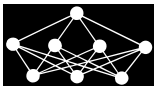


THE USE OF COMPUTATIONAL INTELLIGENCE IN DIGITAL WATERMARKING: REVIEW, CHALLENGES, AND NEW TRENDS

Ashraf Darwish[*], *Ajith Abraham*[†]

Abstract: Digital Watermarking (DW) based on computational intelligence (CI) is currently attracting considerable interest from the research community. This article provides an overview of the research progress in applying CI methods to the problem of DW. The scope of this review will encompass core methods of CI, including rough sets (RS), fuzzy logic (FL), artificial neural networks (ANNs), genetic algorithms (GA), swarm intelligence (SI), and hybrid intelligent systems. The research contributions in each field are systematically summarized and compared to highlight promising new research directions. The findings of this review should provide useful insights into the current DW literature and be a good source for anyone who is interested in the application of CI approaches to DW systems or related fields. In addition, hybrid intelligent systems are a growing research area in CI.

Key words: *Computational intelligence, digital watermarking, artificial neural networks, fuzzy logic, rough sets, swarm intelligence, genetic algorithms, fuzzy-neural systems, genetic-swarm systems, genetic-fuzzy systems*

Received: October 10, 2010
Revised and accepted: August 31, 2011

[*]Ashraf Darwish
Faculty of Science, Helwan University, Cairo, Egypt Machine Intelligence Research Labs (MIR Labs), USA, E-mail: amodarwish@yahoo.com
[†]Ajith Abraham
Faculty of Electrical Engineering and Computer Science, VSB – Technical University of Ostrava, Ostrava – Poruba, Czech Republic, E-mail: ajith.abraham@ieee.org
Machine Intelligence Research Labs (MIR Labs), Scientific Network for Innovation and Research Excellence, Seattle, WA, USA, E-mail: ajith.abraham@ieee.org

1. Introduction

CI is considered as one of the most important and rapidly increasing fields, which attract a large number of researchers and scientists working in areas, such as neurocomputing, approximate reasoning, global optimization etc. CI has been a tremendously active area of research for the last years. There are many prominent applications of CI in many subfields, for example, image processing, retrieval audio processing [34], and text processing. However, there are still numerous open problems in different areas, such as in multimedia processing and computer animation that need advanced and efficient computational methodologies [41,48].

DW refers to the process of embedding some labels or signatures into digital media without introducing perceptible artifacts. It plays a vital role in the applications to copyright protection of digital media, authentication, date integrity, fingerprinting, and data hiding. This paper introduces some important techniques of CI, such as RS, FL, ANN, GA and SI to be applied for DW technology, and then the paper introduces the combination of such techniques in order to propose solutions of the new challenges of CI in the DW area as illustrated in [16, 36]. This article also illustrates a comprehensive review on research contributions that investigate utilization of CI techniques in building DW models; as well as to present the researchers in DW the existing research challenges, and to highlight promising new research directions for future investigation.

The remainder of this paper is organized as follows. Section 2 overviews the fundamentals of CI and DW. Section 3 categorizes compares and summarizes core algorithms in CI that have been proposed to solve DW problems, such as RS, FL, ANN, GA, and SI. Section 4 is devoted to some hybrid intelligent techniques in DW. Section 5 introduces some threats of DW technology. Challenges and some open problems of DW, such as collusion attack, signal processing collusion, and cost are presented in Section 6. Section 7 presents the conclusions.

2. Overview of Computational Intelligence and Digital Watermarking

2.1 Computational Intelligence versus Artificial Intelligence

CI is a new research field with competing definitions. For example, the authors in [21] defined CI as the study of the design of intelligent agent. In contrast, the author of [39] defined CI as a system when it deals with only numerical (low-level) data, has pattern recognition components, does not use knowledge in the artificial intelligence sense; in addition it exhibits the following capabilities (i) computational adaptivity, (ii) computational fault tolerance, (iii) speed approaching human-like turnaround, and (iv) error rates that approximate human performance.

There is a difference between CI and Artificial Intelligence (AI), where AI can deal with symbolic knowledge representation, while CI handles numeric representation of information; AI concerns itself with high-level cognitive functions, while CI is related to low-level cognitive functions. Furthermore, AI analyzes the structure of a given problem and attempts to construct an intelligent system based upon this structure, thus operating in a top-down manner, while the structure is expected to

emerge from an unordered beginning in CI, thus operating in a bottom-up manner [3,8,71]. CI is an offshoot of AI. As an alternative to good old-fashioned artificial intelligence (GOFAI) it rather depends on heuristic algorithms, such as in fuzzy sets, ANNs and evolutionary computation. In addition, CI includes techniques that use SI, Fractals and Chaos Theory, Artificial immune systems, Wavelets, etc. CI combines elements of learning, adaptation, evolution and FL to create intelligent systems. Also, CI accepts statistical methods, but often gives a complementary view as in the case of FL. ANNs are a division of CI that is closely related to machine learning [2]. CI includes the following set of main and sub main systems:

- *Fuzzy Sets*: Fuzzy Logic, Rough Sets, Vague Sets, Type-II Fuzzy, etc.
- *Artificial Neural Networks*: Back Propagation (BP), Radial Basis Function (RBF), Learning Vector Quantization (LVQ), Adaptive Resonance Theory (ART), etc.
- *Natural-Inspired Algorithms*: Swarm Intelligence, Ant Colony Algorithm, Evolutionary Algorithms, Evolutionary Programming, Artificial Immune System, Clonal Selection Algorithm.
- *Multi-Scale Geometric Analysis*: Fourier, Wavelet, Ridgelet, Curvelet, Contourlet, Brushlet, Bandelet, Directionlet, etc.

CI can be employed for the sociological concept of human group formation to obtain a better solution to such classification problems [4]. The key concept of the human group formation is about the behavior of in-group members that try to unite with their own group as much as possible, and at the same time maintain social distance from the out-group members. CI and machine learning methods [51] can be applied to extract the biological knowledge from bio-molecular data as in [30], in order to obtain models to both represent biological knowledge and to predict the characteristics of biological systems.

2.2 Information hiding and digital watermarking

Information hiding, also known as data hiding or data embedding, includes DW and steganography, as summarized in Fig. 1. Information hiding systems hide secret information into an object, e.g., an audio, video, image, or written text, to create a watermarked object. DW is used for many purposes such as copyright protection, broadcast monitoring, transaction tracking, and similar activities. A watermarking scheme alters a cover object, either imperceptibly or perceptibly, to embed a message about the cover object.

It is done by hiding data (information) within digital audio, images and video files [57]. One way of such data hiding is copyright label or DW that completely characterizes the person who applies it and, therefore, marks it as being his intellectual property. DW is the process that embeds data called a watermark into a multimedia object such that watermark can be detected or extracted later to make an assertion about the object. Watermarking is either visible or invisible. Although visible and invisible are visual terms, watermarking is not limited to images, it can also be used to protect other types of multimedia object.

