

Robust Watermarking Using FFT and Cordic QR Techniques

Sunil Kumar Vishwakarma¹, Birendra Kumar Sharma², Syed Qamar Abbas³

¹Research Scholar, Department of Computer Science and Engineering

Dr. A.P.J. AKTU

Lucknow, India

sunilvishwakarma83@gmail.com

²Professor and Head, Department of MCA

Ajay Kumar Garg Engineering College

Ghaziabad, India

bksharma888@yahoo.com

³Professor, Department of Computer Science & Engineering

Ambalika Institute of Engineering and Technology

Lucknow

grat_abbas@yahoo.com

Abstract— Digital media sharing and access in today's world of the internet is very frequent for every user. The management of digital rights may come into threat easily as the accessibility of data through the internet become wide. Sharing digital information under security procedures can be easily compromised due to the various vulnerabilities floating over the internet. Existing research has been tied to protecting internet channels to ensure the safety of digital data. Researchers have investigated various encryption techniques to prevent digital rights management but certain challenges including external potential attacks cannot be avoided that may give unauthorized access to digital media. The proposed model endorsed the concept of watermarking in digital data to uplift media security and ensure digital rights management. The system provides an efficient procedure to conduct over-watermarking in digital audio signals and confirm the avoidance of ownership of the host data. The proposed technique uses a watermark picture as a signature that has been initially encrypted with Arnold's cat map and cyclic encoding before being embedded. The upper triangular R-matrix component of the energy band was then created by using the Fast Fourier transform and Cordic QR procedures to the host audio stream. Using PN random sequences, the encrypted watermarking image has been embedded in the host audio component of the R-matrix. The same procedure has been applied to extract the watermark image from the watermarked audio. The proposed model evaluates the quality of the watermarked audio and extracted watermark image. The average PSNR of the watermarked audio is found to be 37.01 dB. It has also been seen that the average PSNR, Normal cross-correlation, BER, SSMI (structure similarity index matrix) value for the extracted watermark image is found to be 96.30 dB, 0.9042 units, 0.1033 units, and 0.9836 units respectively. Further, the model has been tested using various attacks to check its robustness. After applying attacks such as noising, filtering, cropping, and resampling on the watermarked audio, the watermark image has been extricated and its quality has been checked under the standard parameters. It has been found that the quality of the recovered watermark image satisfying enough to justify the digital ownership of the host audio. Hence, the proposed watermarking model attains a perfect balance between imperceptibility, payload, and robustness.

Keywords- FFT decomposition; Watermarking; Cordic QR method; Cyclic encoding; Arnold's cat map.

I. INTRODUCTION

Multimedia data such as text, images, audio, video, and graphics may be easily accessed, saved, and transferred across a communication channel because of the Internet's openness. [1]. As a result, it causes a variety of issues, including patent, illegal access, and security concerns [2]. Now the question is: Why should we get a watermark? To better understand this, imagine that you completed a task and that someone then claims that he, rather than you, completed it. How would you determine who the true owner is in this situation? The answer involves the use of watermarking. The term "Digital Watermark" was coined by Andrew Tirkel and Charles Osborne

in December 1992 [3]. The primary winning embedding and release of the steganographic unfold spectrum watermark were unquestionable in 1993 by Andrew Tirkel, Charles Osborne, and Gerand Rankin [4]. Digital watermarking defines methods as well as technologies that hide information, for example, a number or text, in digital media, such as video, and images. A digital watermark is a type of hidden tag inside a signal that accepts sound, such as audio, video, or picture data. It is widely used to determine who owns signal rights. Non-blind watermarking is a method of watermarking [5] that involves a host image, using a watermark verification process. The performance of a watermarking system is primarily determined by the watermark structure and embedding of the method used.

[6] Two methods can be used to test the effectiveness of digital watermarking: invisibility and durability. Watermarking is a way to hide digital information within a network signal; Encrypted data should, but not necessarily, be related to the network signal. Digital watermarks can be used to verify the authenticity or authenticity of a network signal or to show ownership of its owners. It is commonly used to track copyright infringement and verify banknotes [7].

A digital watermark is a message that can be retrieved or further detected from digital content.

TYPES OF WATERMARKS

VISIBLE – The reader can clearly see the watermark with this style of watermarking.

INVISIBLE – Although there is a watermark in this type of watermarking, the user cannot see it.

