Chapter 7

Dual Watermarking Technique with Multiple Biometric Watermarks

7.1 Introduction

Visible watermarking is important for protecting online resources from unauthorized copying [131, 132, 133, 134]. 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. 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 using dual watermarking strategy. In [135], Mohanty et al. 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 gray-level watermark image, and then, considered the resulting image as a new image to carry out invisible wa-
Invisible watermarking is performed in spatial domain. The fragile watermark consisting of pseudo-random binary sequence (0,1) is EX-ORed with the $k^{th}$ 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. Yongjian [136] suggested dual watermarking method in DWT domain. Secondary image is inserted invisibly into the approximate band at the $4^{th}$ level of wavelet decomposition of host image. Later at second stage, pseudorandom sequence is inserted into the approximate band at the $3^{rd}$ level of wavelet decomposition. In [137], Wong and Memon 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.

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. Multiple invisible watermarks can enhance the protection of the visibly watermarked image. Applications of such scheme are multifold.

### 7.2 Dual Watermarking Scheme Using Multiple Biometric Watermarks such as Face, Speech and Offline Signature

In this technique dual watermarking scheme with multiple biometric watermarks (face, speech and handwritten signature) is proposed. LPC coefficients of owner’s speech and Gabor face are embedded invisibly and then offline signature is overlaid translucently on the image. Such scheme can be used for joint ownership, to prove ownership multiple times or it can also be used for multiple applications. It can also be utilized to embed information concerning both, owner’s speech watermark and end user’s Gabor face. This method proposes multiple biometric re-watermarking scheme. It first embeds the Gabor face in the host image using wavelet packet transform. The band selected for embedding the Gabor face is variable and is selected based on the cost function 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 in DCT domain as proposed by [138]. 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 7.1

7.2.1 Watermark Preparation

As multiple watermarks are inserted, watermark preparation phase consists of face watermark preparation using Gabor filter, LPC encoding of speech watermark and preparation of offline signature watermark.

7.2.1.1 Face watermark preparation

Let FI be an individual face image which is used as a face watermark. As the energy content of such face image is high, embedding such face image directly will degrade the perceptual quality of host image. To overcome this problem, Gabor face is generated through Gabor filtering as discussed in section 6.3.1.2. Filter bank is constructed with 5 scales and 6 orientations. The given face image is filtered with 30 filters. Only the magnitude is used to construct the Gabor face from face image. 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 for 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 is selected as a face watermark. Gabor face is of same size as that of original face image and is denoted as Gabor face watermark $W_{GF}$.

7.2.1.2 Speech watermark preparation

As the speech file contains large number of samples, LPC encoding technique as discussed in section 4.4.1 is applied to reduce the dimensionality of speech watermark.
Figure 7.1: Framework for multiple biometric watermark insertion

[Diagram showing the process of watermark insertion and removal, including stages for Gabor face insertion, wavelet transform, and visible watermark removal.]
7.2.1.3 Signature watermark preparation

Signature watermark preparation consists of preprocessing of signature image with some secret key. 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 scheme for preprocessing the original watermark [139]. Using a key and a chaotic sequence, variant of signature watermark is generated. The generation of such a watermark is key controlled. Without the secret key the same variant of the original watermark cannot be derived. 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 seed [140]. Chaotic logistic map as given by Equation 7.1 is used.

\[ X_{n+1} = \lambda x_n (1 - x_n) \]  

Using a secret key \( K \) in the range (0,1) as initial value \( x_0 \), a chaotic sequence (\( x_1, x_2, x_3, \ldots \)) is generated. \( \lambda \) is a positive number which determines the characteristics of ‘X’. \( \lambda \) is chosen in the range of 3.57 to 4 [141]. The signature image \( W_{sgn} \) 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 wrapped to form 2-D 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.