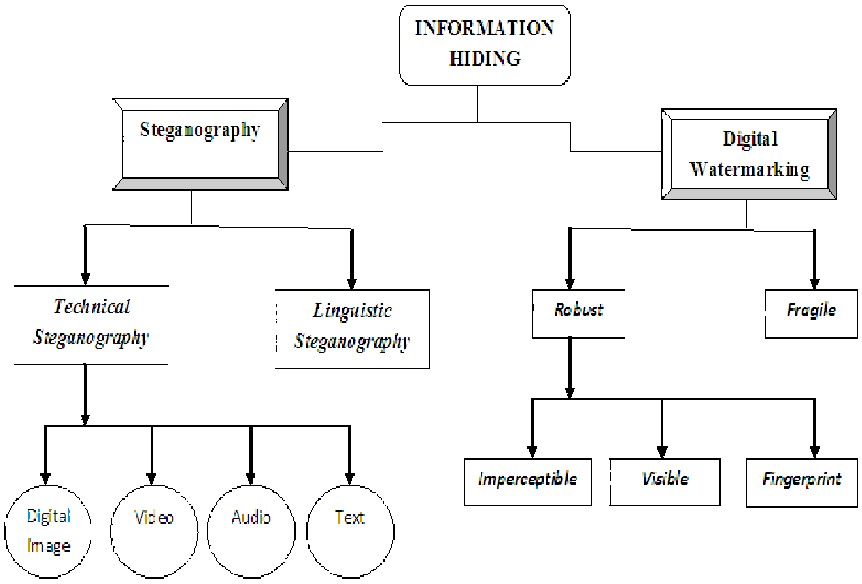


Fig. 1 *Digital watermarking and steganography disciplines of information hiding.*

The watermark can be perceived as an attribute of the cover (carrier). It may contain information, such as copyright copyrights, licensing, tracking and authorship etc., whereas in the case of steganography, embedded message may have nothing to do with the cover. In steganography issue of concern is bandwidth for hidden messages while robustness is more important with watermarking.

The robustness is the ability to resist certain malicious attacks, such as the general operations of signal processing which is important issue in DW. On the other hand, steganography is used for secret data and communications. A steganographic method undetectably alters a cover object to conceal a secret message. Thus, the methods of steganography can hide the very presence of covert communications.

If a data-embedding scheme is irreversible, then a decoder can extract only the secret data and the original cover image cannot be restored. On the other hand, a reversible data-embedding scheme allows the decoder to recover the original cover image completely upon extraction of the embedded secret data. Reversible data hiding schemes are suitably used for some applications, such as in the healthcare applications and online content distribution systems [13].

Information hiding scheme with low image distortion is more secure than one with high distortion because it does not raise suspicions of adversaries. Information hiding system with high payload is preferred because more secret data can be transmitted. The robustness is particularly important in the applications of DW but achieving robustness is technically challenging in high-payload data hiding systems. In this case, visual quality, hiding capacity, and robustness become conflicting factors.

2.3 Digital watermarking: An overview

The 21st century is the age of information as information becomes an important resource in many applications. Information obtaining, processing and security are playing an important role in comprehensive national power, and information security is related to national security and social stability. There are some important theories about information security and technology.

Modern DW technology has a rather short history since 1990. At the beginning of 1990 the idea of DW, embedding information into audiovisual data and images has emerged [43, 58]. Since then research activities have been increasing and industrial interest in DW methods kept growing.

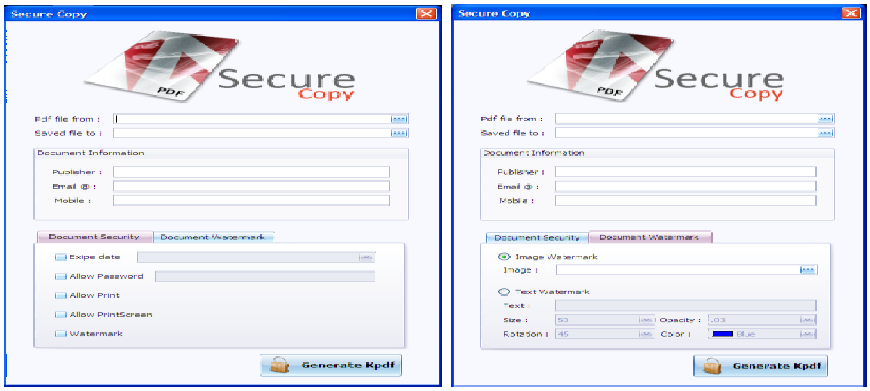
DW algorithms have been proposed for the protection of copyright of digital images. In DW algorithms there are different types of watermarks, such as labels, logos, and trademarks are embedded into the digital image. Generally speaking, which can help to solve ownership disputes by identifying the owner of the disputed media? The embedded watermark in the digital image can be used to verify ownership. DW has three major application fields, namely data monitoring, data and image authentication [42, 48], and copyright protection.

Darwish et al. in [5] proposed a new digital watermarking method that has been proposed to protect PDF files copyright through visible watermarks in such files. As well as to provide the integrity of the digital watermark, an asymmetric cryptographic algorithm (DES) is employed. The proposed watermarking method does not change the values of the stored data objects. Experimental results showed the feasibility of the proposed method and provide a detailed security analysis and performance evaluation to show that the digital watermarking is robust and can withstand various types of attacks. The KPDF (KPDF team [70]) creator is shown in Fig. 2 for the proposed method of [5].

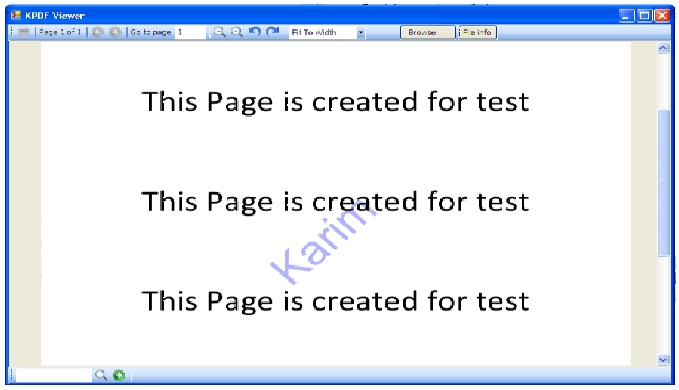
The watermarking methods were presented by Caronni in 1993 [29] for digital images. Since then, DW has been extended to other directions, such as audio and video data. For comprehensive survey about DW methods and techniques, the reader may refer to [22, 52, 64, 67].

Watermarking techniques have been presented in the literature by taking into account the domain in which the watermark is embedded. Watermarking techniques can be divided into two broad categories: spatial domain and frequency domain methods. The watermark is embedded in spatial domain by modifying the values of pixel of the host image. Moreover, watermarking techniques used in the spatial domain directly modify coefficients of images to achieve the purpose for watermarking.

Another important characteristic of DW is that it is a communication security mechanism used to protect intellectual property rights by allowing the owner of a multimedia object to prove that they were the original owners or creators of the object. Watermarking is similar to digital steganographic techniques in that the coded data are hidden in the least significant bits of some larger object [32]. DW may be embedded into, and read from, video, audio and still images to enhance the user experience, facilitate business rules, and enrich the media ecosystem as a whole by allowing all content to be self-identifying or carry information that may trigger a defined behavior [63].