APPLICATIONS OF WATERMARKING

There are several applications of digital watermarking.:

- Copy interference or management
- In the sphere of knowledge security
- Copyright protection
- Source pursuit – totally different recipient gets otherwise watermarked content
- Broadcast watching – newscast generally encompasses watermarked video from numerous international agencies.
- Video authentication
- Screen casting software system is being halted to provoke shoppers to shop for the whole version to disable it.

[8]. Copyright watermarking is a promising way to protect copyright in digital media. However, it is important to carefully assess the watermarking scheme's effectiveness. In the context of change, Zheng also introduced a robust method of creating watermarks of copyright protection [9]. threats, patent leaks, and various other statistical and varied threats can also be security concerns [10]. A complete watermarking system can meet the two basic requirements for copyright protection and firmness and invisibility. Here, stiffness means that the watermark on an image with a watermark can be removed altogether even though the image with a watermark is damaged by the attack. For the copyright protection of digital media, image watermarking offers a promising approach. [11] Jing and Zhang proposed a blind watermarking algorithm based on Shurhur decay and a non-sampled contourlet, which was intended to obtain patents or criminality. Sunesh & Rama Kishore [12] has proposed a system of blurred vision with blurred images, in the absence of blurry images there is no need to photograph with a watermark, and provides high durability and a good process that works at a very low cost. Fahd and Khalid [13] and F. N. Al-Wasabi et al. [14] also proposed ZWAFWMMM, a smart watermarking solution. This method of watermarking correctly and unintentionally prevents the prohibition of goods and any kind of heat in the texts of Arabic text.

Punit Pandey et al. [15] proposed a photo editing program based on the divisive version of the Divide. With his paper, he wants to solve the problem of the coefficients of wavelet coefficients mathematically and visually used during watermarking and the proposed algorithm is much better. In 2019 [16] it is proposed to use the aid vector machine in conjunction with the genetic algorithm. Image authentication has become a major problem in the use of E-health. Digital photography and medical communication (DICOM) are used to transmit medical records over an open network [17]. Encryption methods include important data for medical safety monitoring. It is based on confidential communication between two parties with the intention that no one other than the authorized group may secretly extract or enter the code (embedded), encryption strategies incorporate important information relating to medical safety. It is obtained by confidential communication between the two parties with the intention that no one other than the authorized group may secretly extract or enter the code details. To increase visibility and pay-per-upload volume, watermarks are chosen to be included in the sub-subbands of the Non-Subsampled Contourlet Transform domain. The NSCT computer partner operates, offering anisotropy and variable sub-direct band selection. The proposed process's watermark pictures are further secured by watermark-based encryption of the watermark. The suggested approach has a maximum PSNR level of 92.22 dB, which varies depending on the cover photo,

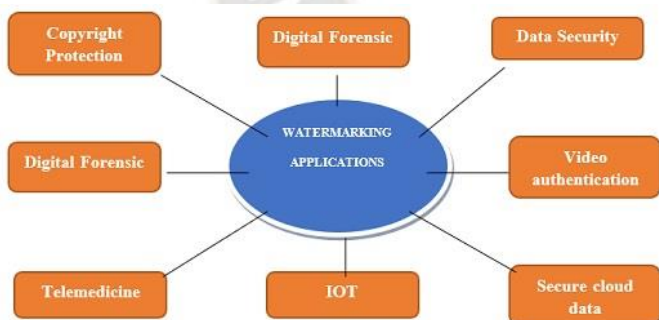


Figure 1. Some applications of Watermarking

Figure 1 depicts the applications of watermarking in today's era. Watermarking technology has been used in various fields including digital forensics, data security, video authentication, etc. The main aim of such applications is to preserve the owner's digital rights or to ensure digital rights management.

II. LITERATURE SURVEY

Digital watermarking uses a distinctive watermark to authenticate ownership of digital media. (e.g., video, audio etc.

watermark image, and gain features. The proposed method is less obvious than comparable methods and is achieved with the accuracy of numerous attacks on color images. The proposed procedure can be used to verify and obtain color-sensitive images for any malicious attack and allows the embedding of gray and watermarks. Disruptive localization and recovery of lost data may focus on future work [18]. The exchange of patient records requires a process to ensure the security and privacy of telehealth services. [19] These services are simple and helpful in the medical field but also bring with them leaks of privacy, identity theft, and the risk of data distortion and authenticity. In addition, digital imaging, and medical communication (DICOM) is commonly used to exchange electronic patient reports with open network encryption methods and demonstrations to provide authenticity and confidentiality of medical records.

