Soft Comput
DOI 10.1007/s00500-008-0324-x

FOCUS

Spiking neural network and wavelets for hiding iris data in digital images

Aboul Ella Hassanien · Ajith Abraham · Crina Grosan

Abstract This paper introduces an efficient approach to protect the ownership by hiding the iris data into a digital image for authentication purposes. The idea is to secretly embed an iris code data into the content of the image, which identifies the owner. Algorithms based on Biologically inspired Spiking Neural Networks, called Pulse Coupled Neural Network (PCNN) are first applied to increase the contrast of the human iris image and adjust the intensity with the median filter. It is followed by the PCNN segmentation algorithm to determine the boundaries of the human iris image by locating the pupillary boundary and limbus boundary of the human iris for further processing. A texture segmentation algorithm for isolating the iris from the human eye in a more accurate and efficient manner is presented. A quad tree wavelet transform is first constructed to extract the texture feature. Then, the Fuzzy c-Means (FCM) algorithm is applied to the quad tree in the coarse-to-fine manner by locating the pupillary boundary (inner) and outer (limbus) boundary for further processing. Then, iris codes (watermark) are extracted that characterizes the underlying texture of the human iris by using wavelet theory. Then, embedding and extracting watermarking methods based on Discrete Wavelet Transform (DWT) to insert and extract the generated iris code are presented. The final process deals with the authentication process. In the authentication process, Hamming distance metric that measure the variation between the recorded iris code and the corresponding extracted one from the watermarked image (Stego image) to test weather the Stego image has been modified or not is presented. Simulation results show the effectiveness and efficiency of the proposed approach.

A. E. Hassanien
Department of Quantitative Methods and Information Systems,
College of Business Administration, Kuwait University,
Safat, Kuwait

A. E. Hassanien (✉)
Information Technology Department, FCI,
Cairo University, 5 Ahamed Zewal Street,
Orman, Giza, Egypt
e-mail: aboitcairo@gmail.com; a.hassanien@fci-cu.edu.eg;
abo@cba.edu.kw

A. Abraham
Center for Quantifiable Quality of Service
in Communication Systems, Norwegian University of Science
and Technology, O.S. Bragstads plass 2E,
7491 Trondheim, Norway
e-mail: ajith.abraham@ieee.org; abraham.ajith@acm.org

C. Grosan
Department of Computer Science, Faculty of Mathematics
and Computer Science, Babeş Bolyai University,
Kogalniceanu 1, 3400 Cluj-Napoca, Romania
e-mail: cgrosan@cs.ubbcluj.ro

1 Introduction

The rapid expansion of the Internet and the overall development of digital multimedia content and nonlinear media distribution requires new enabling technologies, beyond traditional approaches such as password-based encryption that are used for safe custody of private keys do not provide adequate security due to very low entropy in user chosen passwords (Jain and Uludag 2003; Wong 1998; Wong and Memon 2001). Biometric-based personal identification techniques that use physiological or behavioral characteristics are becoming increasingly popular compared to traditional token-based or knowledge based techniques such as identification cards (ID), passwords, etc. One of the main reasons for this popularity is the ability of the biometrics technology to differentiate between an authorized person and an

impostor who fraudulently acquires the access privilege of an authorized person (Jain and Uludag 2003; Sekhar et al. 2002).

Data and information hiding technology (Neil et al. 2000) is a commonly used technique that embeds additional messages into the host signals by modifying their original content. These messages can serve as authentication codes, annotation, or secret data depending on the purpose of the application itself. For instance, if it is a case of copyright protection, a robust digital watermarking method would be a good choice; in case it is the security of secret communication that the users are seeking, then image steganography (information hiding) should be taken into consideration (Leea et al. 2008; Celik et al. 2002, 2006; Zhang and Wang 2005). The basic idea in digital watermarking is to embed a watermark signal into the host data for the purpose of copyright protection, access control, broadcast monitoring, fingerprinting, broadcast monitoring, image authentication, etc. (Chang et al. 2002). A watermark can be a tag, label, digital signal or biometric human print such as iris, signature, etc. A host may be multimedia object such as an image, audio or video.

Digital watermarking allows the user to add a layer of protection to the images by identifying copyright ownership and delivering a tracking capability that monitors and reports where the user's images are being used. Copyright protection of owner is becoming more elusive as computer networks such as the global Internet are increasingly used to deliver electronic documents. Document distribution by network offers the promise of reaching vast numbers of recipients. It also allows information to be tailored and preprocessed to meet the needs of each recipient. However, these same distribution networks represent an enormous business threat to information providers—the unauthorized redistribution of copyrighted materials (Brassil et al. 1999; Nikolaidis and Pitas 1996; Petitcolas 2000). Adding a unique marking to a document can serve many purposes.

This paper introduces an efficient approach to protect the ownership by hiding an iris data into digital image for an authentication purpose. The idea is to secretly embed an iris code data into the content of the image, which identifies the owner. Algorithms based on Biologically inspired Spiking Neural Networks, called Pulse Coupled Neural Network (PCNN) are first applied to increase the contrast of the human iris image and adjust the intensity with the median filter. It is followed by the PCNN segmentation algorithm to determine the boundaries of the human iris image by locating the pupillary boundary and limbus boundary of the human iris for further processing. A texture segmentation algorithm for isolating the iris from the human eye in a more accurate and efficient manner is presented. A quad tree wavelet transform is first constructed to extract the texture feature. Then, the Fuzzy c-Means (FCM) algorithm is applied to the quad tree in the coarse-to-fine manner by locating the pupillary boundary (inner) and outer (limbus) boundary for further processing. Then, iris codes (watermark) are extracted that characterizes the underlying texture of the human iris by using wavelet theory. Then, embedding and extracting watermarking methods based on Discrete Wavelet Transform (DWT) to insert and extract the generated iris code are presented. Finally, the last process deals with the authentication process. In the authentication process, Hamming distance metric that measure the variation between the recorded iris code and the corresponding extracted one from the watermarked image (Stego image) to test weather the Stego image has been modified or not is presented.

Rest of the paper is organized as follows. Section 2 gives a brief introduction to digital watermarking, wavelet theory, and Biologically inspired spiking neural network used the proposed approach. Section 3 discusses the proposed watermarking system in detail, including the authentication approach. Experimental results are discussed in Sect. 4. The paper is concluded in Sect. 5.

2 Related research and preliminary background

2.1 Digital watermarking

Digital watermarking or simply watermarking, which is defined as embedding information such as origin, destination, access level, etc., of multimedia data (e.g., image, video, audio, etc.) in the host data, has been a very active research area in recent years (Jain and Uludag 2003; Cox et al. 2001, 1997; Cox and Miller 2002; Wolfgang and Delp 1996). It is descendent of a technique known as steganography, which has been in existence for at least a few hundred years (Hsu and Wu 1999; Podilchuk and Delp 2001; Hassanien 2005; Hassanien and Jafar 2003). Steganography is a technique where a secret message is hidden within another unrelated message and then communicated to the other party. Some of the techniques of steganography like use of invisible ink, word spacing patterns in printed documents, coding messages in music compositions, etc., have been used by military intelligence since the times of ancient Greek civilization (Hsu and Wu 1999).

Watermarking can be considered as a special technique of steganography where one message is embedded in another and the two messages are related to each other in some way. The most common examples of watermarking are the presence of specific patterns in currency notes, which are visible only when the note is held to light and logos in the background of printed text documents. The watermarking techniques prevent forgery and unauthorized replication of physical objects. Digital watermarking is similar to watermarking physical objects except that the watermarking technique is used for digital content instead of physical objects.

In digital watermarking a low-energy signal is imperceptibly embedded in another signal. The low-energy signal is called watermark and it depicts some metadata, like security or rights information about the main signal. The main signal in which the watermark is embedded is referred to as cover signal since it covers the watermark. The cover signal is generally a still image, audio clip, video sequence or a text document in digital format.

The purpose of watermarks is twofold:

- They can be used to determine ownership;
- They can be used to detect tampering.

There are two necessary features that all watermarks must possess. First, all watermarks should be detectable. In order to determine ownership, it is imperative that one be able to recover the watermark. The steganographic system uses the shared secret to determine how the hidden message should be encoded in the redundant bits. Modern steganography attempts to be detectable only if secret information is known-namely, a secret key (Fabien et al. 1995). This is similar to Kerckhoffs' Principle in cryptography, which holds that a cryptographic system's security should rely solely on the key material (Provos and Honeyman 2003; Kerckhoffs 1883). For steganography to remain undetected, the unmodified cover medium must be kept secret, because if it is exposed, a comparison between the cover and stego media immediately reveals the changes.

