Sādhanā Vol. 39, Part 1, February 2014, pp. 3–26. © Indian Academy of Sciences

Dual watermarking technique with multiple biometric watermarks

VANDANA S INAMDAR[1,*] and PRITI P REGE[2]

[1]Department of Computer Engineering and Information Technology,
College of Engineering, Pune 411 005, India
[2]Department of Electronics and Telecommunication Engineering,
College of Engineering, Pune 411 005, India
e-mail: vhj.comp@coep.ac.in; ppr.extc@coep.ac.in

MS received 21 September 2012; revised 29 August 2013; accepted 29 August 2013

Abstract. In order to improve the robustness of the watermarking algorithm, a dual watermarking method is proposed to prove copyright ownership. Visible watermarking is important for protecting online resources from unauthorized reproduction. However robust, visible watermarks are vulnerable to illegal removal and other common signal processing and geometric attacks. Multiple invisible watermarks can enhance the protection of the visibly watermarked image. When the ownership of tampered image is in question, the invisible watermark can be extracted to provide appropriate ownership information. We have proposed dual watermarking scheme with multiple biometric watermarks in which it embeds speech and face biometric traits of owner invisibly and lastly offline signature is overlaid translucently on image. Before embedding, speech is compressed using Linear Predictive Coding (LPC) and Gabor face is created from face biometric trait. All three watermarks Gabor face, LPC coefficients and offline signature are the biometric characteristics of the owner and hence they are highly related with copyright holder. The proposed scheme is robust enough, Gabor face and LPC coefficients can be extracted from the signature marked image or even from the tampered image from which signature is removed illegally or legally. As multiple watermarks are embedded at least one watermark survives under different attacks. It can find application for joint ownership or to address single ownership multiple times.

Keywords. Biometric features; dual watermarking; multiple watermarking; Gabor filter; linear predictive coding (LPC); human visual system (HVS) model.

1. Introduction

The explosive growth of digital multimedia techniques, together with the rapid development of digital network communication has created a pressing demand for techniques that can be used

[*]For correspondence

for copy protection, copyright protection and content authentication. Owing to the need of copyright protection and authentication validation, Digital Rights Management (DRM) is gaining importance. DRM refers to a range of access control technologies used to limit or restrict usage of digital content. Digital watermarking is useful in DRM systems as it can hide information within the digital content like images, audio and video. Biometrics refers to behavioural and physical characteristics of an individual. These can be used in digital watermarking to uniquely identify an individual, thereby strengthening the power of watermarking in copyright protection and authentication of digital media.

1.1 *Significance of biometric watermark*

Traditionally, watermarking scheme embeds a predefined string such as name of author or logo into the host document which can be text, audio, video, images, or 3D mesh models. There are some limitations to these watermarks such as they are less meaningful, intuitive for easily identifying and low correlative to owner for authentication. Using these as a watermark may lead to imitation, tamper and repudiation. Traditional watermarking method does not convincingly validate the claimed identification of the person as the host might be fraudulently watermarked with a particular string pattern or logo by impersonators.

Recently, there is a trend to incorporate biometrics in watermarking technology with the aim to enhance the credibility of conventional watermarking. This new emerging idea is classified into two primary modes; watermarked biometrics and biometric watermarking.

1.1a *Watermarked biometrics*: Host is a biometrics which is watermarked with another biometrics. Biometric data itself is vulnerable to attacks and security of biometric data is of prime importance. For instance, fingerprint minutiae is embedded in face image as a watermark for couple of reasons, e.g., may be for multimodal verification or transmission of genuine biometric trait over non-secure communication channel. The eavesdropper who intercepts the communication channel might not be aware that the biometric host is invisibly hidden.

1.1b *Biometric watermarking*: The watermark is a biometrics, while the host can be any copyrighted media. By embedding biometrics in the host, it formulates a reliable individual identification as biometrics possesses exclusive characteristics that can be hardly counterfeited. Biometric traits such as handwritten signature, fingerprint, iris, hand geometry, face are widely employed to offer a viable constituent in the context of authentication. If the watermarking is combined with biometric features, then it will be more secured and confidential as biometric features are unique for each individual.

A K Jain and his research team is a pioneer in suggesting watermarking of biometric data. Jain & Uludag (2003a, b) proposed multimedia content protection framework that is based on biometric data of the users. They suggested that only password encryption schemes are vulnerable to illegal key exchange problem. They proposed a method to use biometric data to secure another type of biometric data to increase the overall security of the system.

Literature related to watermarked biometric which uses fingerprint (Hong & Jain 1998), iris (Rajbul *et al* 2007; Feng & Lin 2007), voice (Vatsa *et al* 2009), face (Jain *et al* 2002a; Vatsa *et al* 2005, 2006; Noore *et al* 2007) as a watermark for multimodal verification or for secure transmission is presented by various researchers.

Digital watermarking has reached its maturity, biometric watermarking is still in its infancy phase. Few of the research articles related to biometric watermarking in which fingerprint (Jain and Uludag 2002b; Allah 2007; Jung *et al* 2007a, b; Nagamalleswara *et al* 2009), signature (Low

& Teoh 2007; Low *et al* 2008a, b; Namboodiri & Jain 2004), iris (Hassanien 2007; Wan *et al* 2007), voice (Wang *et al* 2008) are embedded as a watermark in digital media like images, video and 3D model are presented.

1.2 *Visible watermarking technique*

Visible watermarking is important for protecting online resources from unauthorized copying. Visible watermarking is a technique that inserts copyright information perceptibly into the contents so as to identify the ownership in a displayable manner and prevents the consumers from making an unauthorized use. It is the easiest way to identify the originator of the digital content since no special tools are required to extract the ownership information from the watermarked content. Visible watermark should be unobstructive and hard to remove illegally. However robust, visible watermarks are vulnerable to illegal removal and other common signal processing and geometric attacks. Visible watermarking techniques can be divided into two classes; irremovable and removable. In case of irremovable visible watermarking, watermark should not affect the visual quality of the original art. On the contrary, removable visible watermarking techniques provide solution to copyright protection problems.

Hu *et al* (2006) proposed a user-key-dependent removable visible watermarking system in Discrete Wavelet Transform (DWT) domain. Huang & Tang (2006) computed composite coefficients using global and local characteristics of the host and watermark images for visible watermarking algorithm. They used a contrast-sensitive function and block classification in the discrete wavelet transform domain. The original and watermark images are divided into different blocks and classified based on visual masking.

Hu & Jeon (2006) proposed reversible visible watermarking technique for ownership identification as well as for data hiding. To satisfy the requirements of large capacity and high image quality, hiding technique is based on data compression and uses a payload-adaptive scheme. Yang *et al* (2009) proposed reversible visible watermarking scheme for the applications in which the visible watermark is expected to combat copyright piracy but can be removed to recover the original image. Watermark is revealed transparently on image by overlapping it on a user specified region of the host image through adaptively adjusting the pixel values beneath the watermark.

1.3 *Multiple watermarking technique*

Multiple watermarks can be used to address multiple applications or one application may be addressed several times. For example, a first watermark can be used to embed ownership information, a second one for content integrity and a third one for fingerprinting. On the other hand, there can be multiple copyright watermarks, multiple content integrity watermarks. According to the respective applications, watermarking technology exhibits significantly different properties, e.g., robustness as required for ownership claims or fragility as required for integrity investigations. Multiple watermarking techniques can be distinguished into three different categories (Mark *et al* 2007).

A. Composite watermarking: All watermarks are combined into a single watermark which is subsequently embedded in one single embedding step.
B. Segmented watermarking: The host data is partitioned into disjoint segments and each watermark is embedded into its specific share.
C. Successive watermarking: Watermarks are embedded one after the other. This approach is also denoted re-watermarking.

In case of composite watermarking, all watermarks need to be of same type. Both segmented and composite watermarking suffers from the fact that all watermarks that are to be embedded have to be known in advance.

Therefore, successive or re-watermarking seems to be most promising approach (Mascher-Kampfer *et al* 2006). In case of successive watermarking, watermarks need to be embedded in the order of decreasing robustness. Otherwise, detection or decoding of more fragile watermarks is likely to fail due to the interference from more robust watermarks. Figure 1 depicts the scenario of successive watermarking scheme.

Three watermarks A, B and C are embedded successively in host image I using some embedding algorithm which results in watermarked images $\mathbf{I}_{\mathrm{A}}^{W}$, $\mathbf{I}_{\mathrm{AB}}^{W}$ and $\mathbf{I}_{\mathrm{ABC}}^{W}$, respectively. In case of non-blind techniques watermark detection needs the original image. Hence detection of watermarks A, B, C is the function of original and watermarked image which is stated as

$$\mathrm{C}_{\mathrm{extracted}} = \mathrm{f}(\mathbf{I}_{\mathrm{ABC}}^{W}, \mathbf{I}_{\mathrm{AB}}^{W}) \tag{1}$$

$$\mathrm{B}_{\mathrm{extracted}} = \mathrm{f}(\mathbf{I}_{\mathrm{AB}}^{W}, \mathbf{I}_{\mathrm{A}}^{W}) \tag{2}$$

$$\mathrm{A}_{\mathrm{extracted}} = \mathrm{f}(\mathbf{I}_{\mathrm{A}}^{W}, I). \tag{3}$$

The detection rate of C is superior to that of A since the additional watermarks involved in the correlation computation of A and B will simply act as a noise. The decrease in correlation for watermarks A and B is obviously due to watermark interference which is strongest for the first mark embedded since the signal extracted for detection is a signal involving all embedded watermarks. However, in case of blind watermarking algorithms as there is no involvement of reference image, detection rate outperforms the non-blind technique. The use of different frequency bands for embedding is more efficient for avoiding watermark interference in re-watermarking as compared to use of just different domains (Hammerle-Uhe *et al* 2008).

