Stationary wavelet transforms based robust audio Watermarking for authentication

S. R. Ganorkar[1]**, Y. D. Chincholkar**[2]
Department of Electronics and Telecommunication Engineering,
Sinhgad College of Engineering
Pune, India

Abstract: In Current scenario internet technology used for releasing and distributing multimedia data over the web, because of this, it is necessary to maintain rights for copyright enforcement and identification. In the present context, the entertainment industry is suffering from financial loss. Hence, the entire music industry is looking for a practical solution that contradicts the work of the owner. We propose in this paper a blind digital audio watermarking technique using biometric traits as a watermark, patchwork method and stationary wavelet transform to enhance and enrich performance characteristics such as piracy, security, imperceptibility, robustness, and computational complexity. In the proposed work, patches and sub patches are created based on selected desired frequency coefficient, which helps for embedding watermark and achieves better performance parameter value. The implanting efficiency of the suggested method is measured at 8 - 9 bps with less computational complexity, and the Bit error rate is near about less than 1 with average SNR more than 24 dB. Experimental outcomes validate that the recovered biometric watermark can be uniquely distinguished in the iris database, even under different attack circumstances.

Keywords: **Stationary Wavelet Transform (SWT), Patchwork method, Biometric trait, imperceptibility, and Computational complexity.**

1. INTRODUCTION

Recently, digital watermarking providing a significant contribution to the field of information security through copyright enforcement and digital right management. Digital watermarking is an art and science of protecting the original data by adding unique data into it in such a way that the third party does not know the presence of confidential data. It can apply to image, text, audio, video, or a 3D model and hence watermarking can be called as image/text/audio/video watermarking [1][2][3]. The information to be incorporated in the original signal is known as a watermark, and it is known as a watermarked signal that holds the watermark behind it. The watermark included in the original signal may visible or non-visible form. How the watermark obtained depends on the nature of digital watermarking. If any actual information or data needed for the recovery of the watermark, then the process is called non-blind, otherwise called blind watermarking process. The basic requirements of any successful audio watermarking algorithm are that it carries large amounts of information in such a way that the information/data of the watermark should not be noticeable to the human ear and withstand watermark even under extreme signal processing attacks. There are six conflicting specification criteria for digital watermarking: payload capacity, imperceptibility, computational complexity, security, and robustness. Within the literature, substantial research has been reported to optimize the balance between the conflicting design criteria for audio watermarking[1].

The first watermarking method for audio was developed by Laurence Boney et al. in 1996. The technique was expanded by Arnold and other researchers for an audio signal using spread spectrum, least significant bits, echo hiding and patchwork method with or without transformation technique. Patchwork techniques show robustness in contradiction of conventional attacks. The audio watermarking explanations available in the current proposed work typically use arbitrary series, binary bit 1 & 0, picture, or logo as a watermark that may not be enough to prove proprietorship or authentication. Similarly, most of the research work is carried out using discrete cosine transform and discrete wavelet transform which offering higher spectral coefficients truncation, Severe blocking artifact and variant in the shift. Because of this, due to the audio scaling attack, it offers low performance and thus reduces robustness. Current watermarking algorithms are trying to maintain ideal stability between imperceptibility, computational complexity, robustness, and payload. However, these algorithms cannot be used for stating that digital watermarks are owned/authenticated [1][6].

In the case of any violation controversy, the use of arbitrary sequence or image as a watermark cannot be kept physically or asserted for proprietorship or authentication, which indicates that watermarking processes for authentication of digital watermarks need to be strengthened. Through biometric features, digital watermark authentication and identification is already reported in some proposed research work [9][14]. The work proposed in [4][7][10-13][16-17] uses of biometric features as a watermark to claim for ownership. For their specific identification, Biometric characteristics have a minimum size that is too large. The experimental outcomes indicate that the correct identification process after extraction of the watermark. Besides, the proposed algorithms described offer good robustness with imperceptible but did not have a broad capacity for embedding and security.