The baseline structure of digital watermarking is given in Fig. 1. The digital watermarking system essentially consists of a watermark encoder and a watermark decoder. The watermark encoder inserts a watermark onto the host signal and the watermark decoder detects the presence of watermark signal. Note that an entity called watermark key (shared secret key) is used during the process of embedding and detecting watermarks. The watermark key has a one-to-one correspondence with watermark signal and it is private and known to only authorized parties and it ensures that only authorized parties can detect the watermark. Further, note that the communication channel can be noisy and hostile and hence the digital watermarking techniques should be resilient to both noise and security attacks. A comprehensive discussion on information hiding and watermarking can be found in Fabien et al. (1995), Zhang and Wang (2005), Hartung and Kutter (1999), Lee and Jung (2001), and Potdar et al. (2005).

2.2 Wavelet transform

The fundamental idea behind wavelets is to analyze the signal at different scales or resolutions, which is called multiresolution (Shen 2003; Yang et al. 2007; Stephane 1989). Wavelets are a class of functions used to localize a given signal in both space and scaling domains. A family of wavelets can be constructed from a mother wavelet. Compared to Windowed Fourier analysis, a mother wavelet is stretched or compressed to change the size of the window. In this

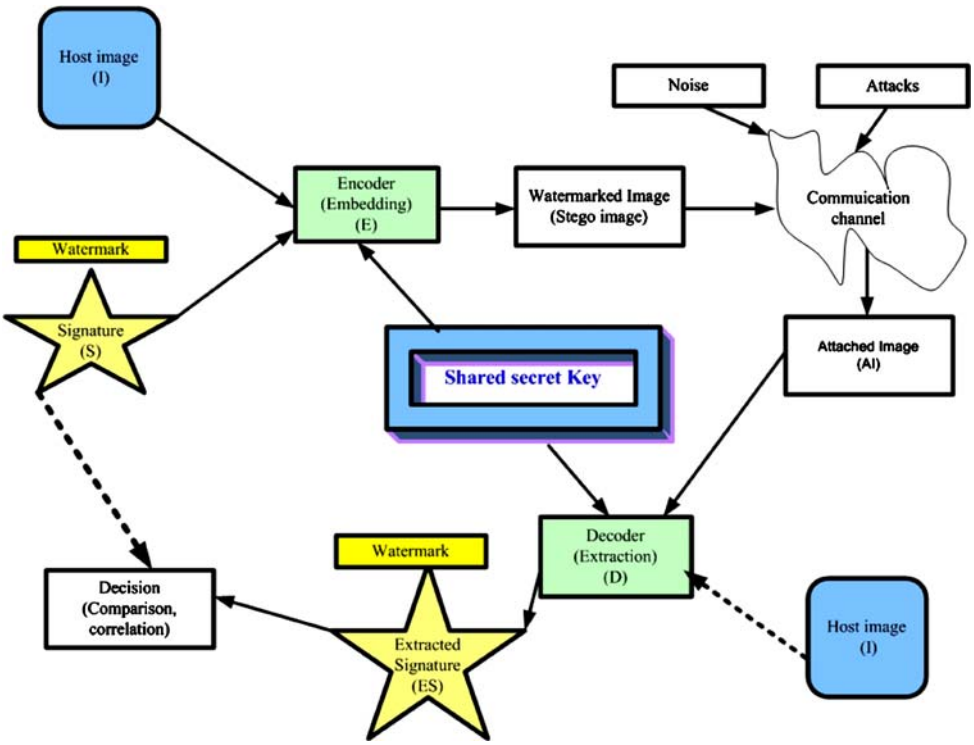

Fig. 1 The baseline structure of digital watermarking

way, big wavelets give an approximate image of the signal, while smaller and smaller wavelets zoom in on details. Therefore, wavelets automatically adapt to both the high-frequency and the low-frequency components of a signal by different sizes of windows. Any small change in the wavelet representation produces a correspondingly small change in the original signal, which means local mistakes will not influence the entire transform. The wavelet transform is suited for nonstationary signals, such as very brief signals and signals with interesting components at different scales (Hubbard 1995). Wavelets mean small waves that segments data into different frequency components and transfer each component with different resolution that is matched to its scale. The main idea of wavelet analysis is to see both coarse and detail data without heavy computational penalty. The goal of most modern wavelet researches is to create a set of basis functions and transform them in order to give an information.

The wavelet transform (WT) decomposes a signal $f(t)$ by performing inner products with a collection of analysis function $\psi(a, b)$, which are scaled and translated version of the wavelet ψ. The wavelet coefficient $W(a, b)$ of the function $f(t)$ is defined as follows:

$$W(a,b) = \langle f, \psi_{(a,b)} \rangle = \int_{-\infty}^{+\infty} f(t)\psi_{(a,b)}(t)dt \tag{1}$$

$$\psi_{(a,b)}(t) = a^{-1/2}\psi\left(\frac{t-b}{a}\right) \tag{2}$$

It refers to the degree of similarity between the basis functions (wavelet) and the original signal at the current scale. The amplitude of the WT therefore tends to be maximum at those scales and locations where the signal most resembles the analysis template. The continuous wavelet transform is a reversible transform, $f(t)$, which can be restored using the following:

$$f(t) = \frac{1}{C_\psi}\int_0^{\infty}\int_{-\infty}^{+\infty}\frac{1}{\sqrt{a}}W(a,b)\left(\frac{x-b}{a}\right)\frac{dbdb}{a^2} \tag{3}$$

where C_ψ is a constant depends on the choice of the wavelet, $a > 0$ is the scale parameter and b is the position parameter.

When the scale a varies, the filter ψ is only reduced or dilated, while keeping the same pattern (Stephane 1989). The reconstruction is only possible if C_ψ is defined by admissibility condition (Coifman et al. 1990), which restricts the class of functions that can be wavelet.

Wavelet Packet Transform (WPT) is a generalization of the Dyadic Wavelet Transform (DWT) that offers a rich set of decomposition structures (Stephane 1989). A WPT corresponds to a general tree-structured filter bank. It allows more flexibility by providing good spectral and temporal resolutions in arbitrary regions of the time–frequency plane. Tree-structured wavelet packet decomposition is used to classify image textures. The main idea of the WPT is based on the fact that most natural textures can be modeled as quasi-periodic signals with the most significant information texture often appearing in the middle frequency channels. An appropriate way to perform the wavelet transform for textures is to detect the significant frequency channels and, then, to further decompose them. This leads to a new type of wavelet transform called a tree-structure wavelet transform or a quad-tree wavelet transform. This type of transform can be achieved by using a maximum criterion of textural measures to locate the dominant information in each frequency channels and decide whether a decomposition is needed for a particular output. Reader may consult Stephane (1989), Helal et al. (2004), Coifman et al. (1990), and Meyer (1993) for more fundamental details on texture analysis based on wavelet packet transform. Figure 2 illustrates the channel representation and quad-tree wavelet transform. The quad-tree structure is shown where the subimage in channel D_1, B_1, C_1 does not contain any significant information and, therefore, they are not expanded further (Helal et al. 2004).

2.3 Pulse coupled neural network

Pulse-Coupled Neural Networks (PCNNs) (Hassanien 2006) are neural networks that are based on cat's visual cortex and developed for high-performance biomimetic image processing. Eckhorn et al. (1988, 1990) and Eckhorn (1999) introduced a neural model to emulate the mechanism of cats' visual cortex. The Eckhorn model provided a simple and effective tool for studying small mammals' visual cortex and was soon recognized as having significant application potential in image processing. In 1994, Eckhorn model was adapted to be an image processing algorithm by Johnson who termed this algorithm Pulse-Coupled Neural Network (PCNN).

A PCNN is a two-dimensional neural network. Each neuron in the network corresponds to one pixel in an input

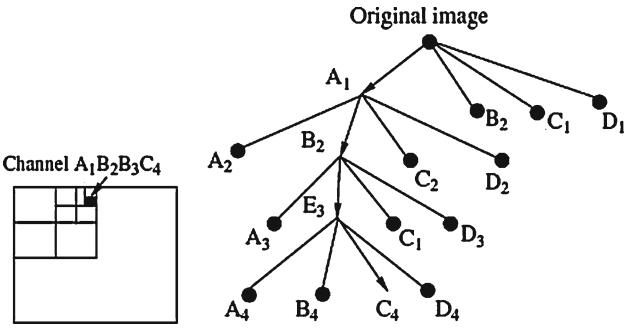

Fig. 2 Channel representation and quad-tree wavelet transform (Helal et al. 2004)

image, receiving its corresponding pixel's color information (e.g., intensity) as an external stimulus. Each neuron also connects with its neighboring neurons, receiving local stimuli from them. The external and local stimuli are combined in an internal activation system, which accumulates the stimuli until it exceeds a dynamic threshold, resulting in a pulse output. Through iterative computation, PCNN neurons produce temporal series of pulse outputs. The temporal series of pulse outputs contain information of input images and can be utilized for various image processing applications, such as image enhancement and segmentation (Hassanien 2006). PCNN model is comprised of four parts that form the basis of the neuron. The first part is the feeding receptive field that receives the feeding inputs (i.e., image pixel values); the second part is the linking receptive field that receives the linking inputs from the neighbor neurons; the third part is modulation field, which the linking input added a constant positive bias, then it is multiplied by the feeding input; the last part is a pulse generator that consists of an output pulse generator and a threshold spike generator. When PCNN is applied to image processing, one neuron corresponds to one pixel. Figure 3 depicts the layout structure of PCNN and its components.