(a) KPDF Creator without watermark Selection (b) KPDF Creator with watermark Selection



(c) KPDF Viewer

Fig. 2 *Embedded and encrypted PDF document.*

There is a difference between DW and pattern matching, such as fingerprinting, since it is not based on statistical techniques versus the databases of known content. In addition, the DW is the equivalent of placing information within the content itself to allow detection in stand-alone or related applications throughout the distribution channel and at play-out. In its most common form, the DW data are not perceptible to the human ear or eye, but can be read by computers. One metric for determining whether the DW is acceptably sound is that, when it is embedded, it cannot be removed out without noticeably degrading the host content.

There are many advantages of adding watermarks to digital contents, such as [54]:

- Ownership Assertion – in order to establish ownership of the content for example, an image.
- Fingerprinting – in order to avoid unauthorized duplication and distribution of publicly available multimedia content.

- Authentication and verification – the authentication is inextricably linked with the content, where the author has a unique key associated with the content and can verify the integrity of this content by extracting the added watermark.
- Content labeling – bits embedded into the data that gives further information about the content, such as a graphic image with time and place information.
- Usage control – there should be control to the number of copies created, where the watermark can be modified by the hardware and to some extent would not create any more copies, such as DVD.
- Protection of contents – contents could be embedded with visible watermark that is very difficult to remove.

The most important properties of any DW techniques are robustness, security, imperceptibility, complexity, and verification. The robustness can be defined as if the watermark can be detected for any reason, such as loss of compression, filtering, or color correction. Security methods must be effective and cannot remove via any targeted attacks. DW can be effectively applied according the criteria given in Tab. I.

Criteria	Digital Watermarking
History	Modern era
Carrier	Image/audio/video/text files
Data hidden	Watermark
Detection	Watermark is needed for recovery
Authentication	Achieved by cross correlation
Objective	Protection of Copyrights
Result	Watermarked file/images
Concern/Problems	Robustness
Type of attacks	Image processing
Visibility	Sometimes
Fails when	It is removed/replaced
Relation to cover	Usually becomes an attribute of the cover image. The cover is more important than the message
Flexibility	Cover choice is restricted

Tab. I *Digital watermarking characteristics.*

In addition, DW techniques can be categorized into different types in various ways. These types are classified according to the following criteria:

a) Watermarking Domain: spatial and frequency

b) Watermarking Document Type: Audio, video, image, and text

c) Watermarking Human Perception: visible and invisible (robust and fragile)

d) Watermarking Applications: source and destination-based

DW does not have the same capability or level of security as data encryption. It does not prevent the viewing or listening of content, nor does it prevent accessing

that content. Therefore, DW is not immune to hacker attacks [58]. The following are some intentional attacks on watermarks as in [15, 17].

- Active Attacks – where hacker tries to remove the watermark or undetected.
- Passive Attacks – hacker tries to determine the watermark and identify it.
- Collusion Attacks – where hacker can use several copies of one piece of media and each one with a different watermark in order to construct a copy with no watermark.
- Forgery Attacks – where hackers try to embed the watermark of their own instead of removing one.
- Distortive Attacks – where hackers use some transformations over the object to degrade the watermark so that it becomes undetectable.

3. Computational Intelligence Methodologies

In this section, we review the core CI approaches that have been proposed to deal with DW problems. We survey RS, FL, ANN, GA, and SI applications in DW. We summarize both individual and hybrid approaches of DW.

3.1 Rough Sets (RS)

Rough set theory was developed by Pawlak as a formal tool for representing and processing information in database [78]. In rough set theory, the data are collected in a table, called decision table. Rows of the decision table correspond to objects, and columns correspond to attributes. In the data set, we assume that the set of examples with a class label to indicate the class to which each example belongs are given. We call the class label the decision attributes, the rest of the attributes the condition attributes.

RS theory defines three regions based on the attribute values: lower approximation, upper approximation and boundary. The lower approximation contains all the objects that are classified on the basis of certain data collected, and the upper approximation contains all the objects that can be classified probably, whereas the boundary is the difference between the upper and lower approximation. Thus, we can define a rough set as any set determined by its lower and upper approximations. On the other hand, the notion of indiscernibility is fundamental to RS theory. Informally, two objects in a decision table are indiscernible if one cannot distinguish between them on the basis of this set of attributes. Explanation of the basic framework of RS theory, along with some of the key definitions and a complete survey of this basic material, can be found in literature [33, 55, 60].

3.2 Fuzzy Logic (FL)

The last decades have witnessed a rapid growth in the number and variety of applications of FL that deal with the vague and imprecise, which is appropriate for DW in watermark embedding and extraction. Robustness of these processes can

be achieved if significant modifications are made to the host image either in spatial or transform domain.

However, such modifications are distinguishable and thus do not satisfy the requirement of transparency or invisibility. For the optimal watermarking application, a trade-off between these two competing criteria (robustness and transparency) has to be made. Therefore, image watermarking can be formulated as an optimization problem. Artificial intelligence techniques, such as FL, have been employed to solve the problem optimally.

A major drawback of clustering method is that it may lose some important information that leads such grouping to become meaningless. To solve this problem, fuzzy cluster analysis uses the membership value for classification of objects. Membership value is ranged from 0 to 1. Many works use fuzzy c-means algorithm for cluster analysis as in [47, 74, 68]. Chen et al. [74] introduced a fuzzy c-means clustering-based fragile watermarking method for image authentication. Wu et al. [47] proposed an alternative c-means clustering algorithms. Lin et al. [68] presented a fuzzy c-means clustering for estimate myocardial ischemia with pulse waveform analysis. Since most existing methods as in [68] require a lot of storage space for cluster analysis. To solve this problem, authors in [68] use fuzzy c-means algorithm to compute the cluster center of each class instead of doing cluster analysis.

Yeh et al. [76] proposed a simple and reliable method named the fuzzy c-means method for classifying the cases of heartbeat from electrocardiogram signals. The proposed method has the advantage of good detection results, no complex mathematical computations, low memory space and low time complexity, which represent the complexity theory. Sakr et al. [69] proposed a novel image watermarking algorithm based on dynamic fuzzy inference system. Chang et al. [18] proposed a fuzzy-ART based adaptive DW approach in DCT domain. Chang et al. [19] presented a robust DWT-based copyright verification technique with fuzzy-ART by combining DWT, fuzzy-ART and the quantization process.

3.3 Artificial Neural Networks (ANN)

ANN is composed of a set of processing units called neurons that are closely interconnected in a given structure. They have been successfully employed in a broad spectrum of data intensive applications.

Yu et al. [59] developed new watermarking techniques based on ANN, integrating both color image processing and cryptography, to achieve content protection and authentication for color images [31]. These watermarking techniques are mainly based on neural networks to further improve the performance of Kutter's technique for color images [50]. Due to neural network learning capability from given learning patterns, the used method can memorize the relations between a watermark and the corresponding watermarked image. This approach can pave the way for developing the watermarking techniques for multimedia data since color images are ubiquitous in the contemporaneous multimedia systems and also are the primary components of MPEG video [35,52].

Chang et al. [13] proposed a full counter-propagation neural network (FCNN) to be applied to copyright authentication, where the watermark is embedded and detected by a specific FCNN. However, in the traditional methods the watermark

is stored in the synapses of the FCNN. In addition to that FCNN has storage and fault tolerance, some attacks do not degrade the quality of the detected watermark image. Moreover, the watermark embedding procedure and detection procedure are integrated into the proposed FCNN. It accomplishes watermark embedding and detection of one or many watermarks using a multi-cover image.