1.4 *Dual watermarking technique*

Dual watermark is a combination of a visible watermark and an invisible watermark. When the ownership of visibly watermarked image is in question, the invisible watermark can be extracted to provide appropriate ownership information. There is hardly any research work carried out

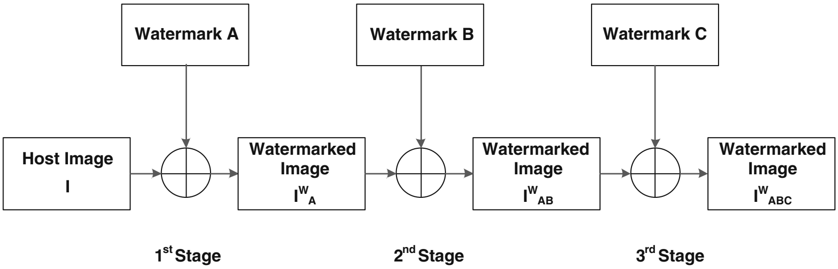


Figure 1. Multiple re-watermarking scenario.

using dual watermarking strategy. Mohanty *et al* (1999) presented a dual watermarking technique which attempts to establish the owner's right to the image and detect the intentional and unintentional tampering of the image. However, this early research is simply a combination of visible and invisible watermarking algorithms. It first used a block-DCT based visible watermarking algorithm to embed a grey scale watermark image, and then considered the resulting image as a new image to carry out invisible watermarking. Invisible watermarking is performed in spatial domain. The fragile watermark consisting of pseudo-random binary sequence (0,1) is EX-ORed with the kth bit-plane of the image. They claimed that if anybody tries to tamper the visible watermark intentionally, they can know the extent of tampering with the help of invisible watermark detection algorithm. Hu *et al* (2004) suggested dual watermarking method in DWT domain. Secondary image is inserted invisibly into the approximate band at the fourth level of wavelet decomposition of host image. Later at second stage, pseudorandom sequence is inserted into the approximate band at the third level of wavelet decomposition. Wong & Memon (2001) used an invisible authentication watermark to ensure the identity of a visibly watermarked image. Any modification to the visible watermark would be reflected in a corresponding error in the fragile watermark.

2. Proposed watermarking scheme

The objective for the development of this algorithm is to check the feasibility of embedding multiple invisible and visible biometric watermarks and study the interference of watermarks with each other. Efforts are also taken to reduce this interference at different stages of watermarking as far as possible.

In this paper, we propose a dual multiple watermarking technique which embeds both visible and invisible multiple biometric watermarks. Two biometric watermarks, owner's speech and Gabor face are embedded invisibly and third watermark which is an offline signature is overlaid visibly. Majority of the reported watermarking techniques use a pseudorandom sequence as a watermark and a binary decision, whether the digital media is watermarked or not is done by calculating the correlation between the watermark and media under considerations. However, watermark like PN sequence does not represent any meaningful information about the owner and thus serves limited applications. Significant motivation for using biometric features such as face, voice and signature as a watermark is that face and signatures are the modalities that humans largely depend for authentication. Secondly, these modalities can be captured easily and every human is a putative expert in face and voice recognition from infancy. Signature is widely accepted trait for all commercial application. These are the major reasons which motivated us to propose multimodal biometric watermarking. When the ownership of visibly marked image is in question, invisible watermarks can be extracted to prove the ownership. We proposed a strategy for re-watermarking scheme which still maintains the high correlation of earlier embedded watermarks in spite of non-blind watermarking technique.

Watermarking scheme proposed here is separable as it is possible to extract each watermark individually at each stage and even from the final watermarked object.

The technique proposes a multiple biometric re-watermarking scheme in which it first embeds the Gabor face in the host image using varying wavelet packet transform. The band selected for embedding the Gabor face is variable and is selected based on the cost function Peak Signal to Noise Ratio (PSNR) of the extracted Gabor face. In the second stage of watermarking in face watermarked image, LPC coefficients of speech watermark are embedded into the horizontal frequency band of wavelet decomposition. Finally, this image with multiple invisible watermarks is marked visibly with offline signature of owner. The size and location of this visible watermark can be decided so that it will not hamper the aesthetic view of image. The frame work for proposed multiple watermarking scheme and extraction of different watermarks at different stages is shown in figure 2.

This watermarking scheme contains following four phases: (1) Face watermark insertion. (2) Speech watermark insertion in face watermarked image. (3) Overlaying of signature watermark on invisibly watermarked image. (4) Extraction of Gabor face and LPC coefficients either from visibly watermarked image or from the image from which signature is removed illegally or legally.

2.1 *Face watermark insertion*

Various approaches like Eigen face method using Principal Component Analysis (PCA), Fisher faces using Linear Discrimination Analysis (LDA), Independent Component Analysis (ICA) are prominently used for extraction of face features. All these methods generate the face features which can be used for identification or verification. Embedding face feature will not suffice the requirement for ownership identification as reverse engineering is not possible from face feature to reconstruct the face for perceptual recognition. In such case, template matching has to be carried out within entire face data base. For generating the watermark from face image, we are using Gabor filter. Face watermark insertion phase consists of Gabor face generation, wavelet packet decomposition of host image and selection of band for watermark insertion and lastly watermark embedding.

2.1a *Gabor filtering*: As can be seen from the filter definition, each Gabor filter represents a Gaussian kernel function modulated by a complex plane wave (Kamarainen *et al* 2006; Struc & Pavesic 2010). The filter has a real and an imaginary component representing orthogonal directions. The two components may be formed into a complex number or used individually.

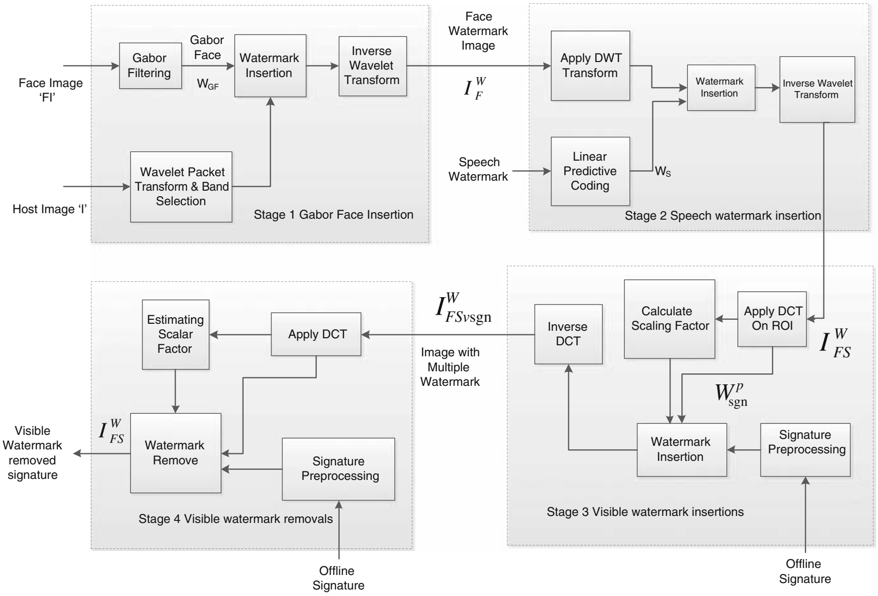


Figure 2. Frame work for multiple watermark insertion and extraction.

The real and imaginary components of Gabor filter are represented by equations (4) and (5), respectively.

$$g\left(x, y; \lambda, \theta, \psi, \sigma, \gamma\right) = \exp\left(-\frac{x'^2 + \gamma^2 y'^2}{2\sigma^2}\right)\cos\left(2\pi\frac{x'}{\lambda} + \psi\right) \tag{4}$$

$$g\left(x, y; \lambda, \theta, \psi, \sigma, \gamma\right) = \exp\left(-\frac{x'^2 + \gamma^2 y'^2}{2\sigma^2}\right)\sin\left(2\pi\frac{x'}{\lambda} + \psi\right), \tag{5}$$

where $x' = x\cos\theta + y\sin\theta$ and $y' = -x\sin\theta + y\cos\theta$, (x, y) is the position of pixel.

The wavelength λ is the wavelength of the sinusoidal factor and can be co-related with the centre frequency f as $f = 1/\lambda$. The parameter θ controls the direction of carrier since x' and y' are rotated by θ. Its value is within a range of 0 to 360°, ψ is the phase offset, standard deviation σ is the width of the Gaussian envelope and aspect ratio γ is the amount kernel is stretched in either along or across the kernel wave pattern. The values of these parameters largely affect the output of the Gabor filter. Parameters selected are $\psi = 0$, $\gamma = 1$, $\sigma = 2\pi$ for present implementation (Shen & Bai 2006).

As the values of these three parameters are fixed, the output of the Gabor filter now depends on x, y, f and θ. Real and imaginary part now can be written as

$$g\left(x, y; f, \theta\right) = \exp\left(-\frac{x'^2 + y'^2}{2\sigma^2}\right)\cos\left(2\pi f x'\right) \tag{6}$$

$$g\left(x, y; f, \theta\right) = \exp\left(-\frac{x'^2 + y'^2}{2\sigma^2}\right)\sin\left(2\pi f x'\right), \tag{7}$$

when using the Gabor filters for facial feature extraction, we construct a filter bank of 5 scales and 8 orientations, that is, $u = 0, 1, \ldots, p$ and $v = 0, 1, \ldots, r$, where $p = 5$ and $r = 8$ and frequency $f = 2^{-(u/2)2\pi}$, orientation $\theta = v\pi/8$. Thus $5 \times 6 = 30$ filters are created at 40 different pairs of scale and orientation.

