regained. However, the complexity of the required synchronization process might be too great to be practical. For image watermarking, the most known benchmarking tools, Unzign and Stirmark, integrate a variety of geometric attacks. Unzign introduces local pixel jittering and is very efficient in attacking spatial domain watermarking schemes. Stirmark introduces both global and local geometric distortions. We give a few more details about these attacks later in this paper. However, most recent watermarking methods survive these attacks due to the use of special synchronization techniques. Robustness to global geometric distortions often relies on the use of either a transform invariant domain (Fourier-Melline) or an additional template or of specially designed periodic watermarks whose auto-covariance function (ACF) allows estimation of the geometric distortions. However, as will be discussed below, the attacker can design dedicated attacks exploiting knowledge of the synchronization scheme. Robustness to global affine transformations is more or less a solved issue. However, resistance to the local random alterations integrated in Stirmark still remains an open problem for most commercial watermarking tools. The so-called random bending attack in Stirmark exploits the fact that the human visual system is not sensitive against local shifts and affine modifications. Therefore, pixels are locally shifted, scaled, and rotated without significant visual distortion. However, it is worth noting that some recent methods are able to resist against this attack.

Cryptographic attacks

Cryptographic attacks aim at cracking the security methods in watermarking schemes and thus finding a way to remove the embedded watermark information or to embed misleading watermarks. One such technique is the brute-force search for the embedded secret information. Another attack in this category is the so-called Oracle attack, which can be used to create a nonwatermarked signal when a watermark detector device is available. Practically, application of these attacks is restricted due to their high computational complexity.

Protocol attacks

Protocol attacks aim at attacking the entire concept of the watermarking application. One type of protocol attack is based on the concept of invertible watermarks [9]. The idea behind inversion is that the attacker subtracts his own watermark from the watermarked data and claims to be the owner of the watermarked data. This can create ambiguity with respect to the true ownership of the data. It has been shown that for copyright protection applications, watermarks need to be non-invertible. The requirement of non-invertibility of the watermarking technology implies that it should not be possible to extract a watermark from a non-watermarked document. A solution to this problem might be to make watermarks signal-dependent by using one-way functions. Another protocol attack is the copy attack. In this case, the goal is not to destroy the watermark or impair its detection, but to estimate a watermark from watermarked data and copy it to some other data, called target data. The estimated watermark is adapted to the local features of the target data to satisfy its imperceptibility. The copy attack is applicable when a valid watermark in the target data can be produced with neither algorithmic knowledge of the watermarking technology nor the

knowledge of the watermarking key. Again, signal-dependent watermarks might be resistant against the copy attack.

Performance Measures Of Watermarking Algorithms

The success of watermarking algorithm is evaluated based on a series of measures [11]. Because of the psychological nature of the problem not all criteria are quantitative in nature. Although only some factors are appropriate for a given application, we present all the most popular metrics below to highlight the character of good watermarking scheme. Without loss of generality, we assume the host and watermarked signals are images.

1. Perceptual Quality: Perceptual quality refers to the imperceptibility of embedded watermark data within the host signal. In most applications, it is important that the watermark is undetectable to a listener or viewer. This ensures that the quality of the host signal is not perceivably distorted; the peak signal-to-noise ratio (PSNR) of the watermarked signal versus the host signal was used as a quality measure. The PSNR is defined as :

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right)$$

$$MSE = \frac{1}{MN}\sum_{j=1}^{M}\sum_{k=1}^{N}(X(m,n) - X_w(m,n))^2$$

in units of dB, where X is host signal, wis the watermark X_w is the watermarked signal MN , is the total number of pixels in X or X_w .

2. Correlation Coefficients: To measure the similarity between embedded and extracted watermarks, the following normalized correlation coefficients is defined as:

$$r = \frac{\sum_m \sum_n w(m,n)\hat{w}(m,n)}{\sqrt{\left(\sum_m \sum_n w^2(m,n)\right)}\sqrt{\left(\sum_m \sum_n \hat{w}^2(m.n)\right)}}$$

where w and wˆ are the embedded and extracted watermarks, respectively.