There are many publications about pulse-coupled neural networks (PCNN) [76]. In [76] the current status of the PCNN and the modified models are briefly reviewed. Furthermore, the PCNN applications in image processing, e.g. image segmentation, image enhancement, image fusion, object and edge detection, pattern recognition, etc. are discussed.

Johnson et al. [40] presented a modified PCNN. The PCNN in this work is a single layer, two-dimensional, laterally connected network [66] of integrate-and-fire neurons, with a 1:1 correspondence between the image pixels and network neurons. This is a neural network without any training needed. The output images at different iterations typically represent some segments or edges information of the input image. As a new generation of neural network, the PCNN is has shown effectiveness in digital image processing and applied in other fields, as for example in [11].

3.4 Genetic Algorithms (GA)

GA starts with a collection of randomly selected initial population of chromosomes that encodes a set of possible solutions. In GAs the variables of a given problem can be represented as genes in chromosomes, and the chromosomes can evaluated according to their fitness using some measures of profit or utility that we want to optimize. Recombination involves two genetic operators: crossover and mutation operators. The genetic operators alter the composition of genes to create new chromosomes called offspring.

The parameters in GAs are represented by an encoded binary string called the chromosome. The elements in the binary strings, or the genes, are adjusted to minimize or maximize the fitness value. The fitness function generates its fitness value, which is composed of multiple variables to be optimized by GAs. For each iteration in GA a pre-determined number of individuals will correspondingly produce fitness values associated with the chromosomes.

Shieh et al. [14] presented an innovative watermarking scheme based on GA in the transform domain. It is robust against watermarking attacks, which are commonly described in the literature. In addition, the watermarked image quality is also considered. In this paper, the GA for optimizing both the fundamentally conflicting requirements is employed. Watermarking with GA is easy for implementation. The effectiveness of the proposed scheme has been checked by the fitness function in GA, which includes both factors related to robustness and invisibility.

The purpose of GA is to obtain an optimal solution under several requirements. Shieh et al. [14] selected two conflicting requirements for typical watermarking applications, mainly the watermarked image quality and the robustness of the watermarking algorithm. Simulation results showed both robustness under attacks and improvement in watermarked image quality with GA.

A watermark hidden in an image can be extracted from the original watermark due to the frequently used rounding approach. Shih et al. [28] presented a new method based on GAs in this work to correct the rounding errors. The main idea was to adopt a fitness function for choosing the best chromosome to be able to determine the conversion the rule of real numbers into integers during the cosine transformation. Experimental results in this work showed that the improvements in reducing the errors are successful when GAs are applied in making a decision.

In medical image, the region of interest (ROI) is an area which includes important information and needs be stored without any distortion in order to achieve optimal compression as well as satisfactory visualization of medical images. Shih et al. in [28] showed that the ROI can be compressed by lossless compression. Watermarking skill is often used for protecting medical image in web-based medical information systems. Authors in this work presented a robust technique for embedding the watermark of signature information or textual data around the ROI based on GAs. Experimental results showed that the embedding of watermark in the frequency domain is more difficult to be pirated than in spatial domain.

Darwish et al. [6] presented a securing patient medical images and authentication system to increase the security, confidentiality and integrity of medical images which is transmitted through the Internet, as described in Fig. 3. A public key encryption technique was used to encrypt the patient capturing fingerprint and then embed it into the patient medical image. The fingerprint has been encrypted using the Rivest-Shamir-Adelman (RSA) public-key encryption algorithm. Then, by embedding the encrypted patient's fingerprint using a technique for digital watermarking in the Discrete Cosine Transform (DCT) domain makes the medical image robust to several common attacks. The experimental results on different medical imaging modalities demonstrate the efficiency and transparency of the watermarking system as in Fig. 4.

The RSA technique in this work was used to encrypt the patient fingerprint and then embed it into a patient medical image in the DCT to increase security, confidentiality and integrity of medical imaging transmitted through the Internet. The proposed scheme is able to achieve a tamper assessment rate (TAR) value of less than 13%. The experimental results on different medical imaging modalities demonstrate the efficiency and transparency of the medical image authentication scheme.

3.5 Swarm Intelligence (SI)

SI is an artificial intelligence technique involving the study of collective behavior in decentralized systems [72]. It computationally emulates the behavior of social insects or swarms in order to simplify the design of distributed solutions to complex problems. The behavior refers to the way complex systems and patterns arise out of a multiplicity of relatively simple interactions. In the last few years, SI has been successfully applied to optimization, robotics, and military applications. In this section, we will review its contributions into the DW domain by discussing some swarm motivated research methods

SI approaches intend to solve complicated problems by multiple simple agents without centralized control or the provision of a global model. Local interactions

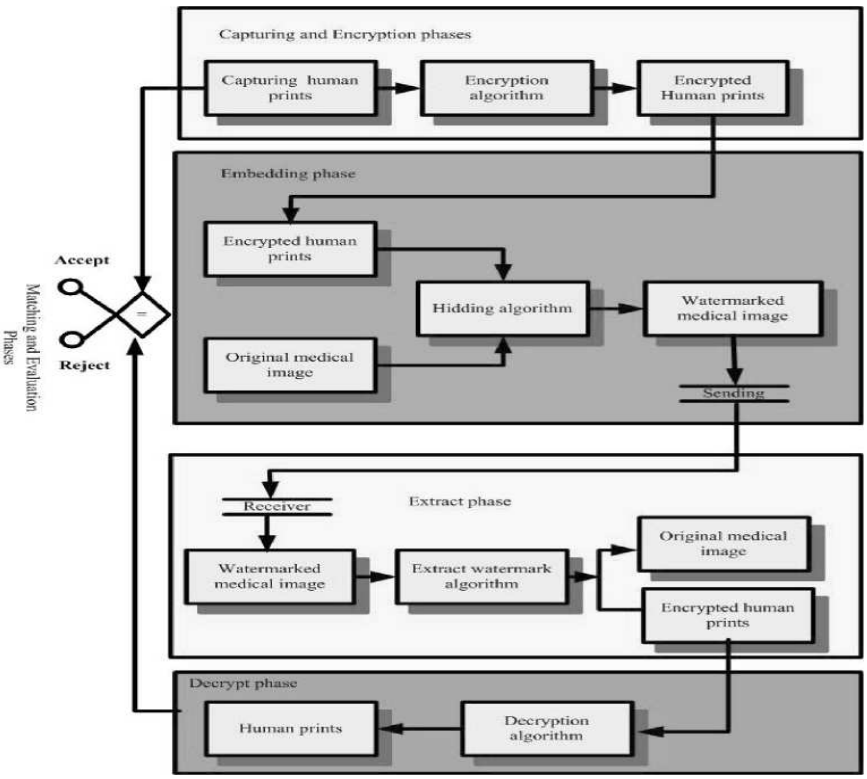
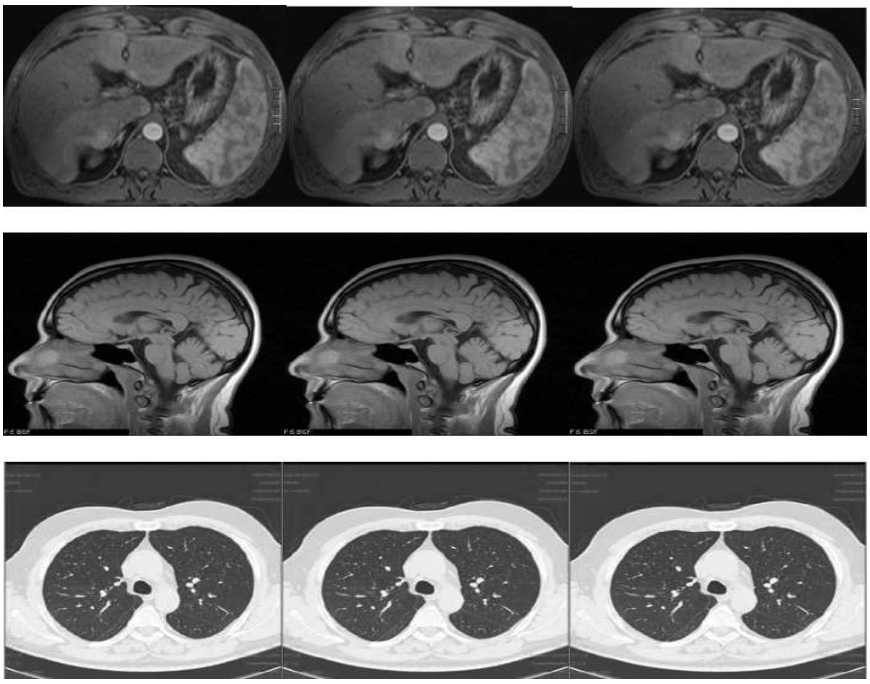