Similarly, they fail to prove robustness against mp3, cropping, de-synchronization, pitch, and time-shifting attacks. There is, therefore, a necessity to offer an optimal solution for stability among design requirements to accommodate biometric watermarks that require greater usefulness than conventional watermarks. This paper's main contribution is to design an audio watermarking algorithm that can incorporate the watermark produced from biometric characteristics, which is usually larger and therefore demands a high watermark payload with low computational complexity and robust against advance attack. In this paper, an ideal balance is achieved between robustness, imperceptibility, security, computational complexity, and payload to implant such a biometric-based watermark. The method proposed is conceived in the frequency domain. The stationary wavelet transformation coefficients are used to embed the watermark on detailed multi-resolution decomposition coefficients at the fifth level.

The paper's respite was organized correspondingly. Section 2 presents the encryption and decoding system based on patchwork and SWT. In Section 3, the simulation results. The interpretation is described in Section 4.

2. WATERMARK IMPLANTING AND EXTRACTING PROCESS

I. Watermark Inserting Process using Stationary Wavelet Transform

First, the private key and audio clip is selected for the watermarking process. The selected audio clip is filtered and separated into an exact number of sub-portions with the fixed-length M, Where M is the even number and real. Let $R(n)$ be the 30s duration audio clip. Let $R(n)^{'}$ be the sub-portion of the audio clip. Each sub-portion of the audio clip is further separated into sub-sections of equal length R, where R is even number and real. Let F consist sampled data of length R in a subsection of an audio clip.

$$F = \{ f_1, f_2, f_3, \ldots\ldots\ldots\ldots, f_R \} \tag{1}$$

The following equation (2) is then used to determine the SWT coefficients of each subsection with m+1 level coefficient from the approximate sequence coefficient of $S_{m,n}$ [18].

$$\begin{aligned} &\textit{Approximate coefficient} \qquad S_{m+1,n} = \frac{1}{\sqrt{2}} \sum_k \bar{A}_k^m S_{m,n+k} \\ &\textit{Detailed coefficient} \qquad T_{m+1,n} = \frac{1}{\sqrt{2}} \sum_k \bar{B}_k^m T_{m,n+k} \end{aligned} \tag{2}$$

Where A_k^m *and* B_k^m are defined by

$$A_k^m = \begin{cases} a_{k/2^m} & \text{if } k/2^m \in z \\ 0 & \text{otherwise} \end{cases} \quad \text{and} \quad B_k^m = \begin{cases} b_{k/2^m} & \text{if } k/2^m \in z \\ 0 & \text{otherwise} \end{cases}$$

Where m indicates the level of coefficient/ constants with equal length. $\bar{A}_k^m$ *and* $\bar{B}_k^m$ are the complex conjugate of A_k^m and B_k^m. Similarly, the inverse formula for SWT is

$$S_{m,n} = \frac{1}{\sqrt{2}} \sum_k A_{n-k}^{m+1} S_{m+1,k} + \frac{1}{\sqrt{2}} \sum_k B_{n-k}^{m+1} T_{m+1,k} \tag{3}$$

Let $R(\zeta)$ be the approximate coefficient calculated at the k^th^ decomposition level of SWT is

$$R(\zeta) = \{ S_{1,n}, S_{2,n}, S_{3,n}, \ldots\ldots\ldots, S_{k,n}; T_{k,n} \} \tag{4}$$

We found that the high-frequency constants are vulnerable to attacks, as well as the human being, would not perceive it and hence are not included during the watermark implantation phase. Only selected frequency (i.e. low and mid-frequency) constants of each sub-section are regarded for patch formation and for implanting of watermarks from approximate coefficients.