7.2.2 Watermark Embedding

As depicted in Figure 7.1 watermark insertion is done successively, first Gabor face is inserted which produces a face watermarked image \( I_{wF}^w \). In the second stage LPC coefficients of speech are embedded into the face watermarked image which generates a watermarked image \( I_{wFS}^w \) with multiple watermarks. In the final stage, signature image is overlaid translucently on \( I_{wFS}^w \) to generate dual watermarked image \( I_{wFSvsgn}^w \). These steps are described in the subsequent section.
7.2.2.1 Gabor face insertion

This stage embeds Gabor face into the host image by utilizing a multi resolution analysis using Wavelet Packet Transform (WPT). WPT is a generalization of the wavelet transform. In wavelet decomposition, usually only low frequency band is further decomposed because it contains most of the information of the signal. In 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. For ‘l’ level decompositions there are $4^l$ different ways to encode the image which provide a better tool for image analysis. Figure 7.2 shows the full quadtree describing the wavelet packet transform with 2 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 WPT. For example, watermark which is a Gabor face, is of size $128 \times 128$ and if host image is of size $1024 \times 1024$, a subband at level 3 is selected for watermark casting. 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

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

(7.2)

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

![Figure 7.2: Full quad tree of 2 level WPT](image)

**Band selection strategy**

The level of decomposition of WPT is dictated by size of the host image and size of wa-
termark image (Gabor face) and there are $4^l$ subbands at $l^{th}$ level. One of the bands at the highest level is selected for watermark insertion based on best band selection strategy [44]. Data loss may occur during watermark insertion and removal due to forward and backward DWT transform. In our work, PSNR of the extracted watermark which is a Gabor face is used for determining the exact band for watermark insertion. Watermark is inserted recursively in all bands at highest level. 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 selecting band for Gabor face insertion gives good perceptual quality of extracted watermark when multiple watermarks are embedded at later stage.

Gabor face insertion process consists of following steps:

1. Decompose the image using WPT to the $l^{th}$ level. The level ‘l’ is governed by size of host image and size of Gabor face.

2. Select a particular band using band selection strategy.

3. In a selected band, insert the Gabor face using Equation 7.3

$$\hat{I}_l(i,j) = I(i,j) + \alpha W_{GF}(i,j)$$ (7.3)

Where $I_l(i,j)$ are the coefficients of host image of selected band at $l^{th}$ level.

$\hat{I}_l(i,j)$ are modified coefficients at $l^{th}$ level subband.

$W_{GF}(i,j)$ are coefficients of Gabor face which is used as a watermark.

4. Apply inverse wavelet transform to get face watermarked image $I_w^F$ which is given as input to second stage for speech insertion.

### 7.2.2.2 Speech watermark insertion

This stage aims to embed biometric trait, speech which corresponds to the identity of owner as a watermark in the image which is already watermarked with Gabor face. Algorithm for speech embedding is as follow:

1. Apply linear predictive coding on speech samples to generate LPC coefficients.

2. Apply the wavelet transform on face watermarked image $I_w^F$ 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 $L_w$ wavelet coefficients, where $L_w$ is chosen to be equal to length of LPC coefficients generated.

4. Insert the LPC coefficients into selected wavelet coefficients using Equation 7.4

$$\hat{I}_F^W(i,j) = I_F^W(i,j)(1 + \alpha W_s^i)$$  (7.4)

Where $W_s^i$ = the $i^{th}$ value of speech watermark.

$I_F^W(i,j)$ = the original wavelet coefficients of face watermarked image.

$\hat{I}_F^W(i,j)$ = modified wavelet coefficients after embedding LPC coefficients.

$\alpha$ = the strength of the watermark.