3. Bit Rate: Bit rate refers to the amount of watermark data that may be reliably embedded within a host signal per unit of time or space, such as bits per second or bits per pixel. A higher bit rate may be desirable in some applications in order to embed more copyright information. In this study, reliability was measured as the bit error rate (BER) of extracted watermark data. For embedded and extracted watermark sequences of length B bits, the BER (in percent) is given by the expression as:

$$BER = \frac{100}{B}\sum_{n=0}^{B-1}\begin{cases}1 & \hat{w}(n) \neq w(n)\\ 0 & \hat{w}(n) = w(n)\end{cases}$$

Computational Complexity: Computational complexity refers to the processing required to embed watermark data into a host signal, and / or to extract the data from the signal. Algorithm complexity is important to know, for it may influence the choice of implementation structure or DSP architecture. Although there are many ways to measure complexity, such as complexity analysis (or “Big-0’ analysis), for practical applications more quantitative values are required.

Fuzzy C-Means Clustering

Advances in cognitive psychology over the past decades have revealed that visual data, in the form of scenes and pictures, are often mentally processed in visual terms alone, without any corresponding translation or recording into verbal labels or representation, and humans often

respond strongly to color cues within image contents. In the past decade, color imaging and printing devices has become more affordable and computer power has been ever increasing. As a result color imaging has become very popular in many applications including object classification and recognition, video surveillance, image indexing and retrieval in image databases, feature based video compression, etc. In this chapter we discuss about color image clustering, which is often a necessary computational process for color-based image retrieval and object recognition.

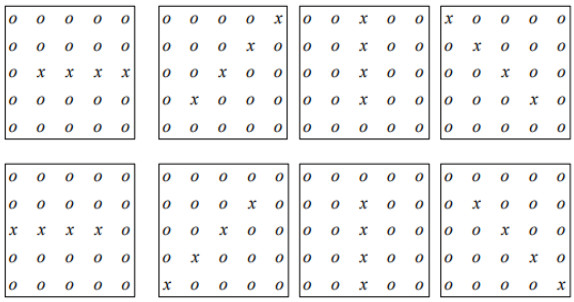

Figure.4. The eight partition of the detection window

Image clustering is a process of partitioning image pixels based on selected image features. The pixels that belong to the same region must be spatially connected and have the similar image features. If the selected clustering feature is color, an image clustering process would separate pixels that have distinct color feature into different regions, and simultaneously, group pixels that are spatially connected and have the similar color into the same region. Every pixel in the image must be assigned to a region when any clustering algorithm terminates. In image processing two terms are usually seen very frequently close to each other: clustering and clustering. When analyzing the color information of an image, for example and trying to separate regions or ranges of color components having same characteristics, the process is called clustering. Mapping the clusters onto the spatial domain and physically separating regions or surfaces in the image is called clustering. The objective of color clustering is to divide a color set into c homogeneous color clusters. Color clustering is used in a variety of applications, such as color image clustering and recognition. Color clustering is an inherently ambiguous task because color boundaries are often blurred. For example, consider the task of dividing a color image into color objects. In color images, the boundaries between objects are blurred and distorted due to the imaging acquisition process. Furthermore, object definitions are not always crisp, and knowledge about the objects in a scene may be vague. Fuzzy set theory and fuzzy logic are ideally suited to deal with such uncertainties. Fuzzy clustering models have proved a particularly promising solution to the color clustering problem. Such unsupervised models can be used with any number of features and clusters. In addition, they distribute membership values across the clusters based on natural groupings in feature space (Bezdek, 1999). In fuzzy clustering, the uncertainty inherent in a system is preserved as long as possible before decisions are made. Of the fuzzy clustering algorithms proposed to date, the fuzzy c-means (FCM) algorithm proposed by Bezdek is the most widely used in image clustering because it has robust characteristics for ambiguity and can retain much more information than hard clustering methods. Fuzzy c-means is an unsupervised technique that has been successfully applied to feature analysis, clustering, and classifier designs in fields such as astronomy, geology, medical imaging, target recognition, and image clustering. An image can be represented in various feature spaces, and the FCM algorithm classifies the image by grouping similar data points in the feature space into clusters.