3 Hiding iris data into digital images system

In general, the process of hiding biometric human iris data into digital cover images system includes four main phases: (Pre-processing, Iris code extraction, watermarking, and authentication). These four phases are described in detail in the following section along with the steps involved and the characteristics feature for each phase. Figure 4 illustrates the overall layout structure of the introduced framework for hiding iris data into digital cover images.

3.1 Pre-processing phase

Human iris characteristics

Human iris has many features that can be used to distinguish one iris from another. One of the primary visible characteristic is the trabecular meshwork, a tissue which gives the appearance of dividing the iris in a radial fashion that is permanently formed by the eighth month of gestation. During the development of the iris, there is no genetic influence on it, a process known as chaotic morphogenesis that occurs during the seventh month of gestation, which means that even identical twins have differing irises. The iris has in excess of 266 degrees of freedom, i.e., the number of variations in the iris that allow one iris to be distinguished from another. The fact that the iris is protected behind the eyelid, cornea and aqueous humor means that, unlike other biometrics such as fingerprints, the likelihood of damage and/or abrasion is minimal. The iris is also not subject to the effects of aging, which means it remains in a stable form from about the age of one until death. The use of glasses or contact lenses (colored or clear) has little effect on the representation of the iris and hence does not interfere with the recognition technology. Figure 5 shows examples of the iris pattern and they demonstrate the variations found in irises.

Human iris acquisition process

Human iris can be captured using a standard camera in both visible and infrared light and may be either a manual or automated procedure. The camera can be positioned between

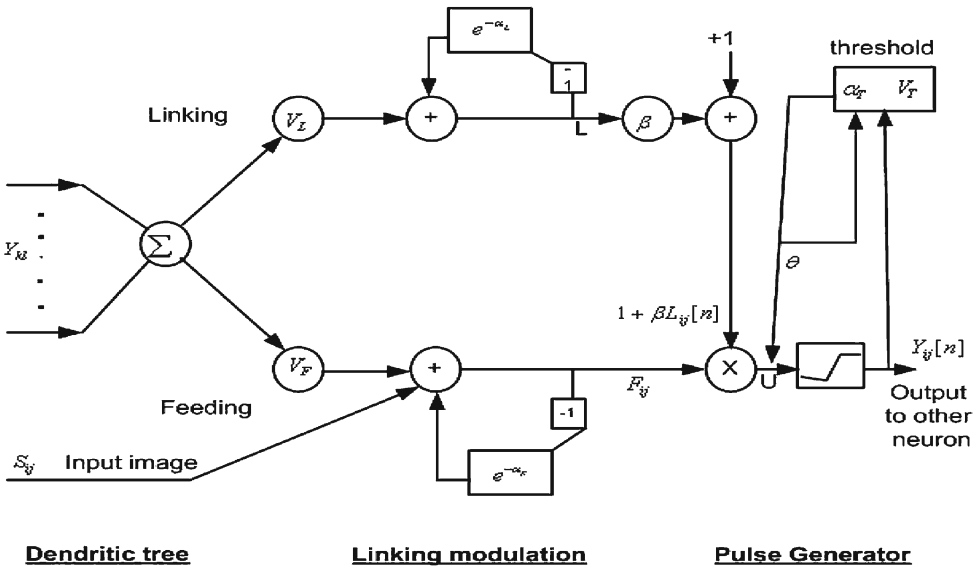

Fig. 3 The layout structure of PCNN and its components (El-dahshan et al. 2007)

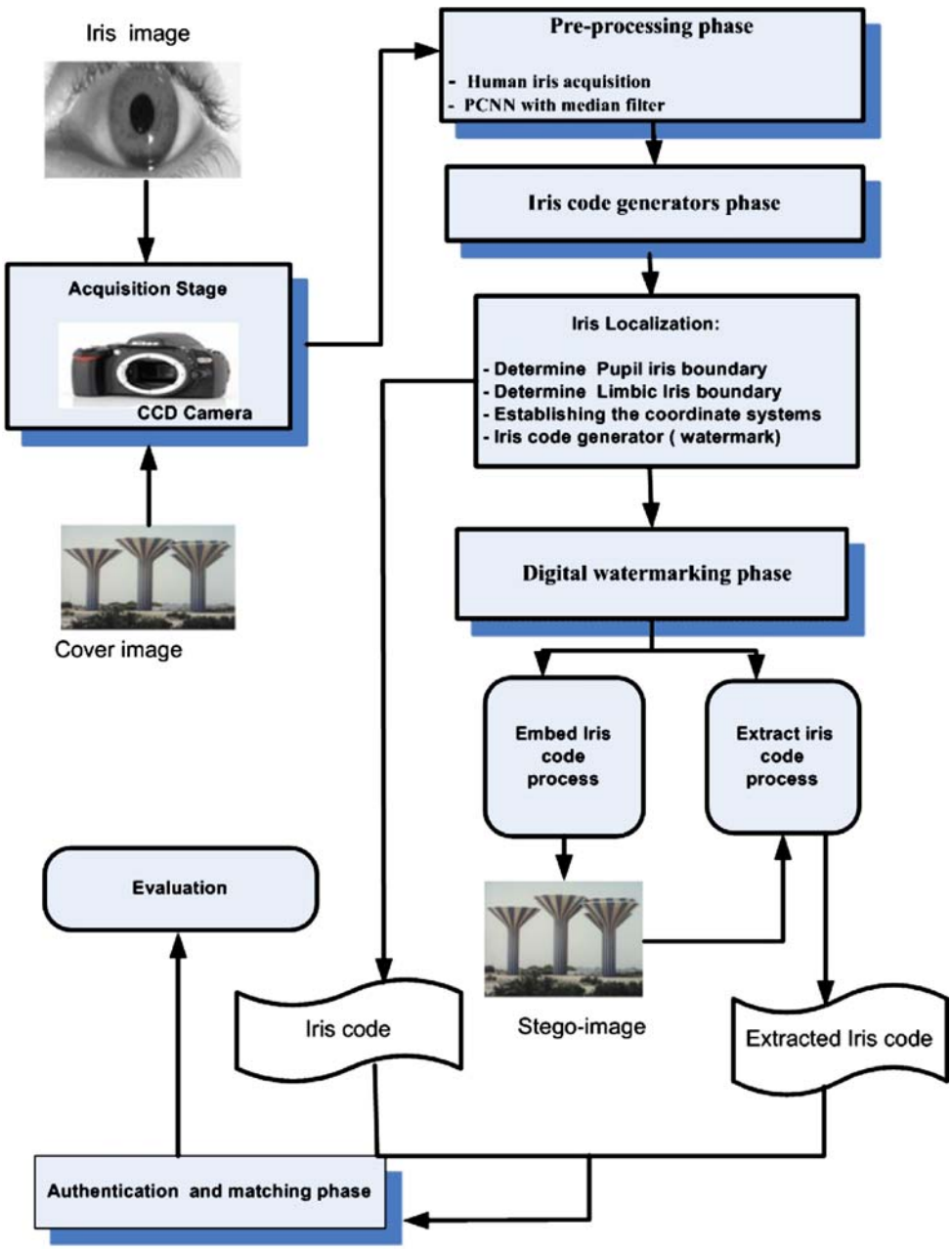

Fig. 4 The hiding iris data into cover image scheme

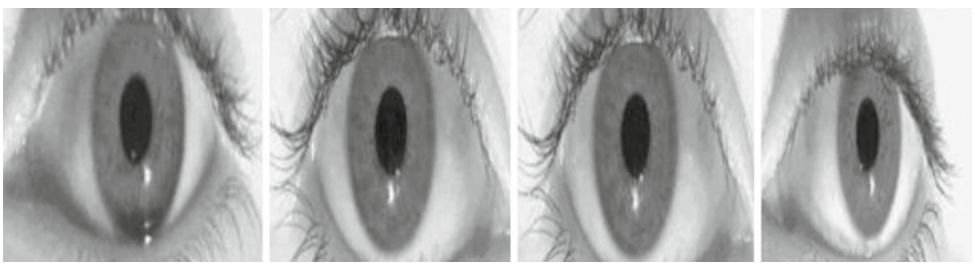

Fig. 5 Samples of human iris patterns

three and a half inches and one meter to capture the image. In the manual procedure, the user needs to adjust the camera to get the iris in focus and needs to be within six to twelve inches of the camera. This process is much more manually intensive and requires proper user training to be successful. The automatic procedure uses a set of cameras that locate the face

and iris automatically thus making this process much more user friendly.