5. Generate the watermarked image $I_{FS}^w$ by applying the inverse wavelet transform.

7.2.2.3 Visible signature insertion

The host image at this stage is the invisibly watermarked image $I_{FS}^w$. For further simplicity the superscript/subscript is omitted. This image is referred as cover image ‘I’. Depending upon the size of covered image which is to be watermarked visibly, preprocessed signature $W_p^{sgn}$ 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 overlaid is considered. The Region of Interest(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 signature watermark. Equation 7.5 is employed to overlay the signature on host image.

$$\hat{I}_{sub}^m(i,j) = \alpha_m \times I_{sub}^m(i,j) + \beta_m \times W_{sgn_m}^p(i,j) \quad m = 0.....N_B$$  (7.5)

Where $\hat{I}_{sub}^m(i,j)$ denote the modified DCT coefficients of $m^{th}$ block of ROI of host image. $I_{sub}^m(i,j), W_{sgn_m}^p(i,j)$ denote the $(i,j)^{th}$ DCT coefficient of the $m^{th}$ $8 \times 8$ element block of watermarked host sub-image $I_{sub}$ and preprocessed watermark $W_{sgn}$ respectively.

$\alpha_m$ and $\beta_m$ 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 $N_B$ is the total number of blocks.

### 7.2.2.3.1 Determination of scaling and embedding factor:

While formulating scaling and embedding factors $\alpha_m$ and $\beta_m$, 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 modeling the scaling and embedding factors. The blocks with mid-luminance intensities are more sensitive to noise. Assigning greater value of the scaling factor $\alpha_m$ for mid-luminance area and attenuating its value for darker and brighter blocks is desirable. Scaling factor $\alpha_m$ exhibits Gaussian distribution with the luminance value of $m^{th}$ block. Most of the energy is concentrated into DC coefficient which is the luminance. Scaling factor is calculated as

$$\alpha_m = \frac{1}{\sqrt{2\pi(\sigma_1^2 + \sigma_2^2)}} \exp\left(-\frac{(l_m - (\mu_1 + \mu_2))^2}{2(\sigma_1^2 + \sigma_2^2)}\right)$$  \hspace{1cm} (7.6)

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

$$l_m = I_{sub}^m(0,0) + W_{sgn}^p(0,0) \quad m = 1, 2, 3, ..., N_B$$  \hspace{1cm} (7.7)

Mean value $\mu_1$ and variance $\sigma_1$ of the DC Coefficients of the host sub-image are found out respectively as

$$\mu_1 = \frac{1}{N_B} \sum_{m=1}^{N_B} I_{sub}^m(0,0)$$  \hspace{1cm} (7.8)

and

$$\sigma_1 = \frac{1}{N_B} \sum_{m=1}^{N_B} [I_{sub}^m(0,0) - \mu_1]^2$$  \hspace{1cm} (7.9)

In the same manner, mean value $\mu_2$ and variance value $\sigma_2$ 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 tend 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 $\alpha_m$ is in direct proportion to the $m^{th}$ block variance of the host sub-image $I_{\text{sub}}$ and preprocessed watermark $W_{\text{psg}}$. Thus Scaling factor is proportional to $v_m$, where $v_m = v^h_m + v^w_m$, where $v^h_m$ and $v^w_m$ 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 7.6 is modeled as

$$
\alpha_m = \frac{1}{\sqrt{2\pi(\sigma_1^2 + \sigma_2^2)}} \exp\left(-\frac{(I_m - (\mu_1+\mu_2))^2}{2(\sigma_1^2 + \sigma_2^2)}\right)
$$

(7.10)

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

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

(7.11)

$\bar{v}_m$ in Equation 7.11 is the natural logarithm of $v_m$. Normalization and natural logarithm is taken so as to control scaling factor $\alpha_m$ in a narrow range.

Variances $v^h_m,v^w_m$ are calculated for the host image and preprocessed watermark by considering only the insignificant coefficients of preprocessed watermark and corresponding coefficients of ROI of host image. Coefficients are deemed to be insignificant if its 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 $I_{\text{sub}}$ which facilitates its retrieval for estimation of two parameters $\alpha_m$ and $\beta_m$ during watermark removal process without referring to original image. $s^r_m$ denote the sub set of $S_m$ after removing one element. There is only one element in $S_m - s^r_m$ and its coordinates are also denoted by $S_m - s^r_m$. Hence to find out the variance $v^h_m$ of the $m^{th}$ block of host sub-image $I_{\text{sub}}$, coefficients in set $s^r_m$ are considered. Equation 7.12 gives the variance of the $m^{th}$ block of host sub-image.