Fuzzy c-means Algorithm

Clustering is a process for classifying objects or patterns in such a way that samples of the same group are more similar to one another than samples belonging to different groups. Many clustering strategies have been used, such as the hard clustering scheme and the fuzzy clustering scheme, each of which has its own special characteristics.

As a consequence, with this approach the clustering results are often very crisp, i.e., each pixel of the image belong to exactly just one class. However, in many real situations, for images, issues such as limited spatial resolution, poor contrast, overlapping intensities, noise and intensity inhomogeneities variations make this hard (crisp) clustering a difficult task. Due to this fuzzy set theory was proposed, which produced the idea of partial membership of belonging described by a membership function. Fuzzy clustering as a soft clustering method has been widely studied and successfully applied to image clustering [37-40].The fuzzy c-means (FCM) algorithm, proposed by Dunn and generalized by Bezdek[41], has the function to describe the fuzzy classification for the pixels by calculating the fuzzy membership value. Fuzzy c-means algorithm is a data clustering algorithm in which each data point belongs to a cluster to a degree specified by a membership grade. It minimizes an objective function, with respect to fuzzy membership U, and set of cluster centroids V.

$$J(U, V) = \sum_{k=1}^{n} \sum_{i=1}^{c} (u_{ik})^m d^2(x_k, v_i)$$

Where,

$$X = \{x_1, x_2, \ldots, x_n\} \subseteq R^p$$

c - the number of cluster centers or data subsets
m - the weighting exponents, 1 for 'hard' clustering, and increasing for fuzzier clustering;
$d^2(x_k, v_i)$ - the distance measure between object xk and cluster center vi;
n - the total number of pixels in image;
uik - the fuzzy membership value of pixel k in cluster i;
vi - the cluster center for subset i in feature space;
U – the fuzzy c-partition

The above fuzzy c-mean algorithm uses iterative operation to get U and V and finally minimizes the objective function. The algorithm is achieved as following:

1. Fix the number of cluster c, 2<c<n
   Fix m< ∞ 2.
2. Initialize the fuzzy c-partition $U^{[0]}$;
3. 3. Assume the steps b = 1, 2 ,…. 4.
4. Calculate the c cluster centers $\{V_i^{(b)}\}$ with $U^{(b)}$, the cluster center for cluster i is .

$$v_i = \frac{\sum_{k=1}^{n} (u_{ik})^m x_k}{\sum_{k=1}^{n} (u_{ik})^m}$$

5. Update $U^{(b)}$, calculate the membership $U^{(b+1)}$) :

(a) Calculate Ik and Tk

$I_k = \{I\ 1<i<c\}$;
$d_{ik} = abs\ (x_i - v_k) = 0$,
$T_k = \{1,2,\ldots c\} - I_k$,

(i) if $I_k = 0$

$$u_{ik} = \frac{1}{\sum_{j=1}^{c} \left(\frac{d_{ik}}{d_{jk}} \right)^{\frac{2}{m-1}}}$$

(ii) else

$u_{ik} = 0, \ \forall \ i \in T_k$ and $\sum_{i \in I_k} u_{i_k} = 1$

Compare $U^{(b)}$ and $U^{(b+1)}$ in a convenient matrix norm,

If $U^{(b)} - U^{(b+1)} < \in_L$, stop;

Otherwise, set b = b+1 and go to step 4.

Here $U^{(0)}$ is the initial partition and can be randomly set or by an approximation method. $\in_L$ is the convergence threshold. The introduction of the term m makes the clustering flexible, m = 1 for 'hard' clustering. The increase of the values of m stresses the fuzzy properties. The FCM process is guaranteed to converge for m >1.

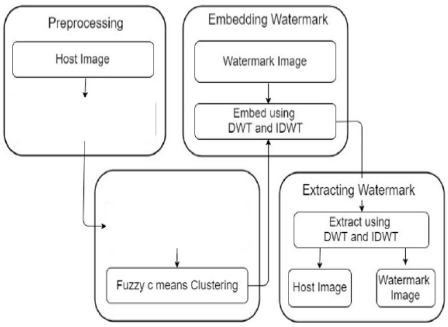

Figure 5. Flowchart of the proposed model.