Fig. 3 *Protecting patient medical image system.*

between agents and their environment often cause a global pattern of behavior to emerge. Hence, emergent strategy and highly distributed control are the two most important features of SI, producing a system autonomous, adaptive, scalable, flexible, robust, parallel, self-organizing and cost efficient [49].

The models of SI are population-based. Individuals in the population are potential solutions. These individuals collaboratively search for the optimum through iterative steps. Individuals change their positions in the search space, however, via direct or indirect communications, rather than the crossover or mutation operators in evolutionary computation. There are two popular swarm inspired methods in computational intelligence areas: Ant colony optimization (ACO) [65] and Particle swarm optimization (PSO) [38,77]. ACO simulates the behavior of ants and has been successfully applied to discrete optimization problems; PSO simulates a simplified social system of a flock of birds or a school of fish, and is suitable for solving nonlinear optimization problems with constraints.

The motivation of particle swarm (PS) algorithm is to create a simulation of human social behavior or the ability of human to process knowledge [45, 46]. PS takes into account a population of individuals able to interact with the environment. Thus, population behaviors will emerge from individual interactions. The main idea of PS algorithm is based on searching for solutions to a given problem to learn from



(a) Original (b) Watermarked (c) Extracted

Fig. 4 *Watermarking and extracted results with PSNR=43db.*

their own past experience and from the experiences of others. Individuals evaluate themselves, compare to their neighbors and imitate only those neighbors that are superior to themselves.

4. Hybrid Intelligent Approaches for Digital Watermarking

For comparison of some of individual DW techniques with the hybrid techniques, we have provided an overview of some of the fusion based watermarking methods in this Section to explain the critical role of these hybrid systems as a powerful tool for the DW.

4.1 Artificial Neural Networks and Fuzzy Logic

The fusion of ANNs and FL can exploit the advantages of each technique, where ANNs facilitate the process of automatically developing fuzzy systems by their learning and adaptation capabilities [73]. This combination is called fuzzy neural networks [37]. In addition, fuzzy neural networks systems (FNNS) are represented as a multi-layer feed forward neural network. The neurons in the first layer accept input information. Whereas, the second layer contains neurons which transform

crisp values to fuzzy sets, and output the fuzzy membership degree based on associated fuzzy membership function. Moreover, neurons in the third layer represent the preceding part of fuzzy rule. The last layer performs what is called "defuzzification" and associates the preceding part with a consequent part of a rule. In some cases, more than one "defuzzification" layer is needed. With the same mechanism, the learning methods work to that of ANNs.

According to the errors between output values and target values, membership functions and weights between reasoning layer and defuzzification layer are adjusted. Through learning, fuzzy rules and membership function will be automatically determined. Zhang et al. [10] employed fuzzy neural networks to detect anomalous system call sequences to decide whether a sequence is normal or abnormal. To avoid determining the number of rules before training ANN, the NEFCLASS system has been introduced. The NEFCLASS system is created from scratch and starts with no rule reasoning layer at all. Rules (neurons in the rule reasoning layer) are created by using the reinforcement learning algorithm in the first run through the training data (rule learning). In the second run, a fuzzy back propagation algorithm adapts the parameters of membership functions (fuzzy set learning) [1,8,62].

4.2 Genetic Algorithms and Swarm Intelligence

Recently, the combination of approaches such, as GAs and SI, has been developed to improve the performance of data hiding procedure. Intelligent algorithms, such as GA and particle swarm optimization (PSO), have shown good performances in optimization problems [7, 20]. These intelligent algorithms based watermark techniques can simultaneously improve security, robustness, and image quality of the watermarked images [44]. They also have significant effects on fields where information needs to be protected from attackers at all costs.

Lee et al. [77] developed a hybrid watermarking technique based on GA and PSO. Watermarking technique is to insert copyright information into digital images that the ownerships can be declared. A fundamental problem for embedding watermarks is that the ways of pursuing transparency and robustness are always a trade-off. To solve this problem, a hybrid watermarking technique is proposed to improve the similarity of extracted watermarks. The main idea of the proposed technique is to combine the advantages of PSO and GA, the ability to cooperatively explore the search space and to avoid premature convergence.

Yannis et al. [74] proposed a hybrid algorithmic nature inspired methodology for the effective handling of the vehicle routing problem. The findings of this work showed that the use of an intermediate phase between the two generations, the phase of evolution of the population, will give more efficient individuals and will improve the effectiveness of the algorithm.

5. Threats to Digital Watermarking

We propose a list of attacks against which watermarking system could be judged.

• JPEG compression – JPEG is considered now as one of the most famous used algorithms for image compression and also can be used with any watermarking

system and should be effective to some degree of compression.

• Scaling – As we noticed earlier, this may occur when the image is scanned and printed at a high resolution digital image level in some electronic applications, such as Web publishing. It should not be neglected as we move more and more to Web publishing. Scaling can be divided into two types, uniform and non-uniform scaling. Under uniform scaling we understand scaling which is the same in bot horizontal and vertical direction. However, the non-uniform scaling uses different scaling factors in the horizontal and vertical direction. Very often DW methods are robust only to unprotecting form scaling.

• Deletion of lines or columns – This was our first attack on some copyright marking systems and is very efficient against any straightforward implementation of spread spectrum techniques in the spatial domain. Removing k samples at regular intervals in a pseudo random sequence (-1; 1) (hence shifting the next ones) typically divides by k the amplitude of the cross correlation peak with the original sequence.