III. PROPOSED MODEL

A general watermarking procedure is shown in the below figure. It has four stages:

1. Generation
2. Embedding
3. Distribution and Attacks
4. Detection and Recovery

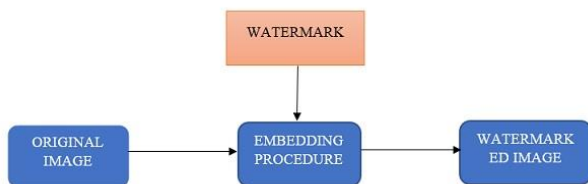


Figure 2. Process of Watermarking

Figure 2 shows the general process of watermarking in which it has been seen that watermark data has been inculcated in the original image results watermarked image which is secure. Here in the normal process of first scanning the first image is taken and the watermark is inserted into the image, to make embedding we can use MS OFFICE provided by Microsoft which adds a watermark to write a feature built into the Design Tab. Each grayscale image has a pixel size of 256 by 256 and an 8-bit depth. Choose the CI image that will serve as a base picture or cover image for the watermark. To use it as a watermark, choose an image file. Read the watermarked WI pictures that will be added to the picture.

n = no. important pieces that can be used to hide the most important pieces of watermark under the base image

A. WATERMARK EMBEDDING MODEL

- With a pixel per base, watermark, watermark image Is Base image: set the most important pieces to zero

- Watermark: go right by 8-n bits
- Watermarked image: add values from the base and watermark

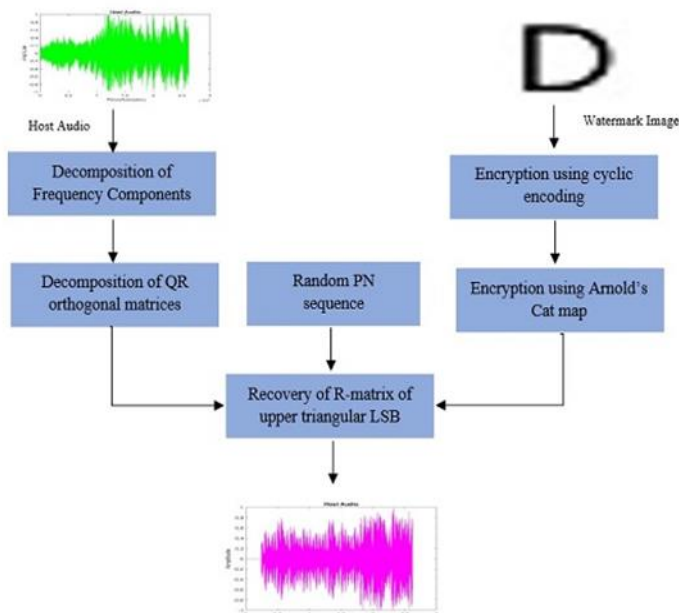


Figure 3. Working on the Watermark Embedding model

Figure 3 shows a watermark embedding model in which host data as the audio signal has been taken from a standard dataset [4]. This audio signal contains music data in which a watermark image containing the logo 'D' is inculcated. The proposed model first applies Fast Fourier Transform (FFT) to resolve frequency components. Then, the crucial FFT coefficients have been used to undergo Cordic Q-R decomposition which results in Q and R orthogonal matrices. The Watermark embedding process has been held in the LSB (least significant bit) of upper triangular data of R-matrix. Before the embedding process, the watermark image of size 16×16 has been encrypted with 2 layers encryption algorithm. The first layer involves cyclic encoding in which the generation polynomial has been integrated with true data bits (watermark bits) to generate code bits. The other layer of encryption involves Arnold's cat map which puzzled the code bits for 7 times as the key in this algorithm is taken as 7. Then, the final encrypted watermark data has been inculcated into the LSB of the upper triangular of the R-matrix using uncorrelated pseudo-random sequences (PN sequence). PN sequence algorithm [20] is a non-deterministic mathematical approach to finding the location in host data for the embedding process. Every step of the PN sequence method is uncorrelated with each other so that randomness can be preserved. This algorithm is used to avoid any kind of systematic tempering with watermarked data.