Feature extraction using Gabor filter: Let FI be a gray-scale face image of size $M \times N$ pixels and $g_{u,v}(x, y)$ denote a Gabor filter given by its centre frequency f and orientation θ at scale u and orientation v. Feature extraction procedure is defined as convolution operation of the given face image FI with the Gabor filter $g_{u,v}(x, y)$ of scale u and orientation v, that is

$$G_{u,v}\left(x, y\right) = FI\left(x, y\right) * g_{u,v}\left(x, y\right), \tag{8}$$

where $G_{u,v}(x, y)$ denotes the complex filtered output that can be decomposed into its real and imaginary parts.

$$E_{u,v}\left(x, y\right) = Re\left[G_{u,v}\left(x, y\right)\right] \tag{9}$$

$$O_{u,v}\left(x, y\right) = Im\left[G_{u,v}\left(x, y\right)\right]. \tag{10}$$

Based on these results, the magnitude $A_{u,v}(x, y)$ and phase $\phi_{u,v}(x, y)$ responses of the filtering operation can be computed as follows:

$$A_{u,v}\left(x, y\right) = \sqrt{E_{u,v}^2\left(x, y\right) + O_{u,v}^2\left(x, y\right)} \tag{11}$$

$$\varphi_{u,v}\left(x, y\right) = \arctan\left(\frac{O_{u,v}(x, y)}{E_{u,v}(x, y)}\right). \tag{12}$$

The given face image is filtered with all 30 filters from the bank resulting in an inflation of data dimensionality to 30 times its initial size. Based on the empirical results, it is observed that Gabor face whose entropy is in the vicinity of half of the entropy of original image is perceptually good from recognition point of view and when embedded in host image produces less visible artifacts and gives better PSNR of host image. Based on this experimentation, one of the Gabor face was selected as a face watermark. Gabor face is of same size as that of original face image and is denoted as W_{GF}.

2.1b *Wavelet packet decomposition of host image*: The proposed algorithm embeds Gabor face into the host image by utilizing a multi resolution analysis proposed by the Wavelet Packet Transform (WPT). In the two dimensional Discrete Wavelet Packet Transform (DWPT), three detail subbands along with approximation subband are further decomposed. In general WPT divides the frequency space into various parts and allows better frequency localization of signals (Bhatnagar & Raman 2012). For 'l' level decomposition there are 4^l different ways to encode the image which provide a better tool for image analysis. Figure 3 shows the full quadtree describing the WPT with two levels. In such quadtree, a node at a level 'l' of the tree corresponds to a subband consisting of $4^{-l} \times M \times N$ coefficients, where $0 \leq l \leq L$, L is the maximum level of the WPT and $M \times N$ is the size of the host image which is considered for decomposition. In general, if the size of the original image and the watermark image is $M \times N$ pixels and $P \times Q$, respectively, then taking WPT to the l^{th} level, where

$$l = \frac{1}{2} \log \frac{M \times N}{P \times Q} \tag{13}$$

results in subbands at level 'l' which can be selected for Gabor face insertion.

2.1c *Band selection and face watermark insertion*: The level of decomposition of WPT is dictated by the size of host image and the size of watermarked image and there are 4^l subband at l^{th} level. One of the bands at the highest level is selected for watermark insertion based on best band selection strategy. The best band selection is done on some cost function such as entropy, threshold of the coefficients and norm of coefficients etc. (Kumhom & Chamnongthai 2004). Data loss may occur during watermark insertion and removal due to forward and backward DWT transform. In our work, we are using PSNR of the watermark image which is a Gabor face for determining the exact band for watermark insertion. Watermark is inserted in all bands at highest level recursively. PSNR of the extracted watermark from each band is calculated and the band which gives highest PSNR is selected for watermark insertion. This pretty simple strategy of

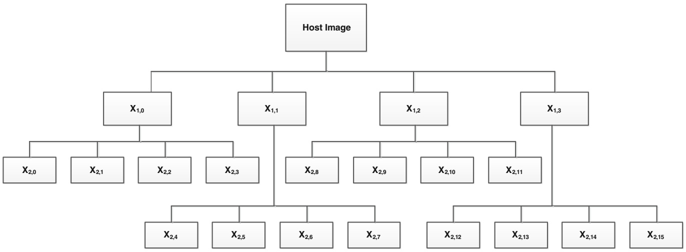


Figure 3. Full quadtree of 2 level WPT.

selecting band for Gabor face insertion gives good perceptual quality of extracted watermark when we embed multiple watermarks at later stage. In a selected band Gabor face is inserted using equation (14).

$$I_F^w\,(i,\,j) = I^l\,(i,\,j) + \propto W_{GF}\,(i,\,j)\,, \tag{14}$$

where $I^l(i,\,j)$ are the coefficients of host image of selected band at l^th level, $W_{GF}(i,\,j)$ are coefficients of Gabor face which is used as a watermark. By applying inverse wavelet transform, we get face watermarked image I_F^w which is given as input to the second stage for speech insertion.

2.2 *Speech watermark insertion*

This stage aims to embed biometric trait, such as speech which corresponds to the identity of owner, as a watermark in the image which is already watermarked with Gabor face. As a biometric of human being, speech is inherent and does not change along with time, it is universal and easily quantifiable. The major challenge in embedding the speech watermark is the exorbitant size of watermark itself. The audio signal is first encoded using Pulse Code Modulation (PCM) encoding technique at 8 KHz sampling rate. As the speech file consists of large number of samples, we have applied linear predictive coding on speech to reduce the size of audio watermark. LPC coefficients are embedded in horizontal detail coefficients of host image using spread spectrum watermarking technique as proposed by Inamdar *et al* (2009). To avoid the interference of second watermarking signal, it is casted into first level of detail coefficient, while face watermark is embedded at higher level in the wavelet packet decomposition. Algorithm for speech embedding is as follows:

(1) Apply LPC on speech samples to generate LPC coefficients.
(2) Apply the wavelet transform on face watermarked image I_F^w to decompose it into four bands.
(3) Select the LH subband of decomposed image and generate the perceptual mask that identifies the significant perceptual components of the wavelet coefficients. The method employs the largest ‘N’ wavelet coefficients, where ‘N’ is chosen to be equal to length of LPC coefficients generated.
(4) Insert the LPC coefficients into selected wavelet coefficients using additive multiplicative equation (15):

$$I_{FS}^w\,(i,\,j) = I_F^w\,(i,\,j)\left(1 + \alpha W_s^i\right), \tag{15}$$

where W_s^i = the i^th value of LPC coefficients of speech watermark.
$I_F^w\,(i,\,j)$ = the original wavelet coefficients of face watermarked image
$I_{FS}^w\,(i,\,j)$ = the wavelet coefficients after embedding LPC coefficients
α = the strength of the watermark.

(5) Generate the watermarked image by applying the inverse wavelet transform.
I_{FS}^w is the invisible watermarked image in which Gabor face and speech is inserted.

2.3 *Visible watermark embedding*

Offline handwritten signature of the owner is overlaid translucently on a user specified region of invisibly watermarked image. The part of image where signature is overlaid which is called as Region of Interest (ROI) is selected such that it will not hamper the aesthetic view. Visible watermarking scheme that adaptively varies the watermark strength of signature image which is be overlaid translucently on host image, depending on the underlying image content and Human

Visual System (HVS) characteristics is implemented in this stage. It is a reversible watermarking technique; legal removal of visible signature will resume the original data. In the presence or absence of visible watermark, speech and face watermark can be independently extracted to prove the ownership.

Approach proposed by Yang *et al* (2008) is referred here for visible watermark insertion and lossless recovery of original image. We embed a variant of signature as the visible watermark into the host image. Entire process of signature embedding is carried out in three phases; watermark preprocessing, watermark insertion and watermark removal.

2.3a *Signature preprocessing*: The watermark preprocessing technique for the generation of the various preprocessed watermark image versions to modulate the original watermark with the user key can successfully prevent illegal removal. Chaotic logistic map is one of the schemes for preprocessing the original watermark (Salleh & Isnin 2002). Using a key and a chaotic sequence, variant of signature watermark is generated. The generation of this watermark is a key controlled. Without the secret key the same variant of the original watermark cannot be derived from the marked image. It is not possible for the adversary to remove the visible watermark unauthentically. Sequences generated by iterating chaotic maps constitute an efficient alternative to pseudorandom watermark sequences. Chaos is known to be a system which is highly sensitive to its initial state and a slight change in initial state (Jakimoski & Kocarev 2001). We have used the chaotic logistic map as given by equation (16).

$$X_{n+1} = \lambda x_n \left(1 - x_n\right). \tag{16}$$

Using a secret key in the range (0,1) as initial value x_0, a chaotic sequence (x_1, x_2, x_3,. . ..) is generated. λ is a positive number which determines the characteristics of x. λ is chosen in the range of 3.57 to 4 (Liu *et al* 2007). The signature image watermark W_{sgn} is divided into non-overlapping blocks of size 16 × 16 pixel and DCT is applied on each block. Randomly 256 elements of chaotic sequence 'X' are selected and warped to form 2D matrix of size 16 × 16. Key-based variant of original signature W_{sgn}^{p} is obtained by element-by-element multiplication of each block of original signature with that 2D chaotic sequence. W_{sgn}^{p} is used for overlaying on pre-watermarked image I_{FS}^{W}.