• Generalized geometrical transformations – A generalized geometrical transformation is a combination of non-uniform scaling, rotation, and shearing.

• Random geometric distortions – These distortions were detailed in earlier papers [24, 25].

• Geometric distortions of JPEG – rotation and scaling alone are not enough and they must be also tested in combination with compression of JPEG. First, we should apply the geometric transformation and after that we need to save the image in a compressed format so that we can test the robustness of watermarking system to geometric transformation followed by compression. In addition, an exhaustive test should also include the contrary since it might be tried by willful infringers. It will be difficult to choose a quality factor for JPEG as artifacts quickly appear. However, the experience of professionals showed that quality factors down to 70% are acceptable [53].

6. Challenges and Open Problems to Digital Watermarking

Many researchers presented DW challenges and proposed solutions for these issues. Uccheddu [46] introduced a new challenge in DW, which is watermarking of 3D objects or, more simply, 3D watermarking. There is a thesis, discussed this issue [27], which relates to the protection of the intellectual property rights (associated with 3D models). This is considered as a new kind of multimedia that has scored an increasing success. The entertainment industry and scientific world are only some of the main important disciplines in which 3D models are applied. This section overviews some of the crucial challenges of DW.

6.1 Collusion attack

A possible threat to DW schemes arises when the same data are watermarked many times and then distributed. The collusion attack concerns a kind of attack that can be performed by a group of attackers, who sharing their watermarked models,

should be able to remove the watermark keys while preserving the visual integrity of the model.

The collusion attack is an easy to implement attack that aims at removing the watermark. When an unauthorized copy is found, the presence of a particular watermark pattern reveals if a certain code is present or less. Traitors may, however, attempt to escape identification by collectively working to disable the watermark. The lack of security assessment in DW systems has led to critical problems against collusion attacks. Such attacks tend to consider watermarked documents and combine them to create un-watermarked content. This attack is more relevant when the digital data constitute a 3D model.

There are a number of protocols that have been introduced to allow the distribution process of multiple copies of digital watermarked images as in [12]. But there are several obstacles involved with these schemes from the widespread and applicability point of view. Among these problems is what is called Marking Assumption, in which the main property that marks should satisfy is that users cannot change the state of detected mark without rendering the object useless.

6.2 Signal processing collusion

Collusion attacks are feasible. The main idea behind the attack is that DW can usually be interpreted as noise over a spread spectrum. Suppose that multiple watermarked images exist and a number of traitors conspire by using the combination of these images. The spread-spectrum noise embedded by the DW has a certain energy that is deemed an acceptable degradation of the image quality by the creator of the DW [75]. Since the noise can reside anywhere within a predetermined frequency band, it must be presumed that adding noise energy anywhere within this frequency band, while retaining the original noise energy, will also result in an acceptable quality signal. We can easily detect that by averaging the signals that we can obtain a combined signal in which the watermarking noise is cancelled from the watermarked images, and the original image will be emerged.

6.3 Watermarking and

Watermarking technology has been applied to very large systems so that its costs are well understood [64]. A watermarking system requires that watermark embedding be integrated into the production system so there is an up-front cost to adopting watermarking. However, there is little additional cost after implementation, where the overall cost of a watermarking system is fixed and, therefore, amortized over the volume of content produced. As the volume increases, the cost per image decreases.

7. Conclusion

DW based upon CI has recently been attracting considerable interest from the scientific community and researchers. In addition, its characteristics, such as adaptation, fault tolerance, high computational speed and error resilience in the face of noisy data, comply with the requirements of creating a robust DW system.

This paper presents the state-of-the-art in research progress of CI methods in DW systems. The scope of this review is focused on the core methods of DW in CI, including RS, FL, ANNs, GAs and SI with the hybrid of such techniques. However, the practice of these methods reveals that each of them has advantages and disadvantages. Hybrid systems have the power to combine the strengths of these methods in such a way that their disadvantages will be compensated, thus offering better solutions. The contributions of research work in each method are systematically summarized and compared, which allows us clearly to define existing research challenges, and highlight promising new research directions. In addition to DW for digital forensics introduces a new challenge for digital information contents. This paper also presented the challenges facing DW technology. While much progress in recent years has been done in this direction, especially by robustness of embedded watermarking, attackers can still encounter many challenges in this area. However, the introduction of a trusted third party serves as a clearinghouse for watermarked data.

Security in wireless sensor networks has recently caught the attention of the scientific research community with increasing the applications of sensors in use. While the use of strong watermarking techniques have resulted in secured wireless communication.

Digital information can easily be copied and distributed through the Internet and any other media. Therefore, challenges associated with DW require more copyright laws. However, laws cannot be the only entity needed to protect digital products. DW technology with its powerful environment should continue further researches, improvements, and developments. The future of DW will be based on setting standards and creating applications that creators of digital content can easily implement. It is hoped that this survey can serve as a useful guide through most of the relevant literature.

Acknowledgment

The authors would like to thank the anonymous reviewers for their comments and constructive suggestions that have improved the paper. Ajith Abraham is supported by the IT4Innovations Centre of Excellence project, reg. no. CZ.1.05/1.1.00/02.0070 supported by Operational Programme 'Research and Development for Innovations' funded by Structural Funds of the European Union and state budget of the Czech Republic.

References

[1] Hofmann A., Schmitz C., Sick B.: Intrusion detection in computer networks with neural and fuzzy classifiers. In: O. Kaynak, E. Alpaydin, E. Oja, L. Xu (Eds.), Artificial Neural Networks and Neural Information Processing (ICANN/ICONIP'03), **2714** of Lecture Notes in Computer Science, Springer, Berlin/ Heidelberg, 2003, pp. 316-324.

[2] Ahmad I., Shah A., Khan A. N.: Application of neural network model for the prediction of shear strength of reinforced concrete beams, International journal of Non-Standard Computing and Artificial Intelligence, 20, 2010, pp. 667-686.

[3] Lawniczak A. T., Di Stefano B. N.: Computational intelligence based architecture for cognitive agents, Procedia Computer Science, Issue 1, 1, 2010, pp. 2227-2235.

[4] Arit Thammano, Jittraporn Moolwong: A new computational intelligence technique based on human group formation, Expert Systems with Applications, Issue 2, 37, 2010, pp. 1628-1634.

[5] Darwish A., Shamekh K., Kouta M.: Hybrid Portable Document Format Protection Scheme based on Public key and Digital Watermarking, International Journal of Computer Science & Network Security, **2**, 10, In Press, 2010, pp. 97-104.

[6] Darwish A., Hassanien A. E., Tan Q., Pal N. R.: Securing Patients Medical Images and Authentication System based on Public Key Infrastructure, Springer proceeding of advances in intelligent and soft computing, **87**, 2011, pp. 27-34.

[7] Esmin A. A. A., Lambert-Torres G., Alvarenga G. B.: Hybrid evolutionary algorithm based on PSO and GA mutation. In: Proceedings of the Sixth International Conference on Hybrid Intelligent Systems, 2006, pp. 57-63.

[8] Craenen B., Eiben A.: Computational intelligence. Encyclopedia of Life Support Sciences. In: EOLSS, EOLSS Co. Ltd., 2002.