Neighboring Pixels Into FCM

This proposed method is based on the FCM incorporating spatial function [42] proposed by K-S Chuang et al. One of the important characteristics of an image is that its neighbouring pixels are highly correlated to each other. The probability that a pixel neighbourhood will belong to same cluster is very high. This property of the pixels is quite helpful when the image is affected by noise. As the spatial relationship among pixels is not considered in the standard FCM algorithm a spatial function is introduced to take into account the neighborhood property. For finding the spatial function, the membership information of each pixel of a cluster is converted to its spatial domain to get the complete image. Then we calculate the spatial function, using the following definition

$$S_{ik} = \sum_{k \in NB(x_k)}^{M} u_{ij}$$

where $NB(x_k)$ represents a square window centered on pixel x_k ($1<k<n$) where n is the total number of pixels in the image) in the spatial domain image containing the membership information of each pixel to a particular cluster 'i '. A 5x5 window was used for this work. Just like the membership function uij the spatial function sik gives the membership of the kth pixel to a particular cluster 'i '. The spatial function is modified in order to take into account the properties of a local neighborhood in a way that the membership of each pixel results as a weighted sum of the pixels in the 5x5 neighborhood. This enables smoothening of the edges or boundaries of objects present in an image. Assuming M as the 5x5 neighborhood of the pixel j, the membership function to a cluster i is modified as follows:

$$h_{ik} = \frac{(h_{ik} + s_{ik})}{25}$$

Hence the new algorithm developed is named Modified spatial fuzzy c means (MSFCM) The spatial function is then introduced in the membership function as follows:

$$u'_{ik} = \frac{u_{ik}^{p} h_{ik}^{q}}{\sum_{j=1}^{c} u_{jk}^{p} h_{jk}^{q}}$$

where p and q are parameters which control the relative importance of both functions. If the pixels in an image are not affected by noise then spatial function will only fortify the original membership, and the clustering result remains unchanged. However, for a noisy pixel, this formula reduces the weight of a noisy cluster by the labels of its neighboring pixels. As a result, misclassified pixels from noisy regions or spurious blobs can easily be corrected. The clustering is a two-pass process. In the first pass we use the standard FCM to calculate the membership value for each pixel. The membership value for each pixel to different clusters is then mapped to spatial domain and the spatial function is calculated from that. In the second pass, the FCM iteration proceeds with the new membership function that is incorporated with the spatial function. The iteration of spatial FCM algorithm stopped when the difference between the present and the previous objective function is less than or equal to a certain value (10^{-5}). After the convergence, defuzzification is applied to assign each pixel to a specific cluster for which the membership is maximal.

Applications

Although the main motivation behind the digital watermarking is the copyright protection, its applications are not that restricted. There is a wide application area of digital watermarking, including broadcast monitoring, fingerprinting, authentication and covet communication [5, 8]. For secure applications a watermark is used for following purposes:

1. Copyright Protection: For the protection of intellectual property, the data owner can embed a watermark representing copyright information in his data.
2. Fingerprinting: To trace the source of illegal copies, the owner can use a fingerprinting technique. In this case, the owner can embed different watermarks in the copies of the data that are supplied to different customers. Fingerprinting can be compared to embedding a serial number that is related to the customer's identity in the data.
3. Broadcast Monitoring: By embedding watermarks in commercial advertisements, an automated monitoring system can verify whether advertisements are broadcasted as contracted. Not only commercials but also valuable TV products can be protected by broadcast monitoring.
4. Data Authentication: The authentication is the detection of whether the content of the digital content has changed. As a solution, a fragile watermark embedded to the digital content indicates whether the data has been altered. If any tampering has occurred in the content, the same change will also occur on the watermark.
5. Covert Communication: The watermark, secret message, can be embedded imperceptibly to the digital image or video to communicate information from the sender to the intended receiver while maintaining low probability of intercept by other unintended receivers.