Let $Z_s(\xi)$ be the selected frequency coefficient of the from $R(\zeta)$.

$$Z_s(\xi) = \{ Z_1, Z_2, Z_3, Z_4, \ldots\ldots\ldots, Z_m \} \tag{5}$$

Upon removal, each sub-section of the low and mid-frequency coefficients is considered to create a patch consisting of an equal number of coefficients of the same length.

Let $R_{s,k}(\varsigma)$ be the number of patches is created.

$$R_{s,k}(\varsigma) = [R_{s,1}(\varsigma), R_{s,2}(\varsigma), R_{s,3}(\varsigma), \ldots\ldots, R_{s,l}(\varsigma)] \tag{6}$$

Where $k = 1, 2, \ldots\ldots, l$

However, the individual patch is split into sub patches of the same length $R_{s,k}(\varsigma)$ as follows:

$$R_{s,k}(\zeta) = [R_{s,k,1}(0), R_{s,k,2}(1)] \qquad \text{where } k = 1 \tag{7}$$

Therefore, each patch consists of a coefficient

$$\begin{aligned} R_{s,k,1}(\zeta) &= \left[R_{s,k,1}(0), R_{s,k,1}(1), \ldots\ldots, R_{s,k,1}\left(\frac{l}{2}-1\right)\right] \\ R_{s,k,1}(\zeta) &= \left[R_{s,k,1}\left(\frac{l}{2}\right), R_{s,k,1}\left(\frac{l}{2}+1\right), \ldots\ldots, R_{s,k,1}(l-1)\right] \end{aligned} \tag{8}$$

When creating a set of patches, for security purposes, a PN sequence $\kappa(n) = \{\kappa(1), \kappa(2), \ldots\ldots, \kappa(l)\}$ of the patch size length is generated. This generated sequence scrambled with patch coefficients and formed a scrambled coded patch. Let $R_{z,k}(\varsigma)$ be the scrambled coefficient of the patch.

$$R_{z,k}(\varsigma) = \left[R_{s,k}(\varsigma) \oplus \kappa(n) \right] \tag{9}$$

Then, for embedding purposes, selected biometric traits iris is used as a watermark from the database. The embedding of this watermark is achieved after obtaining a binary sequence of bit 1 and 0 by sharpening, resizing, and converting watermark. This watermark data ω(n) is ready for incorporation into the scrambled patch. Multiple numbers of patch pairs in the patchwork pairs cannot be used to insert watermarks.

Using equation (10), we define and calculate the mean value of each patch (using a statistical parameter equation of mean) to embed watermark bit in selected patches sub patch $R_{z,k,1}(\zeta)$ and $R_{z,k,1}(\zeta)$.

$$\begin{aligned} m_{k,1} &= \left| \frac{1}{n} \sum_{i=1}^{n} R_{z,k,1}(\zeta) \right| = E\left(\left| R_{z,k,1}(\zeta) \right| \right) \\ m_{k,2} &= \left| \frac{1}{p-n} \sum_{i=n+1}^{p} R_{z,k,2}(\zeta) \right| = E\left(\left| R_{z,k,2}(\zeta) \right| \right) \\ m_{k} &= \left| \frac{1}{p} \sum_{i=1}^{p} R_{z,k}(\zeta) \right| = E\left(\left| R_{z,k}(\zeta) \right| \right) \\ \tilde{m}_i &= \left| m_{k,1} - m_{k,2} \right| - m_k \end{aligned} \tag{10}$$

Where p is the total number of coefficients are present in patch and n, p-n is the total number coefficients present in sub patch.