ALGORITHM OF WATERMARKING

Step 1. Input Host audio

Step 2. Apply reshape process to convert in 2-dimensional data

Step 3. Apply FFT transformation

$$\text{FFT}[A] = \sum_{p=0}^{N-1} \text{FFT}[p] E^{-j2\pi AP/N} \quad (1)$$

$$E^{-j2\pi AP/N} = -j \sin\left(\frac{2\pi AP}{N}\right) + \cos\left(\frac{2\pi AP}{N}\right) \quad (2)$$

In equation 1, FFT[A] is the frequency component of host audio data which is generated after applying FFT transformation. These frequency components contain energy bands of information.

Step 4. Apply Cordic Q-R decomposition on the extracted frequency components to generate Q and R orthogonal components of matrices.

$$\text{CORDIC}(\text{FFT}[A]) = [Q] [R] \quad (3)$$

$$\begin{bmatrix} \cos\phi & \sin\phi \\ -\sin\phi & \cos\phi \end{bmatrix} \times \begin{bmatrix} A_{m-1,k} \\ A_{m,k} \end{bmatrix} = \begin{bmatrix} R_{11} & R_{12} & \dots & R_{1k} \\ 0 & R_{21} & \dots & R_{2k} \end{bmatrix} \quad (4)$$

Equation 3 shows that the CORDIC QR decomposition has been applied to frequency components of host data to generate Q and R matrices. Then, in equation 3, it is shown that the rotation matrix is integrated with the input host matrix (generated after applying FFT transformation) to obtain the upper triangular R matrix.

Step 5. Apply cyclic encoding in the watermark image. In this algorithm, a segment of 4 bits of watermark data has been added with 3 bits of redundant data to generate 7 bits of an encrypted codeword.

$$\text{Code_word}(x) = \text{Watermark_bits}(x) \cdot \text{Generation_polynomial}(x) \quad (5)$$

$$\text{Generation_polynomial}(x) = x^3 + x + 1 \quad (6)$$

Step 6. Apply Arnold's cat map algorithm of the encoded watermark image. The general equation of Arnold's cat map is given below

$$T(a, b) = (2a + b, a + b) \text{ mod } N \quad (7)$$

In equation 7, T is Torus which is a coefficient of Arnold's cat map using a key value of 7 which shows the number of times the data will be puzzled.

Step 7. Perform an Embedding process using an uncorrelated PN sequence algorithm to inculcate encrypted watermark bits into the R-matrix of Host audio data.

$$\begin{aligned} &\text{If } C(K) = 0 \\ &r_n = r_n + K1 \\ &\text{If } C(K) = 1 \\ &r_n = r_n + K2 \\ &\text{end} \end{aligned} \quad (8)$$

In equation 8, C(K) is the puzzled code word generated after applying Arnold's cat map, r_n is the nth bit of LSB of the R matrix, and K1 and K2 are the two PN sequence keys.

Step 8. After the embedding process, the watermarked audio is reconstructed by applying the inverse route of the same transformation. Again, perform the inverse of Reshape with watermarked data to generate the final watermarked audio.

Step 9. Evaluate the watermarked audio in terms of PSNR (peak signal-to-noise ratio).

WATERMARK EXTRACTION MODEL

In an image with a pixel watermark for each pixel in the image and the image removed Watermarked image: Shift left by 8-n bits

Image output: Set to the output value of the image with the watermark

The process used will be the LSB process which is local domain technology.

This method is used to add an invisible and visible watermark to an image by changing the bit exchange rate and the basic image.