[9] Kosko B.: Fuzzy cognitive maps, International Journal of Man-Machine Studies, **24**, 1, 1986, pp. 65-75.

[10] Zhang B.: Internet intrusion detection by autoassociative neural network. In: Proceedings of International Symposium on Information & Communications Technologies, Malaysia, 2005.

[11] Berkane M., Clarysse P., Njiwa Josiane Y., Zhu Yue M., Magnin I. E.: Neural Network Based Summarizing Method of Periodic Image Sequences, International Journal of Neural Network World, 20, 6, 2010, pp. 687-703.

[12] Boneh D., Shaw J.: Collusion-secure fingerprinting for digital data, Lecture Notes in Computer Science 963, ACM, LNCS, 963, 1995, pp. 452-465.

[13] Chang C.-C., Lin C.-C., Tseng C.-S., Tai W.-L.: Reversible hiding in DCT-based compressed images, Information Sciences, 177, 2007, pp. 2768-2786.

[14] Chin-Shiuh Shieh, Hsiang-Cheh Huang, Feng-HsingWang, Jeng-Shyang Pan: Genetic watermarking based on transform-domain techniques, Pattern Recognition, Elsevier, 37, 2004, pp. 555-565.

[15] Collberg C., Thomborson C.: Software watermarking: Models and dynamic embeddings. Paper presented at the Proceedings of the 26th ACM SIGPLAN-SIGACT on principles of programming languages, San Antonio, Texas, 1999, pp. 20-22.

[16] Corchado E., Grana M., Snasel V., Wozniak M.: Hybrid Artificial Intelligence Systems, International Journal of Neural Network World, Sp. No. 7, 20, 2010, pp. 807-809.

[17] Cox I., Miller M., Bloom J.: Watermarking applications and their properties. Paper presented at the Proceedings of the international conference on information technology: Coding and computing, Las Vegas, Nevada, 2000.

[18] Chang C.-H., Ye Z., Zhang M.-Y.: Fuzzy-ART based adaptive digital watermarking scheme. IEEE Transactions on Circuits and Systems for Video Technology, **15**, 1, 2005, pp. 65-81.

[19] Chang C.-Y., Wang H.-J., Pan S.-W.: A robust DWT-based copyright verification scheme with fuzzy-ART. Journal of Systems and Software, 82, 2009, pp. 1906-1915.

[20] Juang C.-F.: A hybrid of genetic algorithm and particle swarm optimization for recurrent network design, IEEE Trans. Syst. Man Cyber. B 34, 2004, pp. 997-1006.

[21] Poole D., Mackworth A., Goebel R.: Computational Intelligence – A Logical Approach, Oxford University Press, Oxford, UK, ISBN-10:195102703, 1998.

[22] Aucsmith D., editor: Information Hiding: Second International Workshop, **1525** of Lecture Notes in Computer Science, Portland, Oregon, USA. Springer-Verlag, Berlin, Germany, ISBN 3-540-65386-4, 1998.

[23] Dittmann J., Mukherjee A., Steinebach M.: Media independent watermarking classification and the need for combining digital video and audio watermarking for media authentication. Paper presented at the Proceedings of the international conference on information technology: Coding and computing, Las Vegas, Nevada, 2000, pp. 62-67.

[24] Petitcolas F. A. P., Anderson R. J.: Weaknesses of copyright marking systems. In: Dittmann et al., 1998, pp. 55-61.

[25] Petitcolas F. A. P., Anderson R. J., Kuhn M. G.: Attacks on copyright marking systems. In: Aucsmith, ISBN 3-540-65386-4, 1998, pp. 218-238.

[26] Petitcolas F. A. P.: Weakness of existing watermarking schemes. `http://www.cl.cam.ac.uk/ fapp2/watermarking/image_watermarking/`, 1997.

[27] Uccheddu F.: Robust and Imperceptible Watermarking of 3D meshes, Ingegneria Informatica, Multimedialita'e delle Telecomunicazioni, 2007.

[28] Shih F. Y., Yi-Ta Wu: Robust watermarking and compression for medical images based on genetic algorithms, Elsevier, Information Sciences, 175, 2005, pp. 200-216.

[29] Caronni G.: Ermitteln unauthorisierter verteiler von maschinenlesbaren daten. Technical report, ETH Zurich, Switzerland, 1993.

[30] Valentini G., Tagliaferri R., Masulli F.: Computational intelligence and machine learning in bioinformatics, Artificial Intelligence in Medicine, Issues 2-3, 45, 2009, pp. 91-96.

[31] Tsai, H.-H., Yu P.-T.: Adaptive fuzzy hybrid multichannel filters for removal of impulsive noise from color images, Signal Processing, 7, 1999, pp. 127-151.

[32] Tipton H. F., Krause M.: Information Security Management Handbook, CRC Press LLC, 2004.

[33] HE Junhui, HUANG Jiwu: Steganalysis of stochastic modulation steganography, Science in China: Series F Information Sciences, 49, 2006, pp. 273-285.

[34] Hong-ying Yang, Xiang-yang Wang, Tian-xiao Ma: A robust digital audio watermarking using higher-order statistics, AEU – International Journal of Electronics and Communications, In: Press, Corrected Proof, 2010.

[35] Cox I. J., Kilian J., Leighton F. T., Shamoon T.: Secure spread spectrum watermarking for multimedia, IEEE Trans. Image Process, 6, 1997, pp. 1673-1687.

[36] Irigoyen E., Larrea M., Valera J., Gomez V., Artaza F.: A hybridized Neuro-Genetic Solution for Controlling Industrial R-3 Work Space, International Journal of Neural Network World, No. 7, Sp. Iss. SI, 20, 2010, pp. 811-824.

[37] An J., Yue G., Yu F., Li R.: Intrusion detection based on fuzzy neural networks. In: J. Wang, Z. Yi, J. M. Zurada, B.-L. Lu, H. Yin (Eds.), Advances in Neural Networks -Third International Symposium on Neural Networks (ISNN'06), **3973** of Lecture Notes in Computer Science, Springer, Berlin/Heidelberg, 2006, pp. 231-239.

[38] Kennedy J., Eberhart R.: Particle swarm optimization. In: Proceedings of IEEE International Conference on Neural Networks, November/December, IEEE, 4, 1995, pp. 1942-1948.

[39] Strom J., Cosman P. C.: Medical image compression with lossless regions of interest, Signal Process, 59, 1997, pp. 155-171.

[40] Johnson J. L., Ritter D.: Observation of periodic waves in a pulse-coupled neural network, Optical Letter, 18, 1993, pp. 1253-1255.

[41] Patra J. C., Karthik A., Bornand C.: A novel CRT-based watermarking technique for authentication of multimedia contents, Digital Signal Processing, Issue 2, 20, 2010, pp. 442-453.

[42] Patra J. C., Phua J. E., Bornand C.: A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression, Digital Signal Processing, Issue 6, 20, 2010, pp. 1597-1611.

[43] Jongweon Kim, Namgyu Kim, Dongwon Lee, Sungbum Park, Sangwon Lee: Watermarking two dimensional data object identifier for authenticated distribution of digital multimedia contents, Signal Processing: Image Communication, Issue 8, 25, 2010, pp. 559-576.

[44] Pan J.-S., Huang H.-C., Jain L. C.: Intelligent watermarking techniques, World Sci., 2004.