2.3b *Watermark insertion*: The host image at this stage is the invisibly watermarked image I_{FS}^{w}. For further simplicity, we will omit the subscript/superscript. Depending upon the size of covered image which is to be watermarked visibly, preprocessed signature W_{sgn}^{p} is scaled up or down accordingly. While calculating the scaling and embedding factors, the watermark signature and part of the host image where watermark is to be cased is only considered. The ROI of host image where signature is overlaid translucently is denoted as I^{sub}. ROI is provided by image provider and has the same size as that of watermark. Equation (17) is employed to overlay the signature on host image.

$$I_m^w\left(i,j\right) = \alpha_m \times I_m^{\text{sub}}\left(i,j\right) + \beta_m \times W_{sgn_m}^{p}\left(i,j\right), \qquad m = 1, 2, 3, \ldots\ldots, M\ . \tag{17}$$

$I_m^W\left(i,j\right)$, $I_m^{\text{sub}}\left(i,j\right)$, $W_{sgn_m}^{p}\left(i,j\right)$ denote the $(i,\ j)^{\text{th}}$ DCT coefficient of the m^{th} 8 × 8 element block of watermarked image I^W, host sub-image I^{sub} and preprocessed watermark W_{sgn}^{p}, respectively.

α_m and β_m are the adaptive scaling and embedding factors for the m^{th} block of host sub- image I^{sub} and preprocessed watermark image W_{sgn}^{p}, respectively and M is the total number of blocks.

Determination of scaling and embedding factor: While formulating scaling and embedding factors, two aspects of HVS, luminance and texture are taken into account. Texture features and luminance of both host sub-image I^{sub} and watermark W_{sgn}^{p} are considered while modelling the scaling and embedding factors. The blocks with mid-luminance intensities are more sensitive to noise. Assigning greater value of the scaling factor α_m for mid-luminance area and attenuating its value for darker and brighter blocks is desirable. Scaling factor α_m exhibits Gaussian distribution with the luminance value of m^{th} block. Most of the energy is concentrated into DC coefficient which represents luminance. Scaling factor is calculated as

$$\alpha_m = \frac{1}{\sqrt{2\pi\left(\sigma_1^2+\sigma_2^2\right)}} exp^{\frac{-[l_m-(\mu_1+\mu_2)]^2}{2\left(\sigma_1^2+\sigma_2^2\right)}}, \tag{18}$$

where l_m is the luminance of the m^{th} block of host sub-image and signature image, which is calculated as

$$l_m = I_m^{\text{sub}}(0,0) + W_{sgn_m}^{p}(0,0), \qquad m = 1, 2, 3, \ldots\ldots, M. \tag{19}$$

Mean value μ_1 and variance σ_1 of the DC coefficients of the host sub-image are found out, respectively as

$$\mu_1 = \frac{1}{M}\sum\nolimits_{m=1}^{M} I_m^{\text{sub}}(0,0) \tag{20}$$

and

$$\sigma_1 = \frac{1}{M}\sum\nolimits_{m=1}^{M}\left[I_m^{\text{sub}}(0,0)-\mu_1\right]^2. \tag{21}$$

On the same ground, mean value μ_2 and variance value σ_2 of the preprocessed signature watermark W_{sgn}^{p} are calculated.

AC coefficients, which mainly reflect the texture features of image, are taken into account to deal with the second aspect of HVS. It has been observed that in strongly textured blocks, energy tends to be more evenly distributed among AC coefficient, thus the variance of AC coefficients tends to be smaller. More energy should be received from the watermark, where the host image is strongly textured because HVS is less sensitive to changes made in highly textured region. Scaling factor α_m is in direct proportion to the m^{th} block variance of the host sub-image I^{sub} and preprocessed watermark W_{sgn}^{p}. Thus scaling factor is proportional to v_m, where $v_m = v_m^h + v_m^{wp}$, where v_m^h and v_m^{wp} are the variances of m^{th} block of host sub-image and preprocessed watermark, respectively. To reflect the direct relationship of scaling factor with variance, equation (18) can be modelled as

$$\alpha_m = \hat{v}_m \frac{1}{\sqrt{2\pi\left(\sigma_1^2+\sigma_2^2\right)}} exp^{\frac{-[l_m-(\mu_1+\mu_2)]^2}{2\left(\sigma_1^2+\sigma_2^2\right)}}, \tag{22}$$

where $\hat{v}_m$ is the normalized version of v_m and calculated

$$\hat{v}_m = \frac{\bar{v}_m - \min(\bar{v}_m)}{\max(\bar{v}_m) - \min(\bar{v}_m)}, \tag{23}$$

$\bar{v}_m$ in the equation (23) is the natural logarithm of v_m. Normalization and natural logarithm is taken so as to control scaling factor α_m in a narrow range.

Variances v_m^h, v_m^{wp} are calculated for the host image and preprocessed watermark by considering only the insignificant coefficients of preprocessed watermark and corresponding coefficients ROI of host image. Coefficients are deemed to be insignificant if it's quantized value is zero. S_m is the set of coordinates whose corresponding DCT coefficients of the preprocessed watermark are insignificant. Randomly one element is removed from this set of insignificant coefficients and is selected for hiding DC coefficient of the m^{th} block of host sub-image I^{sub} which facilitates its retrieval for estimation of two parameters α_m and β_m during watermark removal process. s_m^r denotes the sub-set of S_m after removing one element. There is only one element in $S_m - s_m^r$ and its coordinates are also denoted by $S_m - s_m^r$. Hence to find out the variance v_m^h of the m^{th} block of host sub-image I_m^{sub} coefficients in set s_m^r are considered. Equation (24) gives the variance of the m^{th} block of host subimage.

$$v_m^h = \frac{1}{\mathrm{N}} \sum\nolimits_i \sum\nolimits_j \left(I_{i,j,} - \mu_{\mathrm{AC}}\right)^2, \tag{24}$$

where N is the total number of insignificant coefficients in set s_m^r and μ_{AC} is their mean and is calculated as follows.

$$\mu_{\mathrm{AC}} = \frac{1}{\mathrm{N}} \sum\nolimits_i \sum\nolimits_j I_{i,j}. \tag{25}$$

By the same way, variance v_m^{wp} of preprocessed watermark W_{sgn}^p is calculated. Coefficients corresponding to same locations as that of s_m^r are considered for calculation.

Embedding factor β_m is calculated as follows:

$$\beta_m = 1 - \alpha_m. \tag{26}$$

2.3c *Visible watermark embedding*: With the preprocessed watermark, host image and estimated scaling and embedding factors, the steps for embedding visible watermark are as follows:

Step 1: Select the ROI from host image for overlaying signature watermark. It is of same size as that of preprocessed signature watermark.

Step 2: Divide both host sub-image and preprocessed watermark into 8 × 8 blocks and apply DCT on it.

Step 3: For each host sub-image block I_m^{sub} and preprocessed watermark block W_{sgn}^p, generate the watermarked image block I_m^w by adding significant coefficients of host sub-image to that of corresponding coefficients of preprocessed signature watermark using equation (17).

Step 4: Hide the value $\frac{\beta_m \times \left[I_m^{\text{sub}}(0,0) - W_{sgn_m}^p(0,0)\right]}{10}$ into the $(S_m - s_m^r)^{\text{th}}$ coordinate of the watermarked image block I_m^w for facilitating the retrieval of the DC coefficient of the host image block I_m^{sub} from the marked image block I_m^w during the watermark removal process.

Step 5: Perform the inverse DCT on the marked host sub-image. Marked sub-image is integrated with the other part of image to produce final watermarked image. The watermarked image generated at this final stage is a dual watermarked image with visible and invisible watermarks called as I^w_{FSvsgn}.

During watermark insertion process, only significant coefficients of preprocessed watermark are embedded into the corresponding coefficients of host sub-image. Most of the energy of preprocessed watermark is concentrated into significant coefficients. Embedding in only these coefficients is sufficient enough to reveal the details of the visible signature watermark in the marked image. For calculation of variance v^{wp}_m and v^h_m only insignificant coefficients of signature watermark and corresponding coefficients of host sub-image are used. The reason for such segregation is that as the insignificant coefficients remain intact during embedding process, α_m and β_m can be estimated by using these coefficients directly from the watermarked image I^w_{FSvsgn} without referring the original host image. DC coefficient of each block of host image will help out to estimate α_m and β_m, so it is scaled down to avoid the degradation of watermark image before embedding.

2.3d *Legal removal of visible watermark*: There are some potential applications where a visible watermark needs to be removable or reversible. The interested buyers can remove the embedded watermark pattern to create the unmarked image using retrieval, or called as ‘vaccine’ program that is available at additional cost. Achieving lossless recovery of the original host signal from a visibly watermarked image is still an acute challenge. It is to be noted that watermark removal is an optional stage, interested buyers can remove visible watermark after purchasing media. The removal of the embedded visible watermark for high-quality restoration of the original host image depends on the secret key. Given the availability of the algorithm, watermarked image, and the original watermark, if the embedded visible watermark is removed by using the correct key, then such removal is called legal removal. By using incorrect user key, much energy residue of the watermark still exists in the illegally recovered image there by tampering the watermarked image while removing the visible watermark. This is because the embedded watermark version depends on the private key so that an unauthorized user has no idea about which watermark version should be subtracted from the watermarked image.

Process of visible watermark removal program from the multiple watermarked image I^w_{FSvsgn} (For simplicity the subscript is omitted and simply called as I^w).