If it satisfies the following condition, then the watermark bit 1 and 0 is embedded in a sub patch of a patch

$$\tilde{m}_i \le 0 \quad \& \quad \min\{m_k\} \ge 0.4 \tag{11}$$

For bit 0, $if\left(m_{k,1}-\mu_{k,2}\right)>\alpha_2\mu_k$ is satisfied [20] then the coefficient of the sub patch is kept same otherwise it changes by using additive multiplicative equation [19]

$$\bar{m}_{k,1} \ \& \ \bar{m}_{k,2} = m_k \pm \kappa \times m_k \beta \tag{12}$$

Else, for bit 1, $if\left(m_{k,2}-\mu_{k,1}\right)>\alpha_2\mu_k$ is satisfied then the coefficient of the sub patch is kept same otherwise it changes by using

$$\bar{m}_{k,1} \ \& \ \bar{m}_{k,2} = m_k \mp \kappa \times m_k \beta \tag{13}$$

Where β the strength of the watermark, $\bar{m}_{k,1}$ & $\bar{m}_{k,2}$ is the modified SWT coefficient after watermark embedding.

As soon as the above condition is mention in equation (11) is satisfied, the scrambled watermark ω(n) bits will only be inserted into the scrambled code patch using the above rules. The patch coefficients are altered in terms of mean value then all modified patch & non-altered patch are collected and then applied inverse SWT to get watermark signal.

II. Watermark Extraction Process

After receiving the audio watermarked clip, the private key is provided. If this key match with the transmitted key, then the decoding process starts; otherwise, it ends the process. Once the key match, then the watermarked signal is filtered, sampled, and separated into an exact number of sub-portions with the constant length. Let $R(n)$ be watermarked audio clip. Let $R(n)^{'}$ be the sub-portion of the audio clip. Each sub-portion of the audio clip is further separated into sub-sections of equal length as per mention in the encoding process. Apply SWT to each subsegment to find out its coefficients. Similarly, as per the methodology used in the encoding side only selected frequency coefficients (i.e. low and medium frequency) of each sub-section are considered for the formulation of patches and the extraction of watermarks from estimated coefficients. Upon removal, each sub-section of the low and mid-frequency coefficients is considered to create a patch consisting of an equal number of coefficients of the same length.

However, the individual patch is split into sub patch of the same length as follow:

$$R^{\wedge}_{s,k}\left(\zeta\right)=[R^{\wedge}_{s,k,1}\left(0\right),R^{\wedge}_{s,k,2}\left(1\right)] \tag{14}$$

Before extracting watermark, users first need to find out, is patch & sub patch contain the watermark or not. To find this, we use equation(10) to calculate the mean value of the patch & sub patch. Using this equation, we define and compute the mean value of such patches to remove watermark bit from the selected patch and sub patch $R^{\wedge}_{s,k,1}\left(\zeta\right)$ and $R^{\wedge}_{s,k,1}\left(\zeta\right)$.

If the criteria mention in equation (11) are fulfilled, then the respective patch and sub patch consist of a watermark bit otherwise patch and sub patch will be without watermark bit. Once the criteria satisfied, then the watermark extraction process started by using the following equation

For bit 0, $if\left(m_{k,1}-\mu_{k,2}\right)>\kappa\mu_k$ is satisfied then the coefficient of the sub patch is not change otherwise it changes by using

$$\bar{m}_{k,1}\ \&\ \bar{m}_{k,2}=m_k\mp\kappa\times m_k\beta \tag{15}$$

Else For bit 1, $if\left(m_{k,2}-\mu_{k,1}\right)>\kappa\mu_k$ is satisfied then the coefficient of the sub patch is not change otherwise it changes by using

$$\bar{m}_{k,1}\ \&\ \bar{m}_{k,2}=m_k\pm\kappa\times m_k\beta \tag{16}$$

After extracting watermark bit from patch and sub patch, all extracted bit is collected and then its preprocessing and resizing process will be performed and converted into an image. When the image is restored, the evidence of authentication is compared to the database. The authentication process is completed by calculating the original image coefficients using a Gabor filter. The comparison is provided based on the distance between pixels of Euclidian's. All watermark extracted patch & non extracted patch are collected & unrandomized by using the same PN sequences and then ISWT is applied to get back the original audio signal.