[45] Kennedy J., Eberhart R., Shi Y.: Swarm intelligence. Morgan Kaufmann, 2001.

[46] Kennedy J., Eberhart R.: Particle swarm optimization. In: Proc. of the IEEE Int. Conf. on Neural Networks, Perth, Australia, 4, 1995, pp. 1942-1948.

[47] Wu K. L., Yang M. S.: Alternative c-means clustering algorithms, Pattern Recognition, 35, 2002, pp. 2267-2278.

[48] Cancellaro M., Battisti F., Carli M., Boato G., De Natale F. G. B., Neri A.: A commutative digital image watermarking and encryption method in the tree structured Haar transform domain, Signal Processing: Image Communication, In Press, Corrected Proof, Available online, 26, 2010, pp. 1-12.

[49] Dorigo M.: Optimization, learning and natural algorithms, PhD Thesis, Dipartimento di Elettronica, Politecnico di Milano, Italy (in italian), 1992.

[50] Kutter M., Jordan F., Bossen F.: Digital watermarking of color images using amplitude modulation, J. Electron. Imaging, 7, 1998, pp. 326-332.

[51] Ramadas M., Ostermann S., Tjaden B.: Detecting anomalous network traffic with self-organizing maps. In: Sixth International Symposium on Recent Advances in Intrusion Detection, RAID'03, 2003, pp. 36-54.

[52] Swanson M. D., Kobayashi M., Tewfik A. H.: Multimedia data-embedding and watermarking technologies. Proceedings of the IEEE, 86, 1998, pp. 1064-1087.

[53] Katz M.: Digital watermarks often fail on Web images. The New York Times, 1997.

[54] Memon N., Wong P. W.: Protecting digital media content. Communications of the ACM, 41, 1998, pp. 35-43.

[55] Ning S., Ziarko W., Hamilton J., Cercone N.: Using rough sets as tools for knowledge discovery. In: Fayyad U. M. and Uthurusamy R. (eds.), First International Conference on Knowledge Discovery and Data Mining KDD'95, Montreal, Canada, AAAI, 1995, pp. 263-268.

[56] Williams P. D., Anchor K. P., Bebo J. L., Gunsch G. H., Lamont G. D.: CDIS: towards a computer immune system for detecting network intrusions. In: Fourth International Symposium on Recent Advances in Intrusion Detection, RAID'01, 2001, pp. 117-133.

[57] Wong P. H. W., Au O.-C., Yeung Y.-M.: A novel blind multiple watermarking technique for images, IEEE Trans. Circuit Syst. Video Technol., 13, 2003, pp. 813-830.

[58] Pan-Pan Niu, Xiang-Yang Wang, Hai-Bo Jin, Ming-Yu Lu: A feature-based robust digital image watermarking scheme using bandelet transform, Optics & Laser Technology, Issue 3, 43, 2011, pp. 437-450.

[59] Pao-Ta Yu, Hung-Hsu Tsai, Jyh-Shyan Lin, Digital watermarking based on neural networks for color images, Elsevier, Signal Processing, 81, 2001, pp. 663-671.

[60] Pawlak Z.: Rough sets. International Journal of Computing and Information Sciences, 11, 1982, pp. 341-356.

[61] Pegah Fakhari, Ehsan Vahedi, Caro Lucas, Protecting patient privacy from unauthorized release of medical images using a bio-inspired wavelet-based watermarking approach, Elsevier, Digital Signal Processing, **21**, Issue 3, 2011, pp. 433-446.

[62] Alshammari R., Sonamthiang S., Teimouri M., Riordan D.: Using neuro-fuzzy approach to reduce false positive alerts. In: Fifth Annual Conference on Com- munication Networks and Services Research (CNSR'07), IEEE Computer Society, 2007, pp. 345-349.

[63] Preda R. O., Vizireanu D. N.: A robust digital watermarking scheme for video copyright protection in the wavelet domain, Measurement, Issue 10, 43, 2010, pp. 1720-1726.

[64] Anderson R. J., editor: Information hiding: first international workshop, volume 1174 of Lecture Notes in Computer Science, Isaac Newton Institute, Cambridge, England. Springer-Verlag, Berlin, Germany, ISBN 3-540-61996-8, 1996.

[65] Olariu S., Zomaya A. Y. (Eds.): Handbook of Bioinspired Algorithms and Applications, Chapman & Hall/CRC, ISBN-10: 1584884754, 2006.

[66] Savio A., Charpentier J., Termenon M., Shinn A. K., Grana M.: Neural Classifiers for Schizophrenia Diagnostic Support on Diffusion Imaging Data, International Journal of Neural Network World, No. 7, Sp. Iss. SI. , 20, 2010, pp. 935-949.

[67] Shelly Xiaonan Wu, Wolfgang Banzhaf: The use of computational intelligence in intrusion detection systems: A review, Applied Soft Computing, Issue 1, 10, 2010, pp.1-35.

[68] Lin S. H., Chang K. M., Tyan C. C.: Fuzzy C-means clustering for myocardial ischemia estimation with pulse waveform analysis, Biomedical Engineering - Applications, Basis and Communications, 21, 2009, pp. 139-147.

[69] Sakr N., Zhao J.-Y., Groza V.: A dynamic fuzzy logic approach to adaptive HVS-based watermarking. In: Proceedings of HAVE2005, Ottawa, Ontario, Canada, October, 2005, pp. 121-126.

[70] The KPDF Team, 2008. KPDF Reader. `http://kpdf.kde.org/.`

[71] Duch W.: What is computational intelligence and where is it going? In: W. Duch, J. Mandziuk (Eds.), Challenges for Computational Intelligence, **63** of Studies in Computational Intelligence, Springer, Berlin/Heidelberg, 63, 2007, pp. 1-13.

[72] Wikipedia: `http://en.wikipedia.org/.` Retrieved 26, 2008.

[73] Wilk T., Wozniak M.: Combination of one-class classifiers for multiclass problems by fuzzy logic, Intenational journal of Neural Network World, No. 7, Sp. Iss. SI, 20, 2010, pp. 853-869.

[74] Chen W. C., Wang M. S.: A fuzzy c-means clustering-based fragile watermarking scheme for image authentication, Expert System with Application, 36, 2009, pp. 1300-1307.

[75] Xiang-Yang Wang, Pan-Pan Niu, Hong-Ying Yang: A robust digital audio watermarking based on statistics characteristics, Pattern Recognition, Issue 11, 42, 2009, pp. 3057-3064.

[76] Yun-Chi Yeh, Wen-June Wang, Che Wun Chiou: A novel fuzzy c-means method for classifying heartbeat cases from EGG signals, Elsevier, Measurement 43, 2010, pp. 1542-1555.

[77] Zne-Jung Lee, Shih-Wei Lin, Shun-Feng Su, Chun-Yen Lin: A hybrid watermarking technique applied to digital images, Elsevier, Applied Soft Computing, 8, 2008, pp.798-808.

[78] Zhi-Hui Wang, Chin-Chen Chang, Ming-Chu Li: Optimizing least-significant-bit substitution using cat swarm optimization strategy, Elsevier, Information Sciences, In: Press, Corrected Proof, Available online, 23 July 2010.