With the availability of the watermarked image I^w, private key k, and the signature watermark W_{sgn}, watermark removal process consists of following steps:

Step 1: Produce the preprocessed signature watermark W^p_{sgn} using the private key k.
Step 2: Divide the preprocessed watermark W^p_{sgn} and watermarked image I^w into non-overlapping 8 × 8 pixel blocks and apply DCT transform on these blocks.
Step 3: For each watermarked image block I^w_m repeat the step 4 to 5.
Step 4: Select the $(i,\ j)^{\text{th}}$ DCT coefficient, where $(i,\ j)$ corresponds to the $S_m - s^r_m$ and find out approximate value of DC coefficient of original host sub-image as $I^w_m\ (i,j) \times 10 + I^w_m\ (0,0)$.

This can be derived as follows:

DC value of m^{th} block of host sub-image was hidden in $(i,\ j)^{\text{th}}$ coefficient of corresponding block of marked image (refer step 4 of watermark embedding).

Equation $I^w_m\ (i,j) = \frac{\beta_m \times \left[I^{\text{sub}}_m(0,0) - W^p_{sgn_m}(0,0)\right]}{10}$ will lead to

$$I^w_m\ (i,\ j) \times 10 + \beta_m \times W^p_{sgn_m}\ (0,0) = \beta_m \times I^{\text{sub}}_m\ (0,0)\,. \tag{27}$$

Equation (17) of watermark insertion corresponds to DC coefficients yields

$$I_m^w\,(0,0) = \alpha_m \times I_m^{\text{sub}}\,(0,0) + \beta_m \times W_{sgn_m}^p\,(0,0)\,. \tag{28}$$

Substituting value of $\beta_m \times W_{sgn_m}^p\,(0,0)$ in equation (27)

$$I_m^w\,(i,\,j) \times 10 + I_m^w\,(0,0) - \alpha_m \times I_m^{\text{sub}}\,(0,0) = \beta_{\text{m}} \times I_m^{\text{sub}}\,(0,0) \tag{29}$$

$$I_m^w\,(i,j) \times 10 + I_m^w\,(0,0) = \beta_m \times I_m^{\text{sub}}\,(0,0) + \alpha_m \times I_m^{\text{sub}}\,(0,0)\,. \tag{30}$$

As $\alpha_m + \beta_m = 1$

$$I_m^w\,(i,j) \times 10 + I_m^w\,(0,0) = I_m^{\text{sub}}\,(0,0)\,. \tag{31}$$

Step 5: Select the DCT coefficients from the watermarked image corresponding to the set s_m^r and we get $I_m^{\text{sub}}\,(i,j) = I_m^w\,(i,j)$.

These correspond to insignificant coefficients of host sub-image as we have considered only significant coefficients for watermark insertion.

Step 6: Using approximate DC coefficients as calculated in step 4 and DC coefficients of preprocessed watermark $W_{sgn_m}^p$ model α_m as per equations (18)–(21).

Step 7: Using the insignificant coefficients of host sub-image which are found out in step 5, and that of processed watermark $W_{sgn_m}^p$, find out v_m^h and v_m^{wp}. Update the scaling factor by α_m by plugging it with normalized version of v_m as calculated by equation (22).

Also find out β_m.

Step 8: Obtain the unmarked image by removing the significant DCT coefficients of preprocessed signature watermark W_{sgn}^p, from the marked image I^w using the equation (32)

$$I_m^{\text{sub}}\,(i,j) = \frac{I_m^w\,(i,j) - \beta_m \times W_{sgn_m}^p\,(i,j)}{\alpha_m}, \qquad i = 1, 2, \ldots\ldots\ldots, 8; \quad j = 1, 2, \ldots\ldots\ldots, 8 \quad m = 1, 2, \ldots\ldots\text{M}. \tag{32}$$

These recovered coefficients are integrated with the other part of image to get reversed image.

3. Experimentation and result

As the proposed scheme involves multiple watermarks, testing is carried out at different stages for evaluation of robustness, to check the interference of different watermarks with each other, fidelity of watermarked image and that of extracted watermark. Apart from perceptual quality,

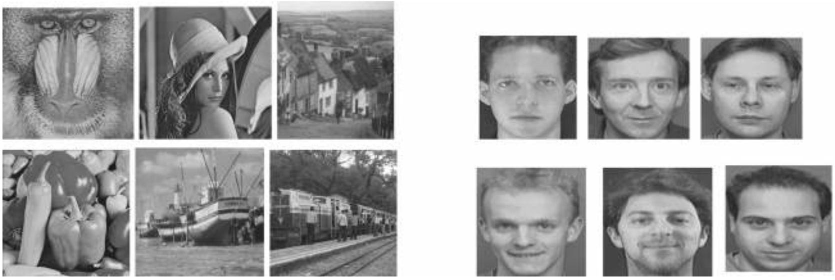


Figure 4. Sample of host images and face images.

Table 1. Selected band for Gabor face insertion.

Host	Face 1	Face 2	Face 3	Face 4	Face 5
Baboon (256 × 256)	$X_{1,1}$	$X_{1,0}$	$X_{1,2}$	$X_{1,1}$	$X_{1,1}$
Boat (512 × 512)	$X_{2,0}$	$X_{2,0}$	$X_{2,0}$	$X_{2,0}$	$X_{2,0}$
Goldhill (512 × 512)	$X_{2,0}$	$X_{2,10}$	$X_{2,6}$	$X_{2,0}$	$X_{2,10}$
Peppers (512 × 512)	$X_{2,8}$	$X_{2,14}$	$X_{2,0}$	$X_{2,0}$	$X_{2,15}$
Matheran (1024 × 1024)	$X_{3,0}$	$X_{3,11}$	$X_{3,34}$	$X_{3,4}$	$X_{3,21}$
Lena (512 × 521)	$X_{2,12}$	$X_{2,2}$	$X_{2,15}$	$X_{2,5}$	$X_{2,15}$

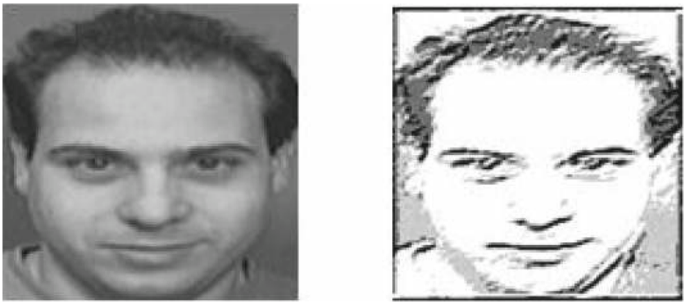
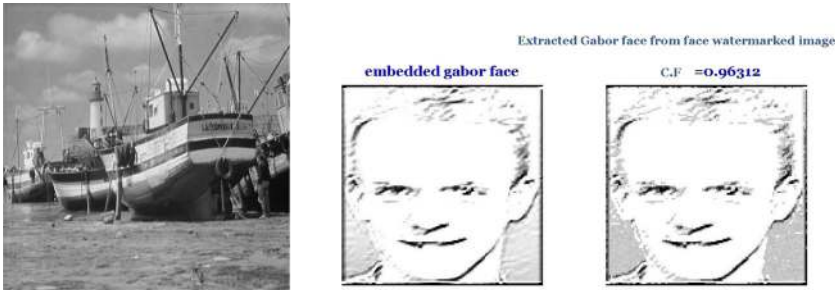


Figure 5. Original and Gabor face for sample face image.

quantitative metric used for watermarked image is PSNR. Correlation Factor (CF) and Similarity Factor (SF) are used as a quantitative measure for Gabor face and speech, respectively. ORL face database is used for experimentation. Figure 4 shows few of the host images used for testing and face images for generating Gabor face as a watermark.

Gabor face is inserted into one of the bands at l^{th} level and PSNR of the extracted face is found out in each case. The process is repeated for all bands. The band for which PSNR is highest is selected for final watermark insertion. Table 1 shows the band selected for Gabor face insertion for different host images with different faces with respect to figure 3. It is to be noted that for the same host image with different face as a watermark, different band is selected. Sample of original face and its Gabor face is shown in figure 5.

A sample of face watermarked image and embedded and extracted Gabor face at first stage of watermarking is shown in figure 6.

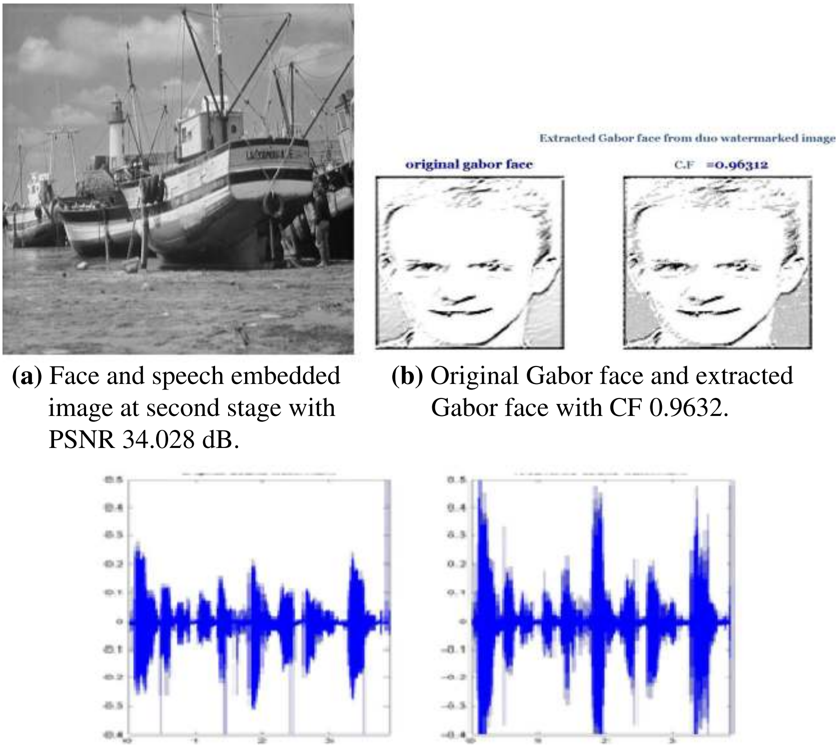


(a) Face watermarked image with PSNR 35 dB at first stage.