$$
v^h_m = \frac{1}{N} \sum_i \sum_j (I_{\text{sub}}^{i,j} - \mu_{AC})^2
$$

(7.12)
Where $N$ is the total number of insignificant coefficients in set $s^r_m$ and $\mu_{AC}$ is their mean and is calculated as follow.

$$\mu_{AC} = \frac{1}{N} \sum_i \sum_j I^s_{i,j}$$

(7.13)

In the same manner, variance $\nu^{wp}_{m}$ of preprocessed watermark $W^p_{sgn}$ is calculated. Coefficients corresponding to same locations as that of $s^r_m$ are considered for calculation. Embedding factor $\beta_m$ is calculated as follow:

$$\beta_m = 1 - \alpha_m$$

(7.14)

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

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

2. Divide both host sub-image and preprocessed watermark into $8 \times 8$ block and apply DCT on it.

3. For each host sub-image block $I^s_{m}$ and preprocessed watermark block $W^p_{sgn}$ generate the watermarked image block $I^w_{m}$ by adding significant coefficients of host subimage to that of corresponding coefficients of preprocessed signature watermark using Equation 7.5.

4. Hide the value $\frac{\beta_m \times [I^s_{m}(0,0) - W^p_{sgn}(0,0)]}{10}$ into the $(S_m - s^r_m)_{th}$ coordinate of the watermarked image block $I^w_{m}$ for facilitating the retrieval of the DC coefficient of the host image block $I^s_{m}$ from the marked image block $I^w_{m}$ during the watermark removal process.

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 $I^w_{FSesgn}$. 
During watermark insertion process, only significant coefficients of preprocessed water-
mark are embedded into the corresponding coefficients of host sub-image. Most of the
energy of preprocessed watermark is concentrated in 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 $v_{wp}^{up}$ and $v_{hp}^{up}$ only insignificant
coefficients of signature watermark and corresponding coefficients of host subimage are
used. The reason for such segregation is that as the insignificant coefficients remain intact
during embedding process, $\alpha_m$ and $\beta_m$ can be estimated by using these coefficients directly
from the watermarked image $I_{FSvsgn}$ without referring the original host image. DC coeffi-
cient of each block of host image will help in estimating $\alpha_m$ and $\beta_m$. It is scaled down to
avoid the degradation of watermark image before embedding.

### 7.2.3 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 which is called as ‘vaccine’ program that is made 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
a 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 resulting
in tampering of watermarked image while removing the visible watermark. This is because
the embedded watermark version depends on the private key and an unauthorized user has
no idea about which watermark version should be subtracted from the watermarked image.
Process of visible watermark removal program from multiple watermarked image $I_{FSvsgn}^w$
(for simplicity the subscript is omitted and simply called as $I^w$) is as follow. 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:
1. Generate the preprocessed signature watermark \( W_{sgn}^p \) using the private key \( k \).

2. Divide the preprocessed watermark \( W_{sgn}^p \) and ROI of watermarked image \( I^w \) into non-overlapping \( 8 \times 8 \) pixel blocks and apply DCT transform on these blocks.

3. For each watermarked image block \( I^w_m \) repeat the step 4 to 5.

4. Select the \((i,j)\)th DCT coefficient, where \((i,j)\) corresponds to the \( S_m - s_m^r \) and find out approximate value of DC coefficient of \( m^{th} \) block of original host sub-image as \( I^w_m(i,j) \times 10 + I^w_m(0,0) \).