One of the major challenges in automated iris recognition systems is to capture a high quality image of the iris while keeping the procedure noninvasive. Given that the iris is a relatively small (1 cm in diameter), dark object and that people are very sensitive about their eyes, this matter required careful engineering. The following points should be of concern:

- It is desirable to acquire images of the iris with sufficient resolution and sharpness to support recognition;
- It is important to have a good contrast in the interior iris pattern without increasing the level of illumination that annoys the operator;
- The images should be well framed (i.e., centered);
- Noise in the acquired images should be eliminated as much as possible.

Figure 6 illustrates the used device configuration for acquiring human eye images. The human eye should be offset by nine centimeters from the camera, as shown in Fig. 6. The halogen lamp is fixed to get the same illumination effect over all images, thus excluding the illuminated part from the iris while making the iris code easier. To acquire more clear images through a CCD camera and minimize the effect of the reflected lights caused by the surrounding illumination, we arrange the two halogen lamps as the surrounding lights and they should be in front of the eye.

Human iris intensity adjustment: PCNN with the median filter

To increase efficiency of automating the boundary detection process, a pre-processing process should be considered to enhance the quality of the captured human eye images before isolating the iris pattern. The median filter (El-dahshan et al. 2007) is used to reduce noise in an image. It operates one pixel in the image at a time and looks at its closest neighbors to decide whether or not it is representative of its surroundings. To begin with, one should decide the size of the window that the filter operates the image within. The size could, for example, be set to three, which means that the filter will operate on a centered pixel surrounded by a frame of 3×3 neighbors. Then the filter sorts the pixels contained in the image area surrounded by the window. The center pixel will be replaced by the median, the middle value, of the ranking result. The advantage of the median filter, compared with other smoothing filters of similar size, is that it performs noise-reduction with considerably less blurring. Thus, the filter also preserves the edges in an image very well. The median filter works especially well for random noise. The algorithm works as follows: it first finds out the concrete position of the noised pixel according to the firing pattern and then removes the noise from the image with median filter. Initially the threshold of all of the neurons is set to zero, and at the first iteration all the neurons are activated which means all neurons receive the maximal linking input at the next iteration. So the proper set of the SNN's parameters will make the neurons corresponding to noised pixels with high intensity fire before its neighborhood at the second iteration, and according to the current firing pattern the concrete position of noised pixels

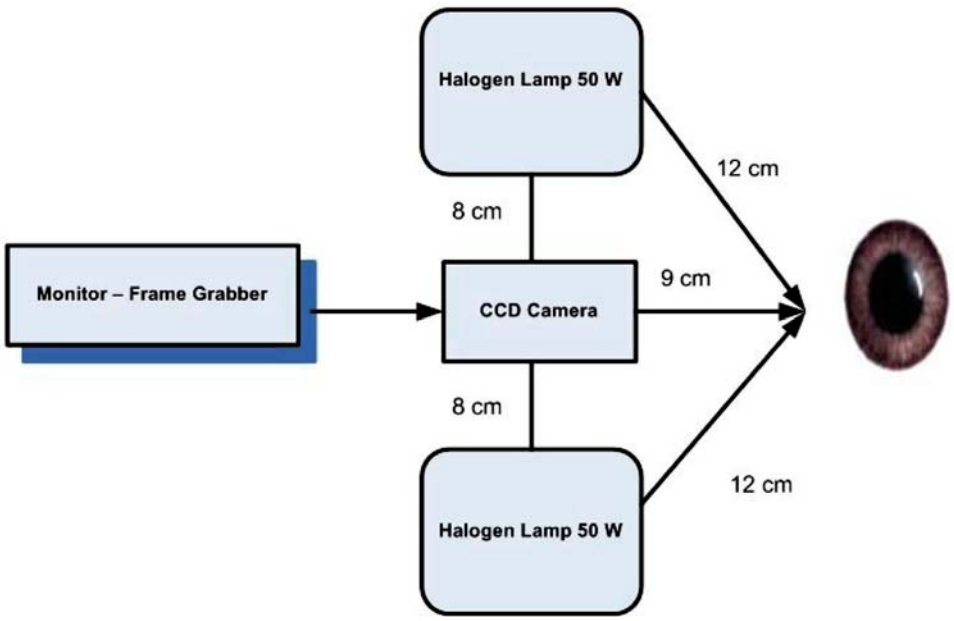

Fig. 6 Configuration of the used image acquisition device

can be found out. Then the noised pixels can be removed with 3×3 median filter. The removal of noised pixels with low intensity is the same as the removal of noised pixels with high intensity if the intensity is inverted. Due to the fact that this algorithm can find out the concrete positions of noised pixels and apply median operation only on the noised regions, its ability to keep the details of the image is strong, for more details, reader may consult (El-dahshan et al. 2007).

Determine pupil and limbic iris boundaries

The success of the application of PCNNs to image segmentation depends on the proper setting of the various parameters of the network, such as the linking parameter β, threshold θ, decay time constants α_θ, and the interconnection matrices M and W (Hassanien 2006). Proper setting of the parameters is especially important when intensity significantly varies across a single segment. The PCNN segmentation work as follows: An input gray-scale image is composed of $M \times N$ pixels. This image can be represented as an array of $M \times N$ normalized intensity values. Then the array is fed in at the $M \times N$ inputs of PCNN. If initially all neurons are set to 0, the input results in activation of all of the neurons at the first iteration. The threshold of each neuron, Θ, significantly increases when the neuron fires; then the threshold value decays with time. When the threshold falls below the respective neuron's potential (U), the neuron fires again, which again raises the threshold. The process continues creating binary pulses for each neuron. While this process goes on, neurons encourage their neighbors to fire simultaneously in a way that is supported through interconnections. The firing neurons begin to communicate with their nearest neighbors, which in turn communicate with their neighbors. The result is an autowave that expands from active regions. Thus, if a group of neurons is close to firing, one neuron can trigger the group. Due to connections between the neurons, the pulse activity of invoked neurons leads to the synchronization between groups of neurons corresponding to subregions of the image that have similar properties and produces a temporal series of binary images, for more details we refer to Helal et al. (2004). Figure 7 depicts the output PCNN enhanced and boundaries contours around iris and pupil pattern of the human eye based on the PCNN.

3.2 Iris code extraction phase

Isolating human iris process

We presents a texture segmentation algorithm for isolating the iris from the human eye in a more accurate and efficient manner. A quad tree wavelet transform is first constructed to extract the texture feature (Chen and Lin 2006). Then, the FCM algorithm (Hassanien 2007) is then applied to the quad tree with the coarse-to-fine manner. This approach has a hierarchical structure and consists of two steps: texture feature extraction followed by clustering process.

During the first step, we can extract the texture feature of the image by generating the Q-level tree-structured wavelet transform. First, we decompose the root image into four subimages using the low pass h and high pass g filters. Then, we compute the feature as local energies using Gaussian weighting in a square window. If the local energy of a subimage is greater than the others, then this subimage is used as a separated root node and is decomposed into four further subimages at the lower resolution. The decomposition is repeated until the minimal size of the subimage is exceeded. In the second step, we accumulate all features from the child nodes in level Q as vector values based on the FCM algorithm. We use these segmentation results at the lowest level when segmenting the next higher level of resolution (i.e., level Q–1). This means that, at the next finer resolution (Q–1), we use the membership function that we had from the coarser resolution (level Q) as a good initial start for the fuzzy clustering algorithm; for more details we refer to Helal et al. (2004).