(b) Original Gabor face and extracted Gabor face with CF 0.9632.

Figure 6. Sample output at first stage of multiple watermarking technique.

In the second stage of watermarking, the face watermarked image is given as input to embed the speech watermark. Speech up to 7 s duration can be embedded without degrading the perceptual quality of host media. Figure 7 shows multiple invisible watermarked image along with

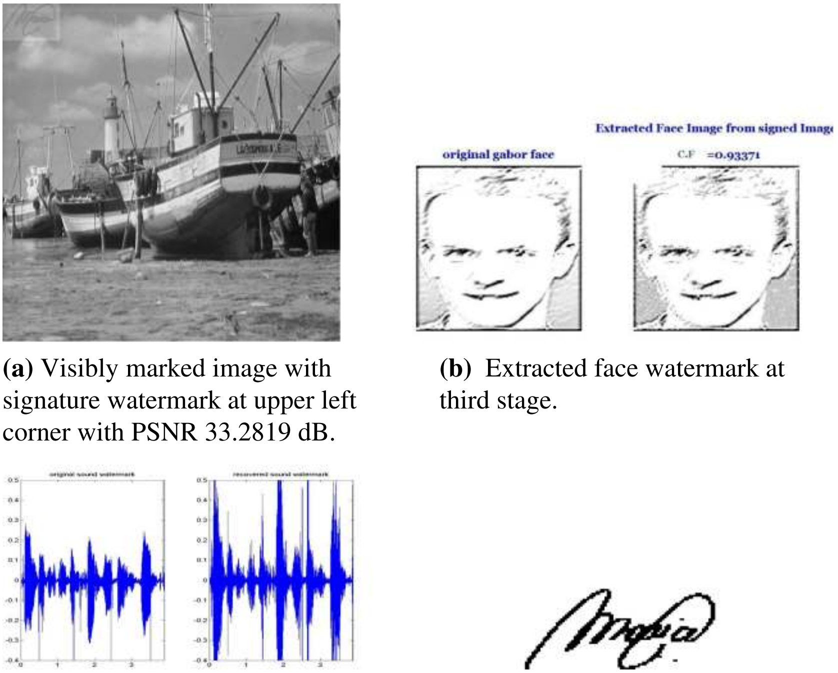


(a) Face and speech embedded image at second stage with PSNR 34.028 dB.

(b) Original Gabor face and extracted Gabor face with CF 0.9632.

(c) Embedded and extracted speech watermark of 4 s duration with SF 0.9775.

Figure 7. Sample output at second stage of multiple watermarking technique.


Extracted Face Image from signed Image
original gabor face
C.F =0.93371
original sound watermark
recovered sound watermark

(a) Visibly marked image with signature watermark at upper left corner with PSNR 33.2819 dB.

(b) Extracted face watermark at third stage.

(c) Extracted speech watermark at third stage.

(d) Overlaid signature watermark.

Figure 8. Sample output at third stage of multiple watermarking technique.

embedded and extracted face and speech watermark at second stage. Subjective tests of extracted speech watermark are taken to evaluate perceptual quality of extracted speech.

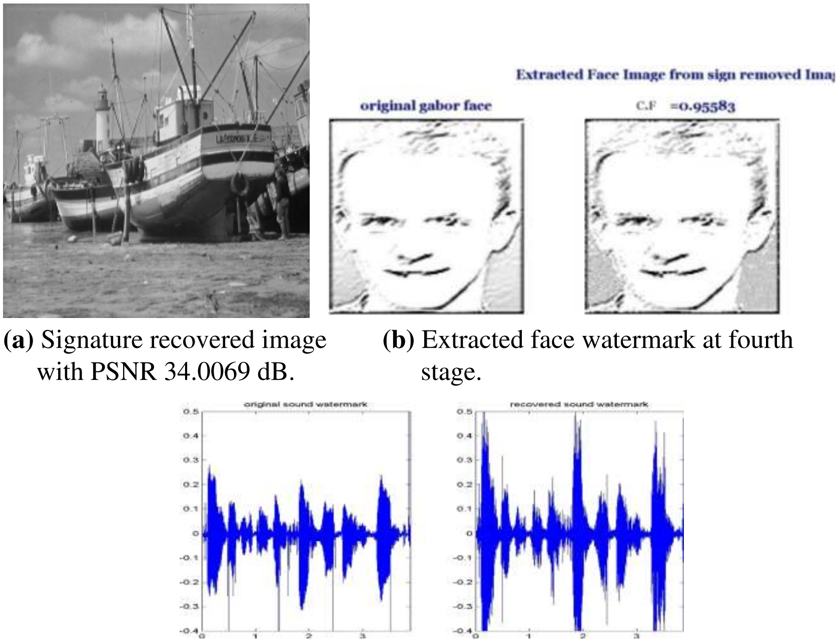
In the third stage of testing, the image which is invisibly watermarked with face and speech is visibly marked with the signature of owner. Figure 8 shows the image which is marked visibly and invisibly multiple times.

There are some potential applications where a visible watermark is first used as a tag or ownership identifier and then needs to be removable. Visible watermarking scheme implemented here is irreversible. At fourth stage of testing, overlaid visible watermark can be removed by using a key and a ‘vaccine program’. Figure 9 shows signature recovered image which still contains face and speech invisible watermarks.

Few more watermarked images with multiple watermarks are shown figure 10.

Table 2 shows the average PSNR for different test images at different stages of watermarking.

Watermarked image at third and fourth stage is tested for robustness against different attacks. The purpose of multiple watermarking scheme proposed here is to prove ownership and authentication multiple times. Common image processing such as compression, filtering and noise addition can not hinder the embedded visible watermark from indicating ownership. When the owner’s visible watermark is illegally removed or it is removed by legitimate consumer and ownership of such media is in question, extracted invisible watermark can suffice the requirement to prove the ownership. Two invisible watermarks are hidden in a host image so that at least one



(a) Signature recovered image with PSNR 34.0069 dB.

(b) Extracted face watermark at fourth stage.

(c) Extracted speech watermark from signature recovered image at fourth stage.

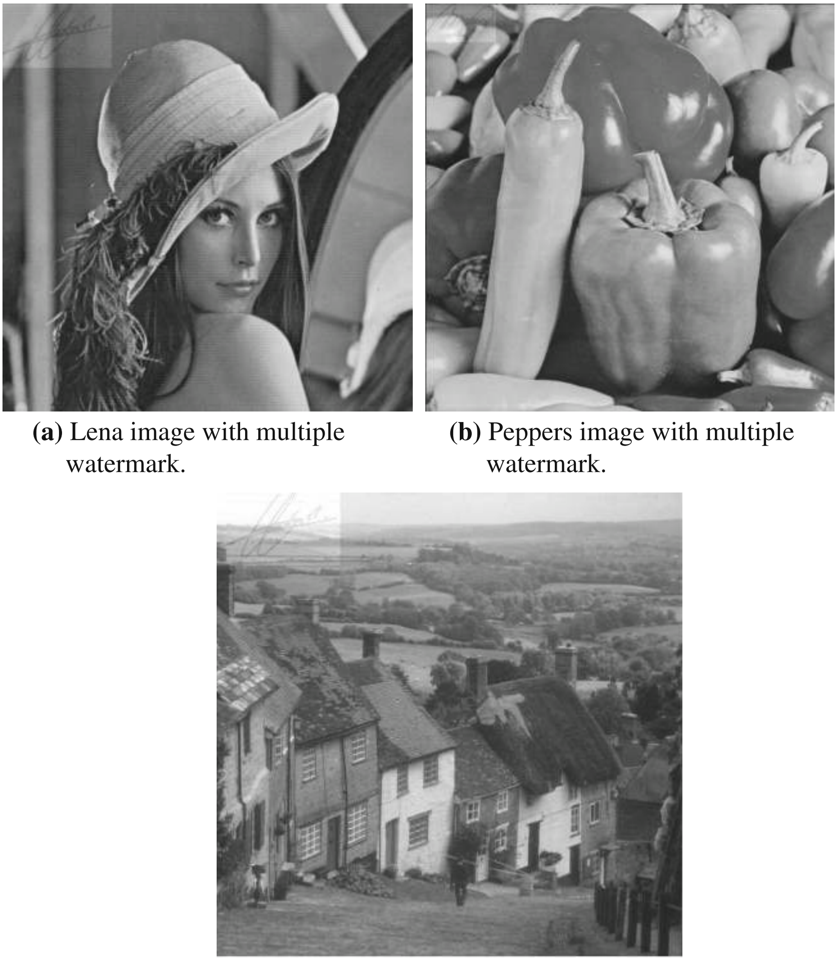
Figure 9. Signature recovered image with embedded and extracted Gabor face and speech watermark at fourth stage.

watermark can survive under different attacks. Both invisible watermarks are resistant to common signal processing attacks such as salt and pepper noise, median filtering, Weiner filtering, Gaussian noise, JPEG compression with quality factor up to 70, histogram equalization, brightness attacks, etc. However, it is difficult to cope up with geometric attacks like cropping, rotation and scaling. Figure 11 shows the sample of extracted watermark where Gabor face survives but speech watermark fails under cropping attacks. Figure 12 shows extracted Gabor face and speech watermark under JPEG compression attack.