   This can be derived as follow:

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

   Equation \( I^w_m(i,j) = \beta_m \times \frac{[I^w_m(0,0) - W_{sgn_m}(0,0)]}{10} \) will lead to

   \[
   I^w_m(i,j) \times 10 + \beta_m \times W_{sgn_m}(0,0) = \beta_m \times I^{sub}(0,0) \quad (7.15)
   \]

   Equation 7.5 of watermark insertion corresponds to DC coefficients is

   \[
   I^w_m(0,0) = \alpha_m \times I^{sub}(0,0) + \beta_m \times W_{sgn_m}(0,0) \quad (7.16)
   \]

   Substituting value of \( \beta_m \times W_{sgn_m}(0,0) \) in Equation 7.16

   \[
   I^w_m(i,j) \times 10 + I^w_m(0,0) - \alpha_m \times I^{sub}(0,0) = \beta_m \times I^{sub}(0,0) \quad (7.17)
   \]

   \[
   I^w_m(i,j) \times 10 + I^w_m(0,0) = \beta_m \times I^{sub}(0,0) + \alpha_m \times I^{sub}(0,0) \quad (7.18)
   \]

   As \( \alpha_m + \beta_m = 1 \)

   \[
   I^w_m(i,j) \times 10 + I^w_m(0,0) = I^{sub}(0,0) \quad (7.19)
   \]

5. Select the DCT coefficients from the watermarked image corresponds to the set \( s_m^r \) and we get \( I^{sub}(i,j) = I^w_m(i,j) \). These correspond to insignificant coefficients of host sub-image as only significant coefficients are considered for watermark insertion.

6. Using approximate DC coefficients as calculated in step 4, and DC coefficients of
preprocessed watermark $W_{\text{sgm}}^p$ model $\alpha_m$ as per Equation 7.6 to 7.9.

7. Using the insignificant coefficients of host sub-image which are found out in step 6 and that of processed watermark $W_{\text{sgm}}^p$, find out $v_{m}^h$ and $v_{m}^{wp}$. Update the scaling factor by $\alpha_m$ by plugging it with normalized version of $v_m$ as calculated by Equation 7.10. Also find out $\beta_m$.

8. Obtain the unmarked image by removing the significant DCT coefficients of preprocessed signature watermark $W_{\text{sgm}}^p$ from the marked image $I^w$ using the Equation 7.20

$$I_{\text{sub}}^m(i,j) = I^m_{w}(i,j) - \frac{\beta_m \times W_{\text{sgm}}^p(i,j)}{\alpha_m} \quad \text{for } i = 1, 2, \ldots, 8; \quad j = 1, 2, \ldots, 8; \quad m = 1, 2, \ldots, N_B$$ (7.20)

These recovered coefficients are integrated with the other part of image to get visible signature removed image.

### 7.2.4 Experimentation and Results

#### 7.2.4.1 Data payload

In this technique payload varies at different stages of watermarking as multiple watermarks are embedded into different frequency bands. In the First stage of watermarking, Gabor face is inserted into one of the band of wavelet decomposition. The size of Gabor face is same as that of face image, while its entropy is much less than original face. This avoids degradation of perceptual quality of watermarked image. Original image and its Gabor face are shown in Figure 7.3.

At the second stage of watermarking, speech watermark of maximum 7 seconds duration, which is LPC encoded is embedded into LH band of the image. At last stage signature image which varies between $60 \times 30$ to $120 \times 120$ is overlaid translucently on the pre-watermarked image.
7.2.4.2 Results

With reference to Figure 7.2, Table 7.1 shows the band selected for Gabor face insertion for different host images with different faces. A sample of face watermarked image and embedded and extracted Gabor face is shown in Figure 7.4.
At the second stage of watermarking, the face watermarked image is watermarked with speech. Figure 7.5 shows multiple invisible watermarked image along with embedded and extracted face and speech watermark at second stage.