For non-secure applications a watermark is used for following purposes:

1. Indexing: Indexing of video mail, where comments can be embedded in the video content; indexing of movies and news items, where markers and comments can be inserted that can be used by search engines.
2. Medical Safety: Embedding the date and the patient's name in medical images could be a useful safety measure.
3. Data Hiding: Watermarking techniques can be used for the transmission of secrete private messages. Since various governments restrict the use of encryption services, people may hide their messages in other data.

Although not yet widely recognized as such, bandwidth-conserving hybrid transmission is yet another information embedding application, offering the opportunity to re-use and share existing spectrum to either backwards-compatibility increase the capacity of an existing communication network, i.e., a "legacy" network, or allow a new network to be backwards-compatibility overlaid on top of the legacy network. In this case the host signal and embedded signal are two different signals that are multiplexed, i.e., transmitted simultaneously over the same channel in the same bandwidth, the host signal being the signal corresponding to the legacy network. Unlike in conventional multiplexing scenarios, however, the backwards compatibility requirement imposes a distortion constraint between the host and composite signals.

So-called hybrid in-band on-channel digital audio broadcasting (DAB) is an example of such a multimedia application where one may employ information embedding methods to backwards-compatibility upgrade the existing commercial broadcast radio system. In this application one would like to simultaneously transmit a digital signal with existing analog (AM and/or FM) Commercial Broadcast radio without interfering with conventional analog reception. Thus, the analog signal is host signal, and the digital signal is the watermark. Since embedding does not degrade the host signal too much, conventional analog receivers can demodulate the analog host signal. This embedded signal may be all or part of a digital audio signal, an enhancement signal used to refine the analog signal, or supplemental information such as station identification.

SIMULATION RESULTS

For simulations, we take Lena image of size 512×512 as the host image shown in Fig. and watermark is visually recognizable gray-scale image of size 32 32× shown in Fig. . To form the watermark, the DC value is first subtracted from the watermark image and then made its variance value to 1, before watermark image is used for simulation. We chose 75 B = , ;5 L = and α value was set to 60, 40, 20, 10, and 5 percent of mean value of detail image blocks for lower resolution level to higher resolution level respectively, and α value was set to 1.6% of approximate image blocks in our simulation. The PSNR value of watermarked image is 37.5381 as shown in Fig. , and is perceptually identical to the original host and watermark can be exactly extracted. The resulting watermarked image is corrupted using one of many common distortions which we discuss in the subsequent section. When the watermark was extracted it was scaled, so that its minimum pixel value was set to black and its maximum pixel value to white and correlated with the embedded watermark to measure the robustness and detection capability of the technique.

After the embedding process, the watermarked image was passed through different attacks. Then, the watermark image was extracted from the watermarked image. The extraction process was performed by IDWT [23], which is the reverse process of DWT. After

completion of the extraction process, the performance was evaluated by comparing the extracted watermark image and the original watermark image.

The performance (in terms of robustness and imperceptibility) of our model was evaluated with the following parameters: PSNR, BER, where PSNR was used for imperceptibility, and BER and CC were used for robustness. PSNR measured the amount of distortion of the watermarked image. In general, the greater value of PSNR represents less distortion.

$$PSNR = 10\log_{10}\left(\frac{peakval^2}{\sqrt{\frac{\sum_{x=1}^{M}\sum_{y=1}^{N}\{W(x,y)-W'(x,y)\}^2}{M*N}}}\right)$$

For Equations (1) and (2), *M* and *N* are the number of rows and columns, respectively, w and w' represent the original image and extracted image, respectively, and x and y denote the pixel location. Length of the watermark image is expressed by L [24]. Pixel values can be positive or negative. Due to this fact, the summation is squared to avoid the issue where positive and negative values can cancel out each other. Then, the mean value is the square rooted for equality. On the other hand, peakval represents the maximum possible pixel value of the original image. When each pixel is denoted by 8 bits, the peakval will be 255. For instance, if two images are identical to each other, then the divisor value is zero, which is eventually converted to a PSNR value of infinity.