3. PERFORMANCE AND EVALUATION EVIDENCE

This section includes descriptions of the simulation that validate the performance of the proposed scheme. We have 15 audio clips randomly picked for simulation from various classes of songs such as Bollywood (B), Classical (C), Folk (F), Jazz (J), and Instrumental (I). The audio clip has 30 seconds duration. Samples are sectioned into 16 bits, quantified, and obtained at 44.1 kHz. Each sub-portion and sub section of audio clip consists of 4096 and 2048 samples. Similarly, from 5th level SWT coefficients, there are 52 patches and 104 sub patches of the length of 40 and 20 samples are formed, respectively. A suggested watermarking technique should be enough for traditional and advanced attacks while keeping high efficiency of the sensual process. The physical property of the suggested watermark is dependent on the watermarking parameters. Based on the parametric quantity carefully selected, the implant potential of the proposed scheme can be approximated up to 8-9 bps. Imperceptibility confirmed using signal to noise ratio parameters, which is required to a greater extent than 20 dB. Similarly, validated using PEAQ algorithm to grade(ODG) it [6]. Our proposed method provides the average SNR for the selected audio clips is more than 24 dB and showing imperceptibility grading using PEAQ Algorithm. This test is used to evaluate the watermark design's robustness concerning traditional and advanced attacks. This measures the imperceptibility, robustness, payload, and computational complexity with the following description:

A. **Signal to Noise ratio (SNR):** It is calculated between the original audio signal and watermark audio signal.

$$SNR=10\log_{10}\frac{\sum_{i=1}^{N}A_i^2}{\sum_{i=1}^{N}\left(A_i-A_o\right)^2} \tag{17}$$

Where A_i^2 is original audio and A_o^2 is the watermarked audio

B. **Bit error rate (BER):** it is calculated between the amount of watermark bit implanted and watermark bit extracted.

$$BER = \frac{w_o}{w_i} \tag{18}$$

Where w_i is the watermark bit implanted and w_o is the watermark bit extracted

C. **Payload:** This can also be specified and measured rendering to the number of watermark bit implanted and the length of the audio clip.

$$Payload(PC) = \frac{F_S}{N_L} = \frac{Sampling\ rate}{Number\ of\ samples\ for\ one\ bit\ information} \tag{19}$$

D. **Computational Complexity:** It can be added or measured in terms of speed under a different type of watermark. It is estimated in bps[15].

$$Computational\ Complexity(CC) = \frac{Total\ watermark\ bit}{T_{implanting\ time}} \tag{20}$$

For the robustness analysis on the watermarked signal, the subsequent formal and advance attacks are used:

1. **No attack/loop closed:** without any attack, the watermarks are withdrawn.
2. **Resampling attack:** Introduce down-sampling with frequency 44.1 kHz to 16 kHz and then introduced the up-sampling.
3. **Low-pass filtering (LPF):** This method incorporates filtering with a frequency between 8 and 12 kHz.
4. **High-pass filtering (HPF):** This method involves filtering with a possible frequency of 50-100 Hz.
5. **Amplitude attack:** The magnitudes were 1.2 times higher.
6. **Jitter attack:** Many of the samples are randomly removed from 5000 samples of watermarked signals.
7. **Noise attack:** In the watermark signal, signal to noise (SNR) ratios are of 20 dB added.
8. **Cropping attack:** 100 samples are taken from the audio watermarked signals.
9. **Re-quantization attack:** It executed from 16 to 8 bits and vice versa.
10. **MP3 Attack:** MP3 operation executed using 128 kbps.
11. **AAC Attack:** AAC operation executed using 96 kbps.
12. **Pitch scaling:** Pitches are scaled using a 10% scaling factor.
13. **Time scaling:** Times are scaled using a10% scaling factor.
14. **Echo Addition:** Echo of the watermarked signal is added with the watermarked signal by creating a delay of 1s.