![Sample output at second stage of multiple watermarking technique](image)

**Table 7.1: Selection of band for different host images with different face image**

<table>
<thead>
<tr>
<th>Host</th>
<th>Face1</th>
<th>Face2</th>
<th>Face3</th>
<th>Face4</th>
<th>Face5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baboon (256 × 256)</td>
<td>$X_{1,1}$</td>
<td>$X_{1,0}$</td>
<td>$X_{1,2}$</td>
<td>$X_{1,1}$</td>
<td>$X_{1,1}$</td>
</tr>
<tr>
<td>boat (512 × 512)</td>
<td>$X_{2,0}$</td>
<td>$X_{2,0}$</td>
<td>$X_{2,0}$</td>
<td>$X_{2,0}$</td>
<td>$X_{2,1}$</td>
</tr>
<tr>
<td>Goldhill (512 × 512)</td>
<td>$X_{2,0}$</td>
<td>$X_{2,10}$</td>
<td>$X_{2,6}$</td>
<td>$X_{2,0}$</td>
<td>$X_{2,10}$</td>
</tr>
<tr>
<td>Peppers (512 × 512)</td>
<td>$X_{2,8}$</td>
<td>$X_{2,14}$</td>
<td>$X_{2,0}$</td>
<td>$X_{2,0}$</td>
<td>$X_{2,15}$</td>
</tr>
<tr>
<td>Matheran (1024 × 1024)</td>
<td>$X_{3,0}$</td>
<td>$X_{3,11}$</td>
<td>$X_{3,34}$</td>
<td>$X_{3,4}$</td>
<td>$X_{3,21}$</td>
</tr>
<tr>
<td>Leena (512 × 512)</td>
<td>$X_{2,12}$</td>
<td>$X_{2,2}$</td>
<td>$X_{2,15}$</td>
<td>$X_{2,5}$</td>
<td>$X_{2,15}$</td>
</tr>
</tbody>
</table>

Figure 7.5: Sample output at second stage of multiple watermarking technique
At the third stage of testing, the image which is invisibly watermarked with face and speech is visibly marked with the signature of owner. Figure 7.6 shows the image which is marked visibly and invisibly multiple times and extracted speech and face watermark at this stage.

(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

Figure 7.6: Sample output at third stage of multiple watermarking technique
At fourth stage of testing, overlaid visible watermark is removed, which still contains multiple invisible watermarks, speech and Gabor face. Figure 7.7 shows signature recovered images which still contains face and speech invisible watermarks.

![Signature recovered image with PSNR 34.0069dB](image)

(b) Extracted face watermark at fourth stage

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

Figure 7.7: Signature recovered image with embedded and extracted Gabor face and speech watermark at fourth stage

Few more output samples of multiple watermarked images along with embedded and extracted Gabor face, embedded and extracted speech (at 3rd stage) and signature image which is overlaid translucently are shown in Figure 7.8 to 7.10.
Figure 7.8: Lena image with multiple biometric watermarks and extracted watermarks
Figure 7.9: Pepper image with multiple biometric watermarks and extracted watermarks
Figure 7.10: Goldhill image with multiple biometric watermarks and extracted watermarks
Table 7.2 shows the average PSNR for different test images at different stages of watermarking. The average C.F between the embedded Gabor face and extracted Gabor face at each stage and percentage drop of C.F at 3rd and 4th stage for different images is shown in Table 7.3. An average S.F between embedded speech vector and extracted speech vector at different stages and percentage drop of S.F at 3rd and 4th stage for different test cases is tabulated Table 7.4.

Table 7.2: PSNR of watermarked images at different stages for multiple watermarked technique

<table>
<thead>
<tr>
<th>Images</th>
<th>PSNR in dB</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Face Watermarked Image (1st stage)</td>
<td>Face, speech Watermarked Image (2nd stage)</td>
<td>Face, speech Signed Image (3rd stage)</td>
<td>Sign Removed Image (4th stage)</td>
<td></td>
</tr>
<tr>
<td>Lena</td>
<td>36.6991</td>
<td>35.9289</td>
<td>35.1819</td>
<td>35.9049</td>
<td></td>
</tr>
<tr>
<td>Boat</td>
<td>35.4132</td>
<td>34.0289</td>
<td>33.2819</td>
<td>34.0069</td>
<td></td>
</tr>
<tr>
<td>Pepper</td>
<td>36.6885</td>
<td>36.1221</td>
<td>344.5005</td>
<td>36.1595</td>
<td></td>
</tr>
<tr>
<td>Camera</td>
<td>30.8656</td>
<td>30.4181</td>
<td>25.6308</td>
<td>40.4022</td>
<td></td>
</tr>
<tr>
<td>Matherann</td>
<td>44.3626</td>
<td>40.5639</td>
<td>39.1878</td>
<td>40.5378</td>
<td></td>
</tr>
<tr>
<td>Hat</td>
<td>31.6214</td>
<td>31.4171</td>
<td>26.8725</td>
<td>31.3892</td>
<td></td>
</tr>
<tr>
<td>Baboon</td>
<td>30.4592</td>
<td>28.1408</td>
<td>25.2655</td>
<td>28.1254</td>
<td></td>
</tr>
<tr>
<td>Goldhill</td>
<td>37.0592</td>
<td>36.0378</td>
<td>32.4872</td>
<td>36.0045</td>
<td></td>
</tr>
</tbody>
</table>