BER evaluates the transmission accuracy where the value closer to zero illustrates a higher quality of image.

$$BER = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N}|w'(x,y)-w(x,y)|}{L}$$

Robustness against JPEG Lossy Compression Figures shows the effect of compression on the correlation coefficient for different quality factors. The correlation coefficient remains high for reasonable quality factor values. Severe visual image degradation in which the features of the face were not distinguishable occurred for quality factors of 15 and above. The results show that the watermark still remains present and correlation coefficient is still high about 0.8. Fig. shows the degraded watermarked image.

Conclusions

In this paper, an approach to digital watermarking on biomedical images was put forward to ensure the safety and confidentiality of the image. This process is an application of biometrics since it provides unique identification through retention of a watermark after transmission. Additionally, access to the medical images by the authorized users can be validated through cross checking of the distinct watermark. The proposed model utilizes the improved fuzzy c-means, DWT, and IDWT. Firstly, the model operates on threshold to pre-process the image. Secondly, the enhanced image is segmented using the fuzzy c-means. Then, the segmented image is watermarked using DWT and IDWT. After that, the watermark is extracted using the reverse process of embedding. Finally, the performance was measured, which indicates that the suggested scheme shows superior results in terms of efficiency and imperceptibility as well as upholding the robustness against various attacks.

FUTURE WORK

1. The execution time of the proposed method is an area of concern. Hence clustering methods which are less time consuming can be developed for segmentation.

2. The fuzzy clustering based method can be combined with other methods like Genetic algorithm and Level set methods to give better segmentation results.
3. The number of cluster has to be fixed initially in FCM based segmentation methods. Some method which doesn't require fixing of number of clusters before clustering can also be used for segmentation

Future work will also concentrate on making the watermarking methods more practical by modifying the techniques such that the host image is not required to extract the watermark and robust to both geometric and non geometric attacks.

REFERENCES

[1] Van Schyndel, R.G., Tirkel, A.Z., and Osborne, C.F., "A digital Watermark." Proc. of the IEEE Int. Conference on Image Processing. Vol. 2, (1994): pp. 86-90.
[2] Swanson, M.D., Kobayashi, M., and Tewfik, A.H., "Multimedia Data-Embedding and Watermarking Technologies." Proc. of the IEEE. Vol. 86, No. 6, (June 1998): pp. 1064–1087.
[3] Petitcolas, F., Anderson, R., and Kuhn, M., "Information Hiding - a Survey." Proc. of the IEEE. Vol. 87, No. 7, (July 1999): pp. 1062–1078.
[4] Barni, M., Bartolini, F., Cox, I.J., Hernandez, J., and Perez-Gonzalez, F., "Digital Watermarking for Copyright Protection: A communications perspective." IEEE Communications Magazine. Vol. 39, No. 8, (August 2001):pp. 90–133.
[5] Langelaar, Gerhard C., Setyawan, I., and Lagendijk, R.L., "Watermarking Digital Image and Video Data: A state-of-the-art-overview." IEEE Signal Processing Magazine. Vol. 17, No. 5, (September 2000): pp. 20-47.
[6] Voyatzis, G., Mikolaides, N., and Pitas, I., "Digital watermarking: An overview." Proc. of IX European Signal Processing Conference(EUSIPCO), Island of Rhodes, Greece. (September 8-11, 1998): pp. 13-16. [7] Wolfgang, R.B., Podilchuk, C.I., and Edward J. Delp, "Perceptual Watermarks for Image and Video." Proc. of the IEEE. Vol. 87, No. 7, (July 1998): pp. 1109-1126. [8] Cox, I.J., Miller, M.L., and Bloom, J.A., "Watermarking Applications and their Properties." Proc. of IEEE Int. Conference on Information Technology, Las Vegas. (March 2000): pp. 6-10.
[9] Craver, S., Memon, N., Yeo, B.-L., and Yeung, M.M., "Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks and Implications." IEEE Journal On Selected Areas in Communications. Vol. 16, No. 4, (May 1998): pp. 573-586.
[10] Voloshynovskiy S. et al., "Attacks on Digital Watermarks: Classification, EstimationBased Attacks, and Benchmarks." IEEE Communication Magazine. Vol. 39. No. 8, (August 2001): pp. 118-126.
[11] Gordy, J.D., and Bruton, L.T., "Performance Evaluation of Digital Audio Watermarking Algorithm." Proc .of 43rd IEEE Midwest Symposium on Circuits and Systems. Vol. 1, (August 2000): pp 456-459.
[12] Ruanaidh, J.J.K.O', Dowling, W.J., and Boland, F.M., "Phase Watermarking of Digital Images." Proc. of IEEE Int. Conference on Image Processing, Lausanne, Switzerland. Vol. 3, (September 16-19, 1996): pp. 239-242.
[13] Ruanaidh, J.J.K.O', and Pun, T., "Rotation, Scale and Translation Invariant Digital Image Watermarking." Proc. of IEEE Int. Conference on Image Processing, Santa Barbara, CA, USA. Vol. 1, (October 1997): pp. 536-539.
[14] Cox, I.J., Kilian, J., Leighton, F.T., and Shamoon, T., "Secure Spread Spectrum Watermarking for Multimedia." Proc. of IEEE Int. Conference on Image Processing.