Table 1. Average performance BER of the proposed scheme for different signal under attacks

Original Signal	Types of Attacks	BER	Types of Attacks	BER	Types of Attacks	BER
B1 - B3	No attack	0.060	Resampling	0.099	LPF 8 kHz	0.102
C1 – C3		0.060		0.108		0.105
F1 – F3		0.060		0.102		0.097
I1 - I3		0.061		0.110		0.107
J1 – J3		0.059		0.100		0.107
B1 - B3	HPF 100Hz	0.094	Amplitude	0.101	Jitter	0.099
C1 – C3		0.105		0.105		0.096
F1 – F3		0.104		0.100		0.102
I1 - I3		0.105		0.103		0.096
J1 – J3		0.104		0.102		0.104
B1 - B3	Noise	0.104	Cropping	0.104	Re-quantization	0.096
C1 – C3		0.103		0.099		0.097
F1 – F3		0.097		0.100		0.102
I1 - I3		0.105		0.098		0.100
J1 – J3		0.103		0.104		0.100
B1 - B3	MP3 128 kbps	0.108	AAC 128 kbps	0.102	Pitch scaling	0.108
C1 – C3		0.088		0.098		0.103
F1 – F3		0.100		0.100		0.102
I1 - I3		0.097		0.095		0.102
J1 – J3		0.095		0.099		0.103
B1 - B3	Time scaling	0.068	Echo	0.100		
C1 – C3		0.061		0.100		
F1 – F3		0.062		0.101		
I1 - I3		0.062		0.101		
J1 – J3		0.062		0.104		

Table 2. Average performance parameter for the proposed scheme for different signals

Original Signal	SNR dB	PEAQ / ODG Grade	NCC	Payload(bps)	Computational complexity (bps)
B1 - B3	24.03	- 0.4	≈1	8-9	44
C1 – C3					
F1 – F3					
I1 - I3					
J1 – J3					

Results of the investigation shown in Table-1 suggest that the watermark is considerably invented under traditional as well as advanced signal processing attack. With the increase in embedding the imperceptibility of all the methods decreases but robustness increases. The watermark for a high-energy audio signal remains imperceptible still if the low-frequency constants are altered. Due to the perceptual value of relatively low-frequency elements, there is no substantial information loss in such regions, so watermarked constancy can be enhanced. Thus to attain an optimal value between payload, robustness, and imperceptibility for the correct value of $\kappa = \beta = 0.5$ are selected randomly from the range 0.1 to 1, as shown in table 2. If we exceed this value, then all parameters are influenced slightly.

4. CONCLUSION

This paper proposes the use of patchwork technique, SWT, and biometric watermark for audio watermarking, which can be used to identify, authenticate and to prove ownership. A proposed scheme using the patchwork approach that incorporates watermark data based on the alteration in the SWT Coefficient, and it is beneficial and reliable to make them extremely imperceptible which proved by observing the value of PEAQ is less than -1. The mathematical model additive multiplicative condition is used for the implantation process for some selected SWT patch pairs. In contrast, the identical insertion is used for scanning the watermarked blocks in the decryption stage. Plan a suggested strategy with chosen frequency bands and different watermark encryptions to ensure a high degree of robustness. The SNR is above 20 dB between the watermarked and the original audio, which indicates that perceptual clarity is preserved above the stated levels. The BER and NCC values against all the attacks are gaining momentum, thus suggesting respectable robustness against attacks. The extracted biometric watermark is matching with the database, and hence authentication is proving under different attacks. Implementation with additional biometric functionality under masking, rotation and replacement attack could be the priority in the future. We presented audio watermarking by integrating biometrics to identify, authenticate and watermark copyrights and copy proof of ownership.

REFERENCES

[1] G. Hua, and et. al., "Twenty Years of digital Audio Watermarking -A Comprehensive Review" *Signal Processing*,128: **(2016),** pp. 222–242.

[2] W. Bender, and et. al., "Techniques for data hiding", *IBM Syst. Journal*, Vol. 35, Nos. 3/4, **(1996)**, pp.131–336.