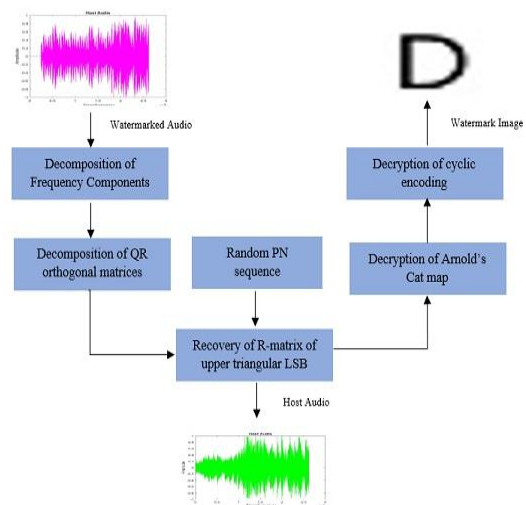


Figure 4. Working of Watermark Extraction Model

Figure 4 is showing watermark extraction process in which the watermarked audio is taken in which the watermark image is installed. The audio is undergone decomposition with FFT transformation and cordic QR transformation techniques. Then, the upper triangular R matrix is evolved from which the hidden watermark bits are extricated using the same PN sequences. Then the decryption and reconstruction of extracted watermark bits are applied to finally generate the watermark image. This extracted watermark image is evaluated further to test the robustness of the algorithm.

ALGORITHM OF WATERMARK EXTRACTION

Step 1. Watermarked audio is first taken to reshape in 2-dimensional data and the FFT transformation is applied to get frequency components in which watermark encrypted image data is hidden.

Step 2. FFT energy bands are decomposed into QR matrices using CORDIC OR decomposition in order to extract the R matrix. In the cordic QR algorithm, the same approach is applied to obtain upper triangular data of R-matrix.

Step 3. Further, the watermark bits are extricated out of the LSB of the R matrix.

If correlation (r_n and K1) > correlation (r_n and K2)

Then C(k)=0

If correlation (r_n and K2) >= correlation (r_n and K2)

Then C(K)=1

Step 4. The encrypted watermark bits are then decrypted using inverse Arnold's cat map first with the key value as 7. Then, the data is further decrypted using the inverse of cyclic coding to generate original watermark bits.

Step 5. After the successful decryption of watermark data, reconstruction of watermark bits is applied to get the final watermark image.

Step 6. Evaluate the extracted watermark image in terms of PSNR (peak signal-to-noise ratio), Bit error rate, normal cross-correlation, and structure similarity index metric (SSIM).

IV. RESULT AND DISCUSSION

Three different categories of audio files—Blues, Classical, and Pop—are used in the experiment. These audio files are taken from a standard database [4]. Each audio file has a different form of information of variable frequency and amplitude components. All the audio files are of 10 sec and have a 44.1Khz sampling rate. The audio file is reshaped into 512×512 size of a 2-dimensional matrix. Further, the watermark image of size 16×16 is taken which contain a total of 256 bit of information. A sample of the host audio file and watermark image is given in Figures 5 and 6.

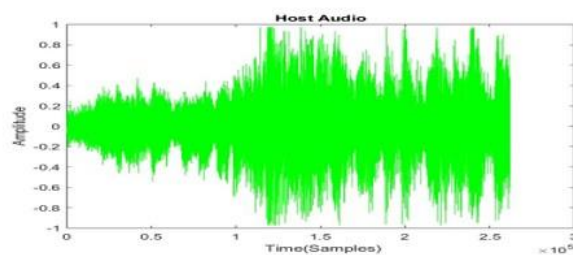


Figure 5. Sample of Audio Data



Figure 6. Sample of Watermark Image

The sample representation of the working of the model is given by GUI in Figure 7. It shows the process of embedding and extraction in the audio signal (Blues) while showing all the assessments of watermarked audio and extracted image. The average PSNR of the watermarked audio is found to be 37.01 dB which is acceptable. For extracted watermark image, the assessment is taken in terms of PSNR, BER, and NC. This assessment parameter matches the quality of the original watermark with extracted watermark. The proposed model ensures the watermark image should successfully recover from the host audio without getting much distortion.

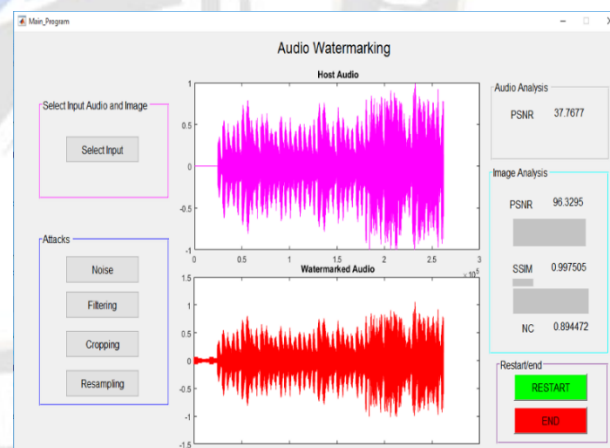


Figure 7. GUI of working of the model

The proposed experiment is conducted in MATLAB with the standard audio dataset. Figure 8 shows the original watermark image and the extracted watermark image without any attack applied. This figure depicts that the extracted watermark contains some distortion as compared to the original watermark image.