Establishing coordinate systems and iris code generator

The iris code generator works as follows: It starts by acquiring the eye image from the digital camera. Then, by utilizing the eye image, the boundary between the pupil and the iris

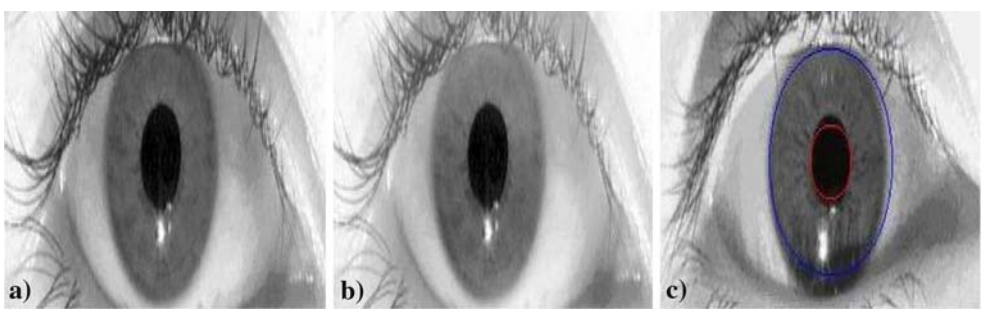

Fig. 7 Determination of iris and pupil boundaries (Hassanien 2006). **a** Original human eye, **b** PCNN enchanced result, **c** iris and pupil boundaries

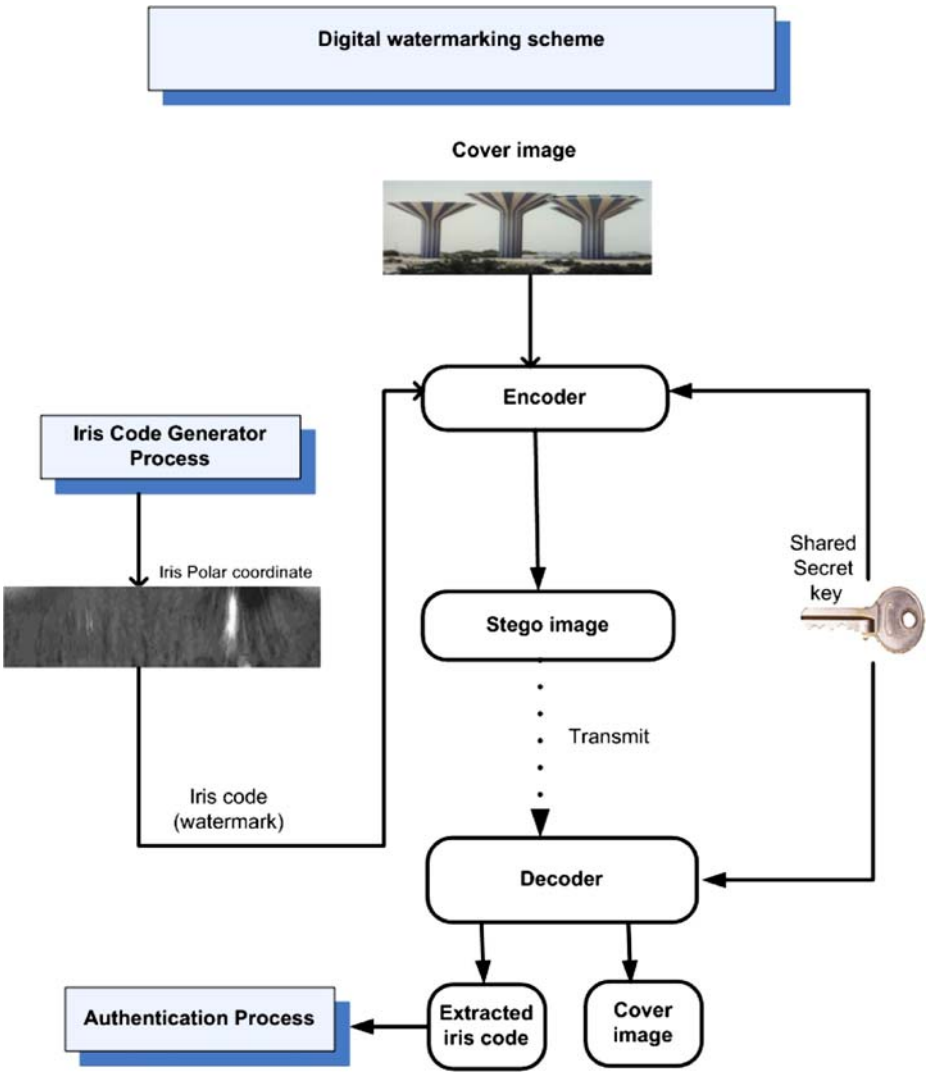

Fig. 8 Digital watermarking phase

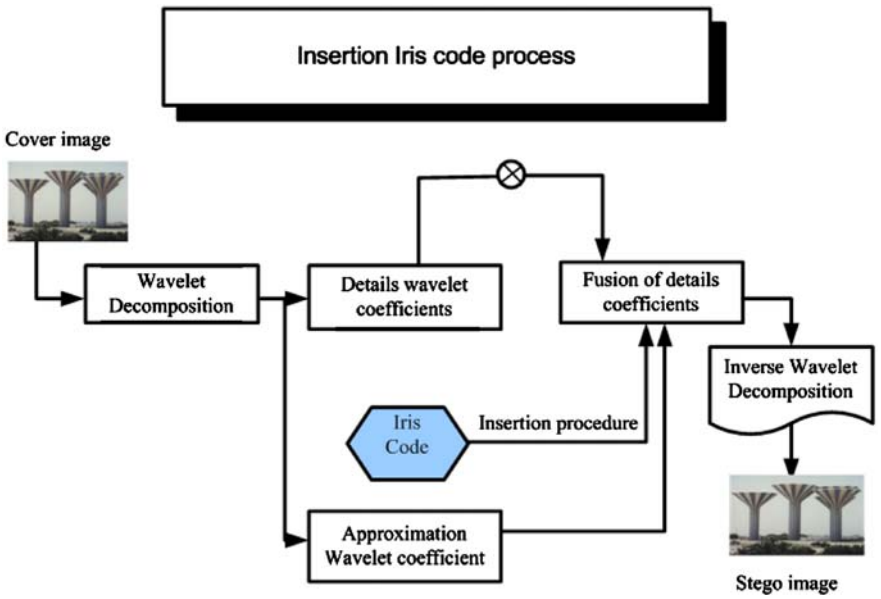

Fig. 9 The embedded watermark process

Algorithm 1 Watermark embedded algorithm

Input: f be the cover image of size $M_1 \times M_2$,
$W_I \in \{-1, 1\}$ be the iris code watermark, and Shared secret key.

Output: Watermarked image *i.e* Stego image

Processing

1: Initialize key pseudo-random number generator with shared secret key
2: Produce the approximation and details coefficients of the original image f
3: Generate a random key
which will be used to select the exact locations in the wavelet domain in which, to embed the watermark, the key has a corresponding value of one or zero (i.e., to indicate if the coefficient is to be marked or not, respectively). The number of ones in the key must be greater or equal to the size of the watermark.
4: **for** each coefficient within the wavelet domain **do**
5: **if** The length of the watermark $\leq$ to the number of ones in the key **then**
6: Embed the watermark into the detail wavelet coefficients of the host image with the key as follows:
7: Sort the detail coefficients in ascending order so that $f_{k1,l}(m,n)$, $f_{k2,l}(m,n)$, $f_{k3,l}(m,n)$ are coefficients such that:

$$f_{k1,l}(m,n) \leq f_{k2,l}(m,n) \leq f_{k3,l}(m,n) \quad (4)$$

Where $k1 \neq k2 \neq k3 \in \{H, V, D\}$ and $f_{kl(m,n)}$ is the kth detail image component at the Lth resolution level of the host image and $\{H, V, D\}$ represents the horizontal, vertical and details coefficients, respectively.
8: **end if**
9: **end for**
Quantization Process
The middle wavelet coefficient $f_{k2,l}(m,n)$ must be quantized to embed the watermark. The range of values between $f_{k1,l}(m,n)$, $f_{k3,l}(m,n)$ is divided into bins of width using the following equation:

$$\Delta = \frac{f_{k3,l}(m,n) - f_{k1,l}(m,n)}{2Q - 1} \quad (5)$$

Where Q a user-defined variable and $f_{k2,l}(m,n)$ is quantized to the nearest value.
We have to note that, in this case an attacker cannot easily determine the exact key given a watermarked image if the specific wavelet transform used in the decomposition is kept a secret and Q is unknown.
10: The fused image components are computed to form the watermarked image using the corresponding Lth level inverse wavelet transform

Algorithm 2 Watermark extracted algorithm

Input: cover image, stego-image *i.e.*, attacked image, shared secret key

Output: Original image and Iris code (watermark)

Processing

1: Apply L^* level Discrete Wavelet Transform (DWT) on the watermarked image;
2: Use the shared secret key to find the locations in which the watermark was embedded for each resolution level
3: Sort the detail coefficients in ascending order
4: Estimate the watermark bit value from the relative position of details coefficients
5: Finding the closest quantized value using the same constant Q {*Which determining if this quantized value was used to embed a one or a negative one.*}
6: **if** The watermark had been embedded in different locations several times **then**
7: The most common bit value extracted is assigned for the estimated watermark
8: **end if**
9: **if** An equal number of ones and negative ones were extracted **then**
10: A random guess is made to its value
11: **end if**
12: Compute the correlation coefficients (CC) between the original iris code watermark and the extracted one
13: **if** The CC is above a pre-specified threshold **then**
14: A given watermark iris code is detected
15: **end if**

is detected after the position of the eye in the given image is localized. After the center and the radius of the pupil are extracted, the right and the left radius of the iris are searched based on these data. By using the iris center and the radius, which are calculated in advanced step, we set the polar coordinate system (Hassanien and Jafar 2003). In this coordinate system, the feature of the iris is extracted. We call it an iris code. Wavelet transforms; especially Haar wavelet is used to extract iris code from iris images. The wavelet transform breaks an image down into four sub-sampled, or images. The results consist of one image that has been high pass in the horizontal and vertical directions, one that has been low passed in the vertical and high passed in the horizontal, and one that has been low pass filtered in both directions. This transform is typically implemented in the spatial domain by using 1-D convolution filters g. The results of wavelet transform is composed of the following four types of coefficients:

- Coefficients that result from a convolution with g in both directions (HH) represent diagonal features of the image;
- Coefficients that result from a convolution with g on the columns after a convolution with h on the rows (HL) correspond to horizontal structures;
- Coefficients from high pass filtering on the rows, followed by low pass filtering of the columns (LH) reflect vertical information;
- The coefficients from low pass filtering in both directions are further processed in the next step.