Vol. 6, (December 1997): pp. 1673-1687. [15] Boland, F.M., Ruanaidh, J. J. K. O´, and Dautzenberg, C. "Watermarking Digital Images for Copyright Protection." Proc. of IEEE Int. Conference on Image Processing and its Application, Edinburgh, U.K. (July 1995): pp. 321-326.

[16] Barni, M., Bartolini, F., Cappellini, V., and Piva, A., "A DCT Domain System for Robust Image Watermarking." Signal Processing Archive. Vol. 66, No. 3, (May 1998): pp. 357- 372.

[17] Burgett, S., Koch, E., and Zhao, J., "Copyright Labeling of Digitized Image Data." IEEE Communication Magazine. Vol. 36, (March 1998): pp. 94-100.

[18] Bors, A.G., and Pitas, I., "Image Watermarking Using DCT Domain Constraints." Proc. of IEEE Int. Conference on Image Processing, Lausanne, Switzerland. Vol. 3, (September 16–19, 1996): pp. 231-234.

[19] Swanson, M.D., Zhu B., and Tewfik, A.H., "Transparent Robust Image Watermarking." Proc. of IEEE Int. Conference on Image Processing. Vol. 3, (1997): pp. 211-214.

[20] Tao, B., and Dickinson, B., "Adaptive Watermarking in the DCT Domain." Proc. of IEEE Int. Conference on Acoustics, Speech and Signal Processing, Munich, Germany. Vol. 4, (1997): pp. 2985-2988. [21] Podilchuk, C.I., and Zeng, W., "Perceptual Watermarking of Still Images." IEEE Workshop on Multimedia Signal Processing, Princeton, New Jersey. (June 23-25, 1997): pp. 363-368.

[22] Wu, J., and Xie, J., "Adaptive Image Watermarking Scheme Based on HVS and Fuzzy Clustering Theory." Proc. of IEEE int. Conference on Neural Network and Signal Processing, Nanjing, China. (December 14-17, 2003): pp. 1493-1496. [23] Zhang, W., Zhu, W., and Fu, Y., "An Adaptive Digital Watermarking Approach." Proc. of IEEE int. Conference on Mechatronics and Automation, Chengdu, China. (August 2004): pp. 690-695. [24] Pu, Y., et el., "A Public Adaptive Watermark Algorithm for Color Images Based on Principal Component Analysis of Generalized Hebb." Proc. of IEEE int. Conference on Information Acquisition. (2004): pp. 690-695.

[25] Xia, X.-G., Boncelet, C.G., and Arce, G.R., "A Multiresolution Watermark for Digital Images." Proc. of IEEE Int. Conference. on Image Processing, Santa Barbara, CA, USA. Vol.3, (October 26-29, 1997): pp. 548-551.

[26] Podilchuk, C.I., and Zeng, W., "Image Adaptive Watermarking Using Visual Models." IEEE Journal on Selected Areas in Communication. Vol. 16, No. 4, (May 1998): pp. 525- 539.