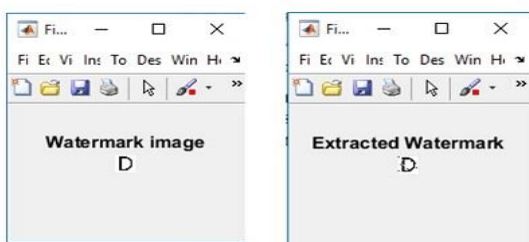


Figure 8. Watermark image and Extracted watermark image

The extracted watermark picture has been evaluated to determine how well it matches the original watermark in terms of quality. It has been seen that the average PSNR, Normal cross-correlation, BER, SSMI (structure similarity index metric) value is found to be 96.30 dB, 0.9042 units, 0.1033 units, and 0.9836 respectively. Figure 9 shows the SSIM metric for a sample of extracted watermark images.

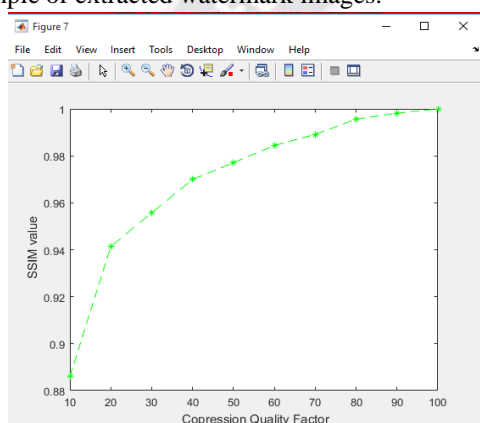


Figure 9. SSIM metric for the Extracted watermark image

Figure 9 clearly shows that the structure similarity index value for an extracted watermark image is sufficient to correlate with the original watermark image so that it satisfies the acceptable

Table I - Assessment of Watermarked audio data and extracted watermark image

Evaluation of quality for watermarked Audio		Evaluation of Extracted watermark image			
Audio files	PSNR rate	Bit Error Rate	Normalized Cross-Correlation	PSNR rate (dB)	Structure similarity index metric (SSIM)
Blues Type	35.52	0.13	0.9	95.03	0.9834
Classic Type	38.24	0.11	0.92	97.62	0.9943
Pop Type	37.27	0.07	0.88	96.3	0.9732

parameters to ensure digital ownership. Table 1 shows the assessment of watermarked audio and extracted watermark images for all types of audio files.

From Table I, it has been seen that the analysis of the watermarked audio and extracted image for all the types of audio files are found to be excellent enough to ensure digital right management. Further, to check the robustness of the model, the proposed model also tested four types of attacks on the watermarked audio and then perform an extraction process. On the watermarked audio, the attack types noise, filtering, cropping, and resampling have been tried so that the recovered extracted watermark quality can be assessed using standard parameters. Figure 10 shows the absolute difference between the host audio signal and the watermarked audio signal under the influence of noise attack.

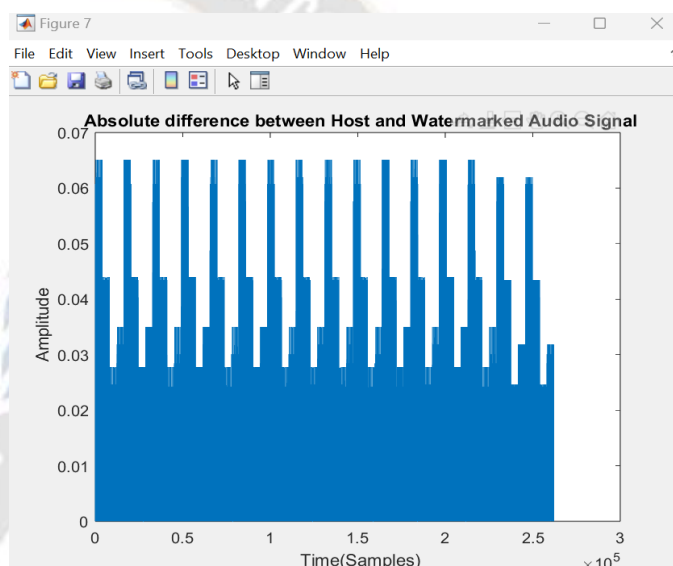


Figure 10. The absolute difference between host and watermarked audio signal

From Figure 10, it has been seen that the difference between the host audio and the watermark audio is not getting broader at the peak values. Figure 11 shows the results of extracted watermarks under the influence of attacks applied over watermarked audio containing watermark images.