Where, H and L refer to the high pass and low pass filters, respectively and HH means that the high pass filter is applied to signals of both directions. For more details, please refer to Hassanien and Jafar (2003) and Hassanien (2005).

3.3 Digital watermarking phase

Research into human perception indicates that the retina of the eye splits an image into several frequency channels each

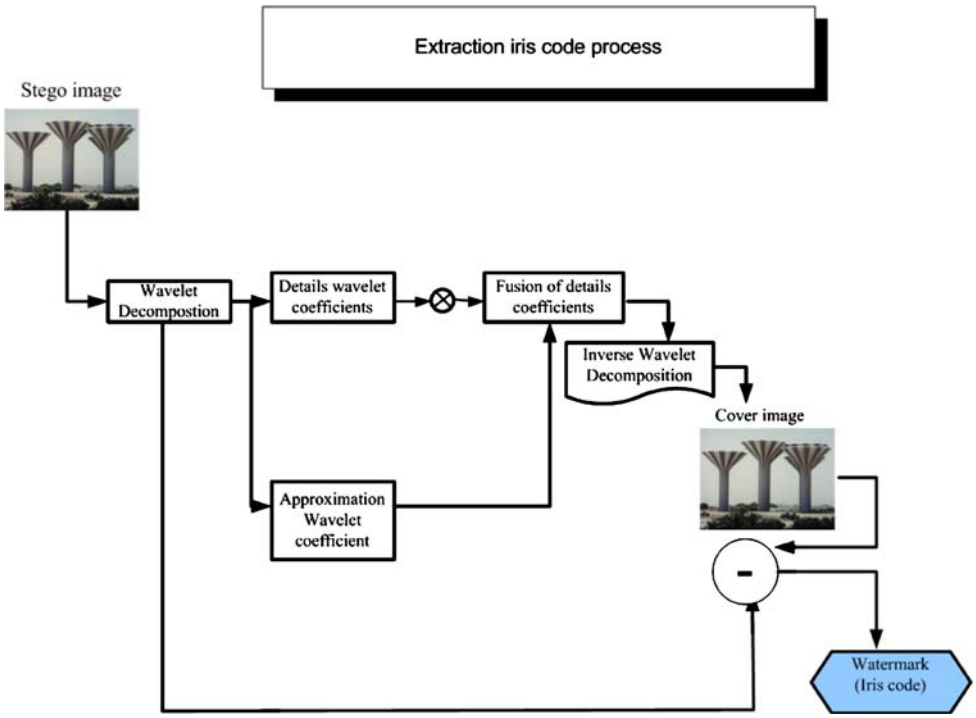

Fig. 10 The detected watermark process

spanning a bandwidth of approximately one octave. The signals in these channels are processed independently. Similarly, in multiresolution decomposition, the image is separated into bands of approximately equal bandwidth on a logarithmic scale. It is therefore expected that the use of the DWT will allow the independent processing of the resulting components without significant perceptible interaction between them, and hence making the process of imperceptible marking more effective. Since digital watermarking involves the merging of a watermark with a host signal, it follows that wavelets are attractive for the watermarking of images. The technique is *unsupervised* since the original image (cover image) is not required for watermark extraction (Hassanien and Jafar 2003; Hassanien 2005; Wang et al. 2002).

In this section, we shall present the technical details of the proposed technique, whose embedding and extracting iris code (watermark) into cover images. Figure 8 illustrates the digital watermarking phase.

Iris code embedded algorithm

In the embedded algorithm, we first decompose an image into several bands with a pyramid structure and then pseudo-random sequence is added to the large coefficients, which are not located in the lowest resolution. The original image and digital watermark are represented as:

$$f = \{f(i, j), 0 \leq i \leq M_1, 0 \leq j < M_2\} \quad (6)$$

$$W_I = \{w(i, j), 0 \leq i \leq N_1, 0 \leq j < N_2\} \quad (7)$$

where $f(i, j) \in \{0, 1, \ldots, 2^L - 1\}$ is the intensity of pixel (i, j) and L is the number of bits used in each pixel, $w(i, j) \in \{0, 1\}$. To find the perceptually significant wavelet coefficients for each sub-band, the threshold value is calculated according to the decomposition level. For example, in the 3-level decomposition, the largest coefficients C_1 for 1-level sub-bands (LH_1, HL_1, HH_1) is selected and the threshold T_1 is calculated by Eq. (8). T_2 and T_3 for the subsequent levels are respectively calculated using the same process (Hassanien 2005).

$$T_i = 2^{\log_2 C_i - 1} \quad (8)$$

where i is the decomposition level and represents the largest integer which is not greater than X.

DWT watermark embedded algorithm is composed of four parts: cover image; calculation of multi-level thresholds for selecting perceptually significant coefficients; watermark insertion process; and inverse wavelet decomposition (IWT) of the coefficients with watermarks. Figure 9 illustrates the watermark embedded process.

The main steps of the embedded watermarking algorithm are provided below [refer to Algorithm (1)].

3.4 Extract iris code algorithm

The aim of the watermark extraction process is to reliably obtain an estimate of the original watermark from a possibly distorted version of the watermarked image. The detection process is an inverse procedure of the watermark insertion process. It requires knowledge of the watermarked image

Algorithm 3 Authentication and matching algorithm

Input : Two iris code watermarks A_i, B_j

Output : Authentication result (accept/reject)

Processing

1: **for** j=1 to 87 **do**
2: Comparing bit by bit code with the first code
3: **if** The result of the XOR is 0 **then**
4: Count the number of zeros
This means the 2 bits are the same
5: **Else**
6: Do not count it and continue to the next bit
7: **end if**
8: **end for**
9: Calculating the similarities (matching) ratio by using the following formula:

$$R = \frac{N_z * 100}{T_n} \tag{9}$$

Where N_z and T_n are the number of zero's and total number of bits in each code, respectively; R is a matching ratio.
10: **if** A_i and A_j are equal **then**
11: The watermark is verified
12: **Else** The marked image has been modified
13: **end if**

and the shared key. One of the advantages of wavelet-based watermarking is its ability to spread the watermark all over the image. If a part of the image is cropped, it may still contain parts of the watermark. These parts of watermark may be detected by certain mechanism even if the image has been further scaled or rotated. Figure 10 illustrates the watermark extracting process.

The main steps of the extracted watermarking algorithm are provided in Algorithm (2).

3.5 Authentication and matching phase

Authentication (sometimes called verification) is when a comparison of newly captured biometric data is made against a stored template to find a match. This method is a one-to-one matching method where the verification situation craves that you are you, not in comparison to anyone else. In the verification procedure the extracted iris code watermark is used as an operator acting on the fresh iris print. If the match is approved, the authentication of the person is completed.

Finally, the iris code of the watermarked image is extracted and compared with the original iris code obtained from the cover watermarked image. If the two sequences of the iris codes match perfectly, the system concludes that the image has not been modified after watermarking; otherwise, the system determines the instants associated to the nonmatching, which correspond the approximate locations where the image has been corrupted. Identical iris codes slightly shifted in time are considered to match, since such shifts may occur when the image is submitted to content-preserving transformations. Comparison of Iris code records includes calculation of a Hamming distance (HD) (Hassanien and Jafar 2003; Kagan et al. 1998), as a measure of variation between the Iris code recorded from the presented iris and each iris code extracted from the watermarked image. Let A_i and A_j be two iris codes watermarks to be compared, the Hamming distance function can be calculated as:

$$HD = \frac{1}{87}\Sigma_1^{87} A_i \oplus B_j \tag{10}$$

where $\oplus$ denotes exclusive-OR operator (the exclusive-OR is a Boolean operator that equals one if and only if the two bits A_i and A_j are different). The main steps of the authentication and matching procedure is given in Algorithm-3:

4 Results and discussion

In this section, some experimental results are demonstrated to show the effectiveness and the robustness of the proposed watermarking algorithm. Several 256 × 256 test images are used for the simulations including Lena, Cameraman, Baboons and water tower images. Each human iris image is preprocessed to form a block of texture and the texture image is decomposed using a 2D two-scale wavelet transform into four subimages. In our experiments, the energy distribution feature used as the textural measure gives the maximum value and always appears in the low-frequency channel. In addition, we use a four-tap Daubechies wavelet filter that has a regularity property, which projected most of the important structural information in the image into a low-frequency subimage.