Table 7.3: C.F of Gabor face at different stages

<table>
<thead>
<tr>
<th>Images</th>
<th>C.F. of extracted Gabor Face</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>from Face Watermarked Image (1st stage)</td>
<td>from face, speech Watermarked Image (2nd stage)</td>
<td>from visibly signed image (3rd stage)</td>
<td>from Sign Removed Image (4th stage)</td>
<td>% drop in C.F. at 3rd stage</td>
</tr>
<tr>
<td>Lena</td>
<td>0.9647</td>
<td>0.9647</td>
<td>0.8931</td>
<td>0.9132</td>
<td>7.42</td>
</tr>
<tr>
<td>Boat</td>
<td>0.96312</td>
<td>0.96312</td>
<td>0.93371</td>
<td>0.9558</td>
<td>3.05</td>
</tr>
<tr>
<td>Pepper</td>
<td>0.9739</td>
<td>0.9739</td>
<td>0.9572</td>
<td>0.9687</td>
<td>1.71</td>
</tr>
<tr>
<td>Camera</td>
<td>0.9915</td>
<td>0.9915</td>
<td>0.9111</td>
<td>0.9662</td>
<td>8.18</td>
</tr>
<tr>
<td>Matherann</td>
<td>0.9193</td>
<td>0.9193</td>
<td>0.9113</td>
<td>0.9173</td>
<td>0.87</td>
</tr>
<tr>
<td>Hat</td>
<td>0.9916</td>
<td>0.9116</td>
<td>0.8525</td>
<td>0.9792</td>
<td>14.02</td>
</tr>
<tr>
<td>Goldhill</td>
<td>0.9713</td>
<td>0.9713</td>
<td>0.8867</td>
<td>0.9102</td>
<td>8.70</td>
</tr>
</tbody>
</table>
Table 7.4: S.F of speech watermark at different stages

<table>
<thead>
<tr>
<th>Images</th>
<th>S.F. of extracted speech watermark</th>
<th>Images from face, speech watermarked Image (2\textsuperscript{nd} stage)</th>
<th>Images from visibly signed Image (3\textsuperscript{rd} stage)</th>
<th>Images from Sign Removed Image (4\textsuperscript{th} Stage)</th>
<th>% drop in S.F. at 3\textsuperscript{rd} stage</th>
<th>% drop in S.F. at 4\textsuperscript{th} Stage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena</td>
<td>0.9358</td>
<td>0.8882</td>
<td>0.9338</td>
<td>5.08</td>
<td>0.21</td>
<td></td>
</tr>
<tr>
<td>Boat</td>
<td>0.9775</td>
<td>0.8124</td>
<td>0.9458</td>
<td>16.89</td>
<td>3.25</td>
<td></td>
</tr>
<tr>
<td>Pepper</td>
<td>0.9407</td>
<td>0.8643</td>
<td>0.9273</td>
<td>8.12</td>
<td>1.42</td>
<td></td>
</tr>
<tr>
<td>Camera</td>
<td>0.9619</td>
<td>0.8649</td>
<td>0.9566</td>
<td>10.08</td>
<td>0.55</td>
<td></td>
</tr>
<tr>
<td>Matheran</td>
<td>0.9391</td>
<td>0.8559</td>
<td>0.9063</td>
<td>8.85</td>
<td>3.17</td>
<td></td>
</tr>
<tr>
<td>Hat</td>
<td>0.9469</td>
<td>0.9448</td>
<td>0.9647</td>
<td>0.21</td>
<td>0.02</td>
<td></td>
</tr>
<tr>
<td>Goldhill</td>
<td>0.9354</td>
<td>0.8872</td>
<td>0.9338</td>
<td>5.15</td>
<td>0.17</td>
<td></td>
</tr>
</tbody>
</table>