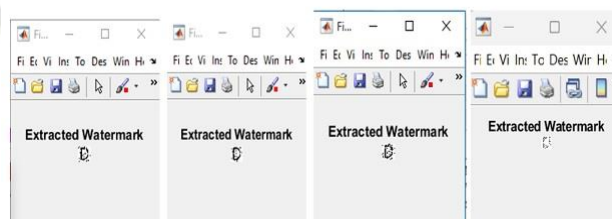


Figure 11. Extracted watermarked under the influence of various attacks

Figure 11 contains the four images of extracted watermarks under the application of attacks. The images from left to right show the results after applying noise, filtering, cropping, and

resampling attacks subsequently on the watermarked audio signal. The quality assessment of the extracted watermark after applying attacks has been checked under the standard parameters to measure the robustness of the model which is reflected in Table II.

Table II Quality evaluation of the extracted watermark image under the influence of various attacks

Audio type and the various attacks		Evaluation of Extracted watermark image			
Audio files	Attacks	Bit Error Rate	Normalized Cross Correlation	PSNR Rate (dB)	SSIM Values
Classic	Noise attack	0.25	0.821	89.342	87.441
	Filtering	0.15	0.834	86.213	91.542
	Crop	0.43	0.897	87.989	86.672
	Resampling	0.32	0.876	84.871	88.437
Blues	Noise attack	0.21	0.802	86.832	91.910
	Filtering	0.25	0.832	87.687	92.914
	Crop	0.37	0.843	84.211	85.521
	Resampling	0.33	0.811	89.991	89.652
Pop	Noise attack	0.29	0.876	89.524	91.715
	Filtering	0.15	0.896	91.876	93.519
	Crop	0.19	0.889	92.763	92.135
	Resampling	0.20	0.871	91.653	92.176

Table II contain the evaluated results for all the types of audio signal under the influence of attacks. This table contains the assessment of extracted watermark images under the four attacks. The results show that the proposed model is robust as the quality of the recovered extracted watermark satisfies the acceptable parameters to ensure digital ownership.

V. CONCLUSION

Watermarking in audio signals using images as watermarks has been utilized with several transformation techniques. Using the fast Fourier transform and Cordic QR decomposition, the audio stream was broken up into several energy components. The relevant R-matrix has been extracted out from the host audio signal in which the encrypted watermark image has been inserted. Utilizing Arnold's cat map and cyclic encoding, the watermark image has been encrypted. The payload of the watermark data is 256 bits which is embedded in the R-component energy band of the host audio with a sampling rate of 44.1 kHz. The average PSNR of the watermarked audio is found to be 37.01 dB. It has also been seen that the average PSNR, Normal cross-correlation, BER, SSMI (structure similarity index matrix) value for the extracted watermark image is found to be 96.30 dB, 0.9042 units, 0.1033 units, and 0.9836 units respectively. Further, the model has been tested using various attacks to check its robustness. The watermark image has been removed from the audio after it has been

subjected to attacks such noise reduction, filtering, cropping, and resampling, and its quality has been evaluated using the industry-standard criteria. It has been found that the importance of the recovered watermark image satisfying enough to justify the digital ownership of the host audio. Hence, the proposed watermarking model attains a perfect balance between imperceptibility, payload, and robustness. In the future, various other lightweight and effective decomposition methods can be applied over the host signal to extract relevant energy bands. Also, the amount of payload can be increased in the future while maintaining imperceptibility and robustness.

REFERENCES

- [1] Kumar, A., Rajput, S. S., & Singh, V. (2021). An Improved Approach to Secure Digital Audio Using Hybrid Decomposition Technique. In Proceedings of the International Conference on Paradigms of Computing, Communication and Data Sciences: PCCDS 2020 (pp. 361-375). Springer Singapore