After determining the center point of the human iris (Helal et al. 2004), we find the inner boundary and the outer boundary by extending the radius of a virtual circle from the center of pupil and counting the number of points of the edge on the corresponding virtual circle. Two virtual circles with the maximum number of points of the edge within each corresponding range determined by some prior knowledge are selected as the two boundaries that we want to find. Figure 11 shows the center of the pupil and the iris part surrounded by two boundaries. It obvious that the drawing circles are almost coincident with the actual pupil and iris of the original image of the eye.

The localized iris part from the image is transformed into polar coordination system in an efficient way so as to facilitate the next process, the feature extraction process. The portion of the pupil is excluded from the conversion process because it has no biological characteristics at all. The distance between the inner boundary and the outer boundary is normalized into [0, 65] according to the radius r that matches the pupillary and limbus boundaries.

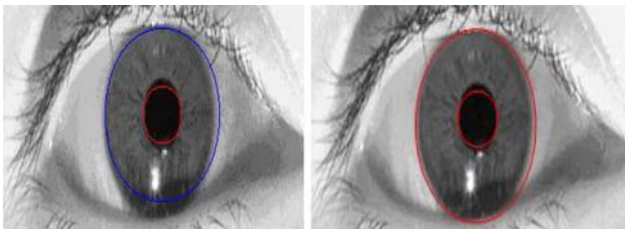

Fig. 11 Results locating the iris and pupil boundaries

Figure 12 illustrates the isolated iris and pupil pattern results from the human eye using the fuzzy c-mean clustering algorithm. Figure 12a depicts the isolated iris and pupil patterns, while Fig. 12b shows the isolated iris pattern. Figure 13 illustrates the isolated pupil pattern.

Figure 14 shows the process of converting the Cartesian coordinate system into the polar coordinate system for the iris part. It is used to extract the iris code (watermark) of the iris print. For the 450 × 60 iris image in polar coordinates, we apply wavelet transform 4-times in order to get the 28 × 3 sub-images (i.e., 84 features). By combining these 84 features in the HH sub-image of the high-pass filter of the fourth transform ($HH4$) and each average value for the three remaining high-pass filters areas ($HH1$, $HH2$, $HH3$), the dimension of the resulting feature vector is 87. Each value of 87 dimensions has a real value between −1.0 and 1.0. By quantizing each real value into binary form by convert the positive value into 1 and the negative value into 0. Therefore, we can represent an iris image with only 87 bits.

Figure 15 shows the water tower cover image and the watermarked image (stego-image), respectively. We see that the stego-image is not distinguishable from the cover image. The watermark length (iris code) is 750 bits.

To evaluate the quality between the attacked image, i.e, stego-image and the original cover image, Fig. 16 illustrates the Peak Signal-to-Noise Ratio (PSNR) of stego-images embedded in levels 1, 2 and 3. As evident, when the PSNR value of a stego-image is greater than 30 dB, the quality is still acceptable to the human eyes. PSNR often requires the existence of the original image, which is often not convenient for the receiver. So, we introduce a new metric that measure

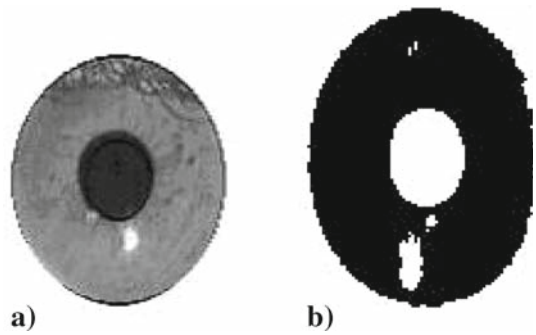

Fig. 12 Results locating the isolated iris and pupil patterns. **a** Iris and pupil pattern, **b** Isolating the iris pattern

Fig. 13 Results illustrating the isolated pupil pattern. **a** Pupil isolated result, **b** Isolated pupil after enhancement

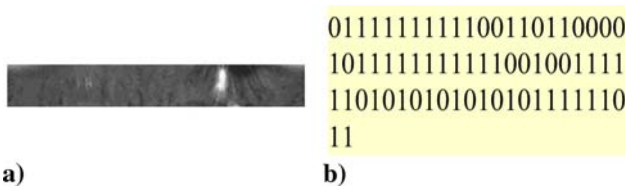

Fig. 14 Polar transformed result. **a** Polar transformed results, **b** A part of the generated iris code

Fig. 15 Cover image—stego image. **a** Water tower cover image, **b** Water tower stego image

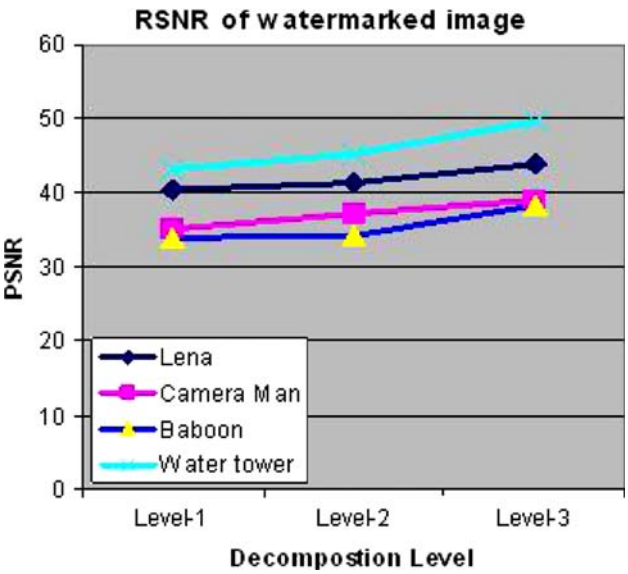

Fig. 16 PSNR of watermarked images embedded in levels 1, 2 and 3

Table 1 Correct rate under the JPEG compression

Image	CR
Lena	0.9775
Cameraman	0.9271
Baboon	0.8862
Water tower	0.9439

the objective quality of the image based on the detected watermark bit. A quality estimation parameter, named the Correct Rate (CR) is computed as an index to the objective quality of the image.

Table 1 depicts the correct rate CR of three tested cover images using JPEG compression. It shows that the proposed method is very effective for predicting the effect on image quality of JPEG compression. The correct rate is calculated by:

$$CR = \frac{NC}{TN} \tag{11}$$

where NC is the number of correctly detected watermarked bits and TN is the total number of watermark bits.

5 Conclusions, future research and challenges

Conclusions

Digital watermarking is an important emerging technique for copyright protection and authentication. The objective of this research is to illustrate how Biologically inspired Spiking Neural Network (SNN) can be successfully integrated with wavelet theory and provide a more effective hybrid approach to resolve security problems. In this paper, we have presented a model to protect the ownership by hiding a human iris data into a digital image for an authentication purpose. The idea is to secretly insert an iris code data into the content of the image, which identifies the owner. Algorithms based on Biologically inspired Spiking Neural Networks (SNN) are first applied to increase the contrast of the iris image and adjust the intensity with the median filter. It is followed by the PCNN segmentation algorithm to determine the boundaries of the human iris image by locating the pupillary boundary and limbus boundary of the human iris for further processing. Then, iris codes are extracted characterizing the underlying texture of the human iris by using the wavelet theory. Finally, embedding and extracting methods based on wavelet transform (DWT) to embed and extract the generated iris code are presented. The last phase deals with the authentication. A distance metric that measure the objective quality of the watermarked image based on the detected watermark bit (iris code) is introduced, which the original unmarked image is not required for watermark detection. Experimental results clearly indicate that the model considered could represent the authentication of the ownership very accurately.

Future research

A combination of various computational intelligence (CI) technologies in information security and, in particular, information hiding and watermarking has become one of the most promising avenues in information security. From the perspective of rough sets, further explorations into possible hybridization of rough sets with other CI technologies are necessary to build a more protected multimedia content. What can be said at this point is that the rough set approach paves the way for new and interesting avenues of research in information hiding and represents an important challenge for CI researchers. Our future works will focus on building a fully integrated rough neural network system in information hiding and fingerprinting of multimedia data. In addition, method for biometric-based authentication in wireless communication for access control will be our future works too.

Challenges

Recently, some work on information-hiding and watermarking capacity has been presented (Zhang et al. 2008; McEliece et al. 1987). Most of the previous works on information-hiding used the information theoretic model, and the research focuses on the maximum amount of information that can be hidden in an image, or the upper limit of hidden information. Determining the lower limit of information hiding, or the minimum detectable information capacity is also an interesting problem. The neural network and rough sets based information-hiding capacity can be applied in almost all information-hiding scenarios, such as Covert Channels, Steganography, Anonymity and Copyright Marking. Copyright Marking and Fingerprinting can benefit from the minimum detectable information capacity based on neural network and rough sets.