The proposed scheme is separable, at each stage the watermarks can be extracted independently. After embedding the speech watermark, previously inserted Gabor face can be extracted at second stage, at third stage after overlaying the visible watermark both Gabor face and speech can be extracted. At fourth stage, it is possible to extract both invisible watermarks from an image which is recovered by reversing visible signature watermark. The CF between the embedded Gabor face and extracted Gabor face at each stage for different test cases is displayed in table 3.

Similarity Factor (SF) between embedded speech watermark and extracted speech watermark at different stages for different test cases is tabulated table 4.

In re-watermarking scheme, the interference of successive watermark keeps on increasing with each other and correlation of extracted watermark with original one keep on decreasing (Mark *et al* 2007). As mentioned by Sheppard *et al* (2001), the expected value of correlation drops by a factor of $\sqrt{2}$, that is there is 30% decrease in expected value. As reported by Mascher-Kampfer *et al* (2006), in case of non-blind algorithm correlation of extracted watermark which



(a) Lena image with multiple watermark.

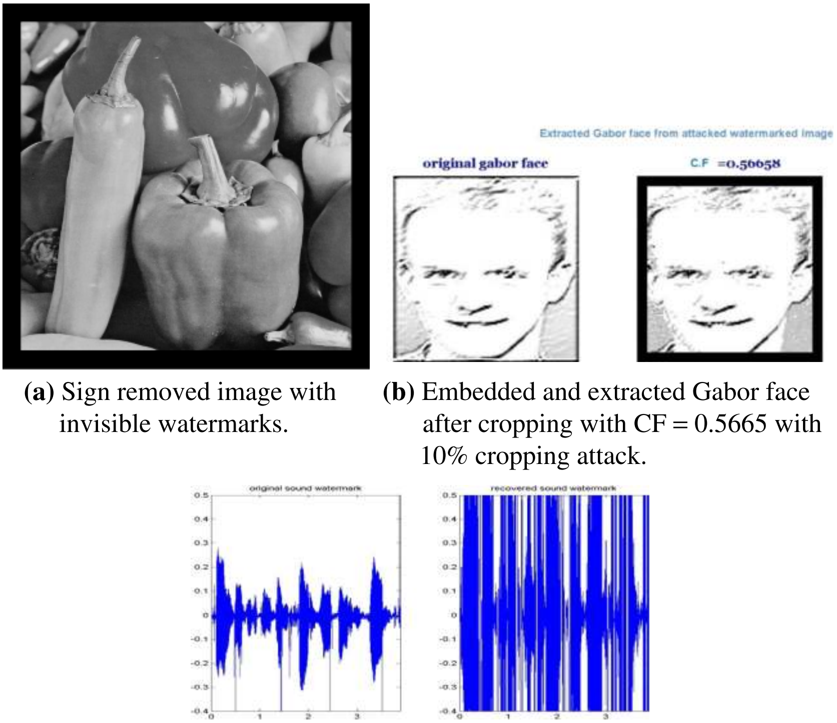
(b) Peppers image with multiple watermark.

(c) Goldhill image with multiple watermarks.

Figure 10. Watermarked images with multiple invisible and visible watermarks.

Table 2. PSNR of watermarked images at different stages for multiple watermarked technique.

	PSNR in dB			
Images	Face water marked image	Face speech watermarked image	Face speech signed image	Sign removed image
Lena	36.6691	35.9289	35.1819	35.9049
Boat	35.4132	34.0289	33.2819	34.0069
Peppers	36.6885	36.1221	34.5005	36.1595
Camera	30.8656	30.4181	25.6308	30.4022
Matheran	44.3626	40.5639	39.1878	40.5378
Hat	31.6214	31.4171	26.8725	31.3892
Baboon	30.4592	28.1408	25.2655	28.1254
Goldhill	37.0582	36.0378	32.4872	36.0045



(a) Sign removed image with invisible watermarks.

(b) Embedded and extracted Gabor face after cropping with CF = 0.5665 with 10% cropping attack.

(c) Extracted speech from attacked image.

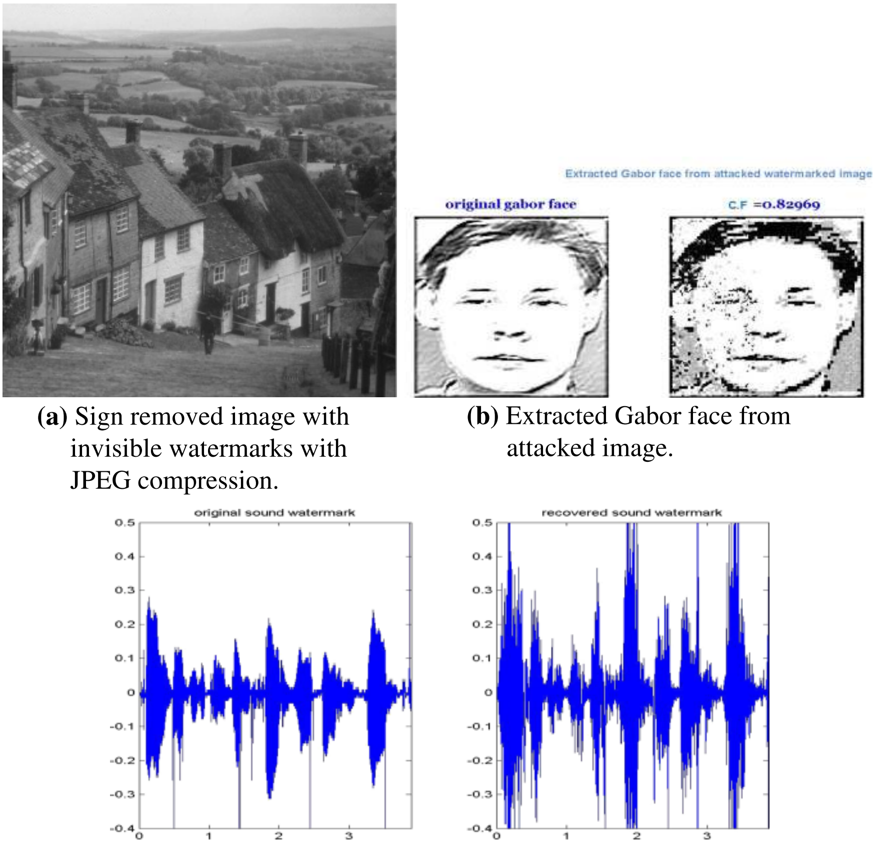
Figure 11. Attacked image with cropping attack at fourth stage and extracted watermarks.

is embedded very first is poor because for extraction original reference image is required and watermarks which are inserted at later stage simply acts as a noise.

In the proposed scheme, the correlation of extracted Gabor face at first stage and second stage is intact. However, correlation of Gabor face is decreased after embedding visible watermark by 8.6% at third stage and at fourth stage is dropped by 4.8%. SF of extracted speech watermark at third stage is decreased by 7.6% while at fourth stage it is decreased by 1.5%. Comparative table of average of percentage decrease in CF at difference stages of Mark *et al* (2007) scheme, Mascher-Kampfer *et al* (2006) proposed the scheme which is presented in table 5. Non-blind watermarking technique with only three stages of re-watermarking are considered here for comparison. Sheppard *et al* (2001) did not reveal any experimentation details.

Compared to results reported by Mark *et al* (2007), Mascher-Kampfer *et al* (2006) and Sheppard *et al* (2001), our approach outperforms with respect to correlation of extracted watermark.

It is due to the fact that we have selected wavelet packet transform to embed the Gabor face at selected band deep down the tree, while speech is embedded at very 1st level of decomposition. Secondly, watermark strength is kept within a range of 0.5–1 for inserting Gabor face and while for that speech, strength is within a range of 2–5. These two strategies used for implementation results in less interference of watermark with each other and do not allow to degrade the correlation of extracted watermark at successive stage of watermarking.



(a) Sign removed image with invisible watermarks with JPEG compression.

(b) Extracted Gabor face from attacked image.

(c) Extracted speech from attacked image.

Figure 12. Attacked image with JPEG compression at fourth stage and extracted watermarks.

Table 3. CF of Gabor face at different stages.

	CF of extracted Gabor face					
Images	From face watermarked image	From face speech watermarked	From visibly signed image (3rd stage)	From sign removed image (4th stage)	% decrease in CF at 3rd stage	% decrease in CF at 4th stage
Lena	0.964	0.964	0.8931	0.9132	7.42	5.33
Boat	0.963	0.9631	0.9337	0.9558	3.05	0.75
Peppers	0.973	0.973	0.9572	0.9687	1.71	0.53
Camera	0.991	0.991	0.9111	0.9662	8.18	2.55
Matheran	0.919	0.919	0.9113	0.9173	0.87	0.21
Hat	0.991	0.991	0.8525	0.9792	14.02	1.25
Goldhill	0.971	0.971	0.8867	0.9102	8.70	6.29

Table 4. SF of speech face at different stages.

	SF of extracted speech watermark				
Images	From face and speech watermarked image	From visibly signed image	From sign removed image	% decrease in SF at 3rd stage	% decrease in SF at 4th stage
Lena	0.935	0.88	0.933	5.08	0.21
Boat	0.977	0.812	0.9458	16.89	3.25
Peppers	0.940	0.864	0.927	8.12	1.42
Camera	0.961	0.864	0.956	10.08	0.55
Matheran	0.939	0.855	0.909	8.85	3.17
Hat	0.946	0.944	0.946	0.21	0.02
Goldhill	0.935	0.887	0.933	5.15	0.17

Table 5. Comparative of proposed scheme with earlier work.