[27] Hsieh, M.-S., Tseng D.-C., and Huang Y.-H., "Hiding Digital Watermarks Using Multiresolution Wavelet Transform." IEEE Transaction on Industrial Electronics. Vol. 48, No. 5, (October 2001): pp.875-882.

[28] Kundur, D., and Hatzinakos D., "Digital Watermarking Using Multiresolution Wavelet Decomposition." Proc. of IEEE Int. Conference on Acoustics, Speech and Signal Processing. Vol. 5, (1998): pp. 2969-2972.

[29] Barni, M., Bartolini F., and Piva, A., "Improved Wavelet-Based Watermarking Through Pixel-wise Masking." IEEE Transaction on Image Processing. Vol. 10, No. 5, (May 2001): pp. 783-791.

[30] Kang X., Huang J., Shi Y.Q., and Lin Y., "A DWT-DFT Composite Watermarking Scheme Robust to Both Affine Transform and JPEG Compression." IEEE Transaction on Circuits and Systems for Video Technology. Vol. 13, No. 8, (August 2003): pp. 776-786.

[31] Wu, J., and Xie, J., "Blind Wavelet-Based Watermarking Scheme Using Fuzzy Clustering Theory." Proc. of IEEE int. Conference on Neural Network and Signal Processing, Nanjing, China. (December 14-17, 2003): pp. 1521-1524
[32] Guannan, Z., Shuxun, W., and Quan, W., "An Adaptive Block-Based Blind Watermarking Algorithm." Proc. of IEEE int. Conference on Signal Processing. (2004): pp. 2294-2297.
[33] Mallat, S.G., "Multifrequency Channel Decompositions of Images and Wavelet Models." IEEE Transaction on Acoustics, Speech and Signal Processing. Vol. 37, No. 12,(December 1989): pp. 2091-2110.
[34] Wilson, T.A., Rogers S.K., and Myers L.R., "Perceptual-based hyperspectral image fusion using multiresolutional analysis." Optical Engineering. Vol. 34, (November 1995): pp. 3154-3164.
[35] Levine, M. D. Vision in Man and Machine. New York: McGraw-Hill, Toronto, 1985.
[36] Kundur, D., and Hatzinakos D., "Toward Robust Logo Watermarking Using Multiresolution Image Fusion Principles." IEEE Transaction on Multimedia. Vol. 6, No. 1, (February 2004): pp. 185-197.
[37] Tolias Y.A. and Panas S.M. On applying spatial constraints in fuzzy image clustering using a fuzzy rule based system, IEEE signal processing letters, 5(1998):pp. 245-247.
[38] Liew A.W.C., Leung S.H., and Lau W.H. Fuzzy image clustering incorporating spatial continuity, IEEE Proc. Visual Image Signal Process. 147, 185.192 (2000).
[39] Siyal M. Y. and Yu Lin. An intelligent modified fuzzy c-means based algorithm for bias estimation and segmentation of brain MRI. Pattern Recognition Letters. vol. 26, no. 13, Oct. 2005, pp. 2052-2062.
[40] Li X., Li L., Lu H., Chen D., and Liang Z. Inhomogeneity correction for magnetic resonance images with fuzzy c-mean algorithm., Proc. SPIE 5032, 995.1005 (2003).
[41] Kwon M.J., Han Y.J., Shin I.H., and Park H.W. Hierarchical fuzzy segmentation of brain MR images., Int. J. Imaging Systems and Technology ,vol. 13, (2003),pp.115-125.
[42] Chuang Keh-Shih, Tzeng Hong-Long, Chen Sharon et al., Fuzzy C-means clustering with spatial information for image segmentation, Computeried Medical Imaging and graphics, 30(2006) 9-15.
[43] Yang Zhang, Chung Fu-Lai, et al, Robust fuzzy clustering-based image segmentation, Applied Soft Computing, vol(9), no. 1, Jan (2009), pp. 80-84. [76] Karmakar G.C, Dooley L. and Rahman S.M. A survey of fuzzy rule based image segmentation techniques, 1st IEEE Pacific-Rim Conf. on Multimedia, Sydney, Australia (2000), pp. 350–353.