In image watermarking area, the robustness against desynchronization attacks, such as rotation, translation, scaling, row or column removal, cropping, and local random bend, is still one of the most challenging issues in information hiding area (Yang 2008).

User verification systems that use a single biometric indicator often have to contend with noisy sensor data, restricted degrees of freedom, nonuniversality of the biometric trait and unacceptable error rates. Attempting to improve the performance of individual matchers in such situations may not prove to be effective because of these inherent problems. Multibiometric systems seek to alleviate some of these drawbacks by providing multiple evidences of the same identity. These systems help to achieve an increase in performance

that may not be possible using a single biometric indicator. Further, multibiometric systems provide anti-spoofing measures by making it difficult for an intruder to spoof multiple biometric traits simultaneously. However, an effective fusion scheme is necessary to combine the information presented by multiple domain experts (Ross and Jain 2003). Neural network based information-hiding can be applied in almost all information-hiding scenarios, such as Covert Channels, Steganography, Anonymity and Copyright Marking. Copyright Marking and Fingerprinting can benefit from the minimum detectable information capacity based on neural network.

References

Aslantas V (2008) A singular-value decomposition-based image watermarking using genetic algorithm. Int J Electron Commun 62: 386–394

Brassil JT, Low S, Maxemchuk NF (1999) Copyright protection for the electronic distribution of text. Proc IEEE 87(7): 1181–1196

Celik MU, Sharma G, Saber E, Tekalp AM (2006) Lossless watermarking for image authentication: a new framework and an implementation. IEEE Trans Image Process 15:1042–1049

Celik MU, Sharma G, Saber E, Tekalp AM (2002) Hierarchical watermarking for secure image authentication with localization. IEEE Trans Image Process 11: 585–595

Chang CC, Hwang KF, Hwang MS (2002) Robust authentication scheme for protecting copyrights of images and graphics. IEE Proc Vis Image Signal Process 149: 43–50

Chen P-Y, Lin H-J (2006) A DWT based approach for image steganography. Int J Appl Sci Eng 4(3): 275–290

Coifman R, Meyer Y, Quake S, Wickerhauser V (1990) Signal processing and compression with wave packets Numerical Algorithms Research Group. Yale University, New Haven, CT

Cox IJ, Miller ML (2002) The first 50 years of electronic watermarking. EURASIP JASP 2: 126–132

Cox IJ, Kilian J, Leighton T, Shamoon TG (1997) Secure spread spectrum watermarking for multimedia. IEEE Trans Image Process 6(12): 1673–1687

Cox IJ, Miller ML, Bloom JA (2001) Digital watermarking. Morgan Kaufmann, Menlo Park

Eckhorn R, Bauer R, Jordan W, Brosch M, Kruse W, Munk M, Reitboeck HJ (1988) Coherent oscillations: a mechanism of feature linking in the visual cortex. Biol Cybern 60: 121–130

Eckhorn R, Reitboeck HJ, Arndt M (1990) Feature Linking via Synchronization among Distributed Assemblies: Simulations of Results from Cat Visual Cortex.. Neural Comp 2: 293–307

Eckhorn R (1999) Neural mechanisms from visual cortex suggest basic circuits for linking field models. IEEE Trans Neural Netw 10: 464–479

El-dahshan E, Redi A, Hassanien AE, Xiao K (2007) Accurate detection of prostate boundary in ultrasound images using biologically inspired spiking neural network. In: International Symposium on Intelligent Siganl Processing and Communication Systems Proceeding, Nov. 28–Dec. 1, 2007. Xiamen, China, pp 333–336

Hartung F, Kutter M (1999) Multimedia watermarking techniques. Proc IEEE 87: 1079–1107

Hassanien AE, Jafar MA (2003) An iris recognition system to enhance E-security environment based on wavelet theory. Adv Model Optim J 5(2): 93–104

Hassanien AE (2005) Watermarking algorithm for copyright protection using discrete wavelet transform. In: Proceedings of the 8th International Conference on Pattern Recognition and Information Processing (PRIP'05), May, 18–20, Minsk, Belarus

Hassanien AE (2006) Pulse coupled neural network for detection of masses in digital mammogram. Neural Netw World J 2/06: 129–141

Hassanien AE (2007) Fuzzy-rough hybrid scheme for breast cancer detection. Image Comput Vision J 25(2): 172–183

Helal MA, HassanienAE Taha E-A, Nahla E-H (2004) An efficient texture segmentation algorithm for isolating Iris pattern based on wavelet theory. Int J Pattern Recognit Image Anal 14(1): 97–103

Hsu C-T, Wu J-L (1999) Hidden digital watermarks in images. IEEE Trans Image Process 8(1): 58–68

Hubbard BB (1995) The world according to wavelets. A K Peters Wellesley, Massachusetts

Jain AK, Uludag U (2003) Hiding biometric data. IEEE Trans Pattern Anal Mach Intell 25(11): 1494–1498

Kagan FG, Leblebici Y, Mlynek D (1998) A compact high-speed hamming distance comparator for pattern matching applications. http://turquoise.wpi.edu

Kerckhoffs A (1883) La Cryptographie Militaire (Military Cryptography). J Sci Militaires (J. Military Science, in French), Feb. 1883

Lee SJ, Jung SH (2001) A survey of watermarking techniques applied to multimedia. In: Proceedings of IEEE international symposium on industrial electronics, Pusan, Korea, pp 272–277

Leea C-C, Wub H-C, Tsaic C-S, Chud Y-P (2008) Adaptive lossless steganographic scheme with centralized difference expansion. Pattern Recognit 41: 2097–2106

Mallat SG (1989) A theory for multi-resolution signal decomposition: the wavelet representation. IEEE Trans Pattern Anal Mach Intell II(7):674–693

McEliece R, Posner C, Rodemich R, Santosh R (1987) The capacity of the Hopfield associative memory. IEEE Trans Inform Theory 33(4): 461–482

Meyer Y (1993) Wavelets: algorithms & applications. SIAM, Philadelphia

Neil FJ, Zoran Dc, Sushil J (2000) Information hiding: steganography and watermarking—attacks and countermeasures. Kluwer, Dordrecht

Nikolaidis N, Pitas I (1996) Copyright protection of images using robust digital signatures. In: Proceedings of ICASSP'96, Atlanta, Georgia, May, pp 2168–2171

Petitcolas FAP, Anderson RJ, Kuhn MG (1995) Information hiding: a survey. Proc IEEE, special issue on protection of multimedia content 87(7):1062–1078

Petitcolas FAP (2000) Watermarking schemes evaluation. IEEE Signal Process 17(5): 58–64

Podilchuk CI, Delp EJ (2001) Digital watermarking: algorithms and applications. IEEE Signal Process Mag, pp 33–46

Potdar VM, Han S, Chang E (2005) A survey of digital image watermarking techniques. In: Proceedings of IEEE third international conference on industrial informatics, INDIN05, pp 709–16

Provos N, Honeyman P (2003) Hide and seek: an introduction to steganography. IEEE Secur Priv 1(3): 32–44

Ross A, Jain A (2003) Information fusion in biometrics. Pattern Recognit Lett 24: 2115–2125

Sarukkai SR, Zhang DD (2002) Biometric solutions for authentication in an E-World. Springer, Berlin

Shen J (2003) A note on wavelets and diffusions. J Comp Anal Appl 5: 147–159

Wang Y, Doherty JF, Van Dyck RE (2002) A Wavelet-based watermarking algorithm for ownership verification of digital images. IEEE Trans Image Process 11(2): 77–88

Wolfgang RB, Delp EJ (1996) A watermark for digital images. Proc ICIP' 96(3): 219–222

Wong PW, Memon N (2001) Secret and public key image watermarking schemes for image authentication and ownership verification. IEEE Trans Image Process 10(10): 1593–1601

Wong PW (1998) A public key watermark for image verification and authentication. IEEE Int Conf Image Process 1: 455–459

Yang M, Trifas M, Bourbakis, Cushing C (2007) A Robust Information Hiding Methodology in Wavelet Domain. Signal and Image Processing, SIP 2007. Honolulu, USA Proceeding

Yang C-H (2008) Inverted pattern approach to improve image quality of information hiding by LSB substitution. Pattern Recognit. http://www.sciencedirect.com. Accessed 9 Feb 2008

Zhang X, Wang S (2005) Steganography using multiple-base notational system and human vision sensitivity. IEEE Signal Process Lett 12: 67–70

Zhang F, Pan Z, Cao K, Zheng F, Wu F (2008) The upper and lower bounds of the information-hiding capacity of digital images. Inform Sci. doi:10.1016/j.ins.2008.03.011