[3] N. Nikolaidis, and et. al., "Digital Image Watermarking: An Overview" *In Proceedings of IEEE International Conference on Multimedia Computing and Systems*, **(1988)**, pp. 1–6.

[4] M. K. Dutta, and et. al., "Audio watermarking using pseudorandom sequences based on biometric templates", *Journal of Computers*, Vol. 5, No. 3, **(2010)**, pp.372–379.

[5] W. N. Lie, and et. al., "Robust and high quality time domain audio watermarking based on low frequency amplitude modification", *IEEE Transactions on Multimedia*, Vol. 8, No. 1, **(2006)**, pp.46–59.

[6] T. Thiede, and et. al., "PEAQ – the ITU standard for objective measurement of perceived audio quality", *J. AES*, Vol. 48, Nos. 1/2, **(2000)**, pp.3–29.

[7] A. Kaur, and et. al., "Hiding biometric features in audio signals using Gram-Schmidt orthogonalisation", *Int. J. Electronic Security and Digital Forensics*, Vol. 8, No. 1, **(2016)**, pp. 63-81.

[8] C. Yang and et. al., "An audio watermarking based on discrete cosine transform and complex cepstrum transform", *Int. Conf. on Computer Application and System Modeling*, **(2010)**, pp.456–458.

[9] J. Daugman, "How iris recognition works", *Proceedings of 2002 International Conference on Image Processing, IEEE*, **(2002)**, pp.1–33.

[10] M. K. Dutta, and et. al., "Biometric based unique key generation for audio watermarking", *International Conference on Pattern Recognition and Machine Intelligence, LNCS*, Vol. 5909, **(2009)**, pp.458–463.

[11] M. K. Dutta, and et. al., "Blind watermarking in audio signals using biometric features in wavelet domain", *International Conference of IEEE Region 10, TENCON 2009*, **(2009)**, pp.1–5.

[12] M. K. Dutta, and et. al., "Generation of biometric based unique digital watermark from iris image", *International Conference on Telecommunications and Signal Processing, IEEE*, **(2013)**, pp.685–689.

[13] A. Kaur, and et. al., "A high payload audio watermarking algorithm robust against Mp3 compression", *IC3*, **(2014),** pp.531–535.

[14] L. Masek, Thesis on "Biometric identification system based on iris patterns", *The School of Computer Science and Software Engineering, The University of Western Australia*. **(2003)**.

[15] Y. Lin and et. al., "Audio Watermark-A Comprehensive Foundation Using MATLAB", *Springer International Publishing, Switzerland,* **(2015)**, pp.1-213**.**

[16] M. S. Al-Yaman, and et. al., "Biometric-based audio ownership verification using discrete wavelet transform and SVD techniques", *Eighth International Multi-Conference on Systems, Signals & Devices*, Sousse, **(2011)**, pp. 1-5.

[17] A. Kaur, and et. al., "A secure and high payload digital audio watermarking using features from iris image", *2014 International Conference on Contemporary Computing and Informatics (IC3I), Mysore*, 2014, **(2014)**, pp. 509-512.

[18] Yoshito Ishida, and et. al., "Digital Audio Watermarking Method Based on Wavelet Transform", *Published in proceeding of the 2015 International Conference on Wavelet Analysis and pattern recognition, Guangzhou*,12-15 July 2015, **(2015)**, pp.87-92.

[19] V. S. Inamdar, Priti P Rege, "Dual watermarking technique with multiple biometric watermarks", *Sadhana*, Vol. 39, Part 1, February 2014, **(2014)**, pp. 3–26.

[20] I. Natgunanathan, and et. al., "Robust Patchwork -Based Embedding and Decoding Scheme for Digital Audio Watermarking," *IEEE Trans. Audio, Speech Lang.Process*.,20(8): **(2012)**, pp.2232–2239.