Parameter for comparison	Mark *et al* (2007) scheme	Mascher-Kampfer *et al* (2006) scheme	Proposed scheme
Type of watermark	Pseudorandom sequence	Pseudorandom sequence	Biometric trait
Watermark detection/extraction	Detection	Detection	Extraction
Percentage decrease in CF of extracted watermark inserted at second stage	35%	32%	7.6%
Percentage decrease in CF of extracted watermark inserted at 1st stage	43%	42%	8.6%

4. Conclusion and future scope

In this paper, we have proposed a novel way for protecting and authenticating visibly marked images. We have presented dual and multiple data hiding technique by using an amalgamation of biometric characteristics for recognition and authentication and watermarking for copy protection and ownership proof. We have presented different approaches for multiple watermarking scheme and their limitations from implementation point of view. We have demonstrated that in case of re-watermarking, using different frequency band, watermark interference with each other can be reduced substantially. Visible watermarking which allows the lossless recovery of original host image provides the identity of ownership. The ownership of visibly marked media is in question, either or both invisible biometric watermarks can be extracted to prove the ownership. Under different attacks at least one of the watermarks will be survived. The current study can be extended to make the algorithm robust against geometric attacks like rotation and scaling.

References

Allah M M A 2007 Embedding biometric data for secure authentication watermarking. *Proc. Fourth IASTED internat. conf. Signal Processing, Pattern Recognition and Appl.*, 191–196

Bhatnagar G and Raman B 2012 Wavelet packet transform-based robust video watermarking technique. *Sadhana* 37(3): 371–388

Feng G and Lin Q 2007 Iris feature based watermarking algorithm for personal identification. *Proc. MIPPR Remote sensing and GIS data Proc. Appl.*, vol. 6790, 5

Hammerle-Uhe J, Liedlgruber M, Uhl A and Wernisch H 2008 Multiple re-watermarking Using Varying Wavelet Packets, pp. 213–216, ICME

Hassanien A E 2007 Hiding iris data for authentication of digital images using wavelet theory. *ICGST International journal of Graphics, Vision and Image processing* (*GVIP special issue on iris recognition*), vol. 17, 27–32

Hong L and Jain A 1998 Integrating faces and fingerprints for personal identification. *IEEE Trans. Pattern Anal. Mach. Intell.* 20(12): 1295–1307

Hu Y, Kwong S and Huang J 2004 Using invisible watermarks to protect visibly watermarked images. *Proc. Internat. Symp. Circuits and Systems (ISCAS '04)*, vol. 5, 584–587

Hu Y, Kwong S and Huang J 2006 An algorithm for removable visible watermarking. *IEEE Trans. Circuits Syst. Video Technol.* 16(1): 129–133

Hu Y and Jeon B 2006 Reversible visible watermarking and lossless recovery of original images. *IEEE Trans. Circuits Syst. Video Technol.* 16(11): 1423–1429

Huang B B and Tang S X 2006 A contrast sensitive visible watermarking scheme. *IEEE J. Multi.* 13(2): 60–66

Inamdar V S, Rege P and Bang A 2009 Speech Based Watermarking for Digital Images. *IEEE Internat. Conf. TENCON*, Singapore

Jain A K, Uludag U and Hsu R-L 2002a Hiding a face in a fingerprint image. *Proc. 16th Internat. Conf. Pattern Recognition*, 3: 756–759

Jain A K and Uludag U 2002b Hiding fingerprint minutiae in images. *Proc. third Workshop Automatic Identification Advanced Technologies*, 97–102

Jain A K and Uludag U 2003a Hiding biometric data. *IEEE Trans. Pattern Anal. Mach. Intell.* 25(11): 1494–1498

Jain A K and Uludag U 2003b Multimedia content protection via biometric based encryption. *IEEE proc. Internat. Conf. Multimedia and Expo, ICME*, Baltimore, USA, vol. 3

Jakimoski G and Kocarev L 2001 Chaos and cryptography: block encryption ciphers based on chaotic maps. *IEEE Trans. Circuits Syst. Fundamental Theory Appl.* 48(2): 163–169

Jung S, Lee D, Lee S and Paik J 2007a Biometric data based robust watermarking scheme of video streams. *Proc. IEEE 6th internat. conf. Inform., Commun. Signal Process.*, Singapore

Jung S, Lee D, Lee S and Paik J 2007b Fingerprint watermarking for H.264 streaming media. *Frontiers in the Convergence of Biosci. Inform. IEEE Conf.*, 671–675

Kamarainen J-K, Kyrki V and Kalviainen H 2006 Invariance properties of Gabor filtering based features overview and applications. *IEEE Trans. Image Process.* 15(5): 1088–1099

Kumhom P and Chamnongthai K 2004 Image watermarking based on wavelet packet transform with best tree. *Trans. Elect. Eng. Electron. Commun.* 2(1): 23–35

Liu S H, Yao H-X, Gao W and Liu Y-L 2007 An image fragile watermark scheme based on chaotic image pattern and pixel-pairs. *Appl. Math. Comput.* 185(2): 869–882

Low C Y and Teoh A B J 2007 A preliminary study on biometric watermarking for offline handwritten signature. *Proc. 2007 IEEE Internat. Conf. Commun.*, 691–695

Low C Y, Teoh A B-J and Tea C 2008a Fusion of LSB and DWT biometric watermarking for offline handwritten signature, 2008 Congress on Image and Signal processing, *IEEE Comp. Soci.*, 702–708

Low C Y, Teoh A B-J and Tea C 2008b Support Vector Machines (SVM) based biometric watermarking for offline handwritten signature. *Proc. 3rd IEEE conf. Indust. Electro. appl., ICIEA*, Singapore, 2095–2100

Mark D, Uhl A and Werniisch H 2007 Experimental study on watermark interference in multiple re-watermarking. *Security, Steganography and Watermarking of Multimedia Contents Ix*, San Jose, CA, USA, vol. 6505

Mascher-Kampfer A, Stonger H and Uhl A 2006 Multiple Re-Watermarking Scenarios. *Proc. 13th Internat. Conf. Systems, Signals and Image processing IWSSIP*, Budapest, Hungary, 53–56

Mohanty S P, Ramakrishnan K and Kankanhalli M 1999 *A dual watermarking technique for images*. ACM Multimedia Orlando, Florida, 49–51

Nagamalleswara Rao N, Trimurthy P and Raveendra Babu B 2009 A Novel scheme for digital rights management of images using biometrics. *IJCSNS Int. J. Comput. Sci. Netw. Sec.* 9(3): 157–167

Namboodiri A and Jain A 2004 Multimedia document authentication using online signatures as watermarks. *Security, Steganography and Watermarking of Multimedia Contents VI* 5306: 653–662

Noore A, Singh R, Vasta M and Houck M 2007 Enhancing security of fingerprints through contextual biometric watermarking. *Proc. Forensic Sci. Int.* 169: 188–194

Rajbul I, Shohel S and Samraj A 2007 Multimodality to improve security and privacy in fingerprint authentication system. *Proc. Internat. Conf. intelligent and Advanced Systems* 753–752

Salleh S I and Isnin I F 2002 Ciphering key of chaos image encryption. *Proc. Internat. Conf. AI and Engineering Technol.*, (Sabah, Malaysia), UNIMAS

Shen L and Bai L 2006 Information theory for Gabor feature selection for face recognition, Hindawi publishing Corporation. *EURASIP J. Appl. Signal Process.* 2006: 1–12

Sheppard N P, Safavi-Naini R and Ogunbona P 2001 On multiple watermarking. *Proceedings of the ACM Multimedia and Security Workshop 2001 (MMSW-01)*, ACM Press, Ottawa, Canada, 3–6

Struc V and Pavesic N 2010 The Complete Gabor Fisher classifier for robust face recognition, Hindawi publishing Corporation. *EURASIP J. Advances Signal Process.* 2010: 1–27

Vatsa M, Singh R and Noore A 2005 Improving biometric recognition accuracy and robustness using DWT and SVM Watermarking. *IEICE Electronics Express* 2(12): 362–367

Vatsa M, Singh R and Noore A 2006 Robust biometric image watermarking for fingerprint and face template protection. *IEICE Electronics Express* 3(2): 23–28

Vatsa M, Singh R and Noore A 2009 Feature based RDWT watermarking for multimodal biometric system. *Science Direct, Image and Vision Computing* 27: 293–304

Wan D-S, Li J P and Yan Y-H 2007 A novel authentication scheme of the DRM system based on multimodal biometric verification and watermarking technique. *Proc. Internat. conf. Apperceiving Computing and Intelligence Analysis*, 212–215

Wang H, Cui X and Cao Z 2008 A Speech based Algorithm for Watermarking Relational Databases. *Internat. Symp. Inform. Process.*, Moscow, Russia

Wong P W and Memon N 2001 Secret and public key image watermarking schemes for image authentication and ownership verification. *IEEE Trans. Image Process.* 10: 1593–1601

Yang H, Sun X and Li C-T 2008 Removable visible image watermarking algorithm in the discrete cosine transform domain. *J. Electronic Imaging* 17(3): 033008

Yang Y, Sun X, Yang H, Li C T and Xiao R 2009 A contrast sensitive reversible visible image watermarking technique. *IEEE Trans. Circuits Syst. Video Technol.* 19(5): 656–667