7.2.4.3 Robustness against attacks

Watermarked image at 3\textsuperscript{rd} and 4\textsuperscript{th} stage is tested for robustness against different attacks. Figure 7.11 and Figure 7.12 show the sample of extracted watermark for JPEG compression and cropping attacks.

(a) Image having invisible watermark after removal of signature watermark with JPEG compression

(b) Extracted Gabor face from attacked image

Figure 7.11: continued
Figure 7.11: Attacked image with JPEG compression at fourth stage and corresponding extracted watermarks

(a) Image having invisible watermark after removal of signature watermark with 10% cropping

(b) Extracted Gabor face from attacked image

(c) Extracted speech from attacked image

Figure 7.12: Attacked image with cropping attack at fourth stage and corresponding extracted watermarks

(b) Extracted Gabor face from attacked watermarked image

(c) Extracted speech from attacked image
7.2.5 Observations

- The average PSNR of face watermarked image, face and speech watermarked image, signature overlaid image with face and speech invisible watermarks and signature removed image is 35.43 dB, 34.41 dB, 31.81 dB and 34.35 dB respectively.

- The average C.F of Gabor face and S.F of extracted speech watermark with all watermarks present is 88% and 87% respectively.

- The main objective for development of this technique was to check the feasibility of embedding multiple invisible and visible watermarks and analyze the effect of interference of different watermarks with each other in successive watermarking scheme. Efforts are taken to reduce the interference as far as possible. In successive watermarking scheme, the interference of successive watermarks keep on increasing and correlation of extracted watermark with original watermark keep on decreasing. In case of non blind algorithm correlation of extracted watermark, which is embedded very first, is poor since for extraction, original reference image is required and watermarks which are inserted at later stage simply act as a noise. As mentioned in [142] the expected value of correlation drops by a factor of $\sqrt{2}$, that is there is 30% decrease in expected value. In the proposed scheme, the correlation of extracted Gabor face at 1st stage and 2nd stage is intact. However, correlation of Gabor face is decreased by 6.3% on an average after embedding visible watermark; while at forth stage it is dropped by 2.41%. Similarity Factor of extracted speech watermark at 3rd stage is decreased by 7.7% on an average; while at fourth stage it is decreased by 1.25%. Compared to results reported in [142], our approach outperforms with respect to correlation of extracted watermarks. It is due to the fact that we have selected wavelet packet transform to embed the Gabor face in the band selected deep down the tree, while speech is embedded at very 1st level of decomposition which results in less interference of these two watermarks with each other. Watermark strength is kept within a range of 0.5 to 1 for inserting Gabor face and speech watermark strength is within a range of 2 to 5. These two strategies result in less interference of watermarks with each other and do not allow to degrade the correlation of extracted watermark with original watermark at successive stages of watermarking.
• The purpose of multiple watermarking scheme proposed here is to prove ownership and authentication multiple times or for joint ownership. Common image processing such as compression, filtering, 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, in such cases 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 watermark can survive under different attacks.

7.3 Summary

This chapter discussed about the combination of visible and invisible multiple watermarking methods. In successive watermarking scenario, effect of interference of multiple watermarks with each other was also studied and results derived were also presented. Watermarking method developed is separable as it is possible to extract each watermark individually at each stage and even from the final watermarked object. Visible watermarking technique is a removable technique. 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 can survives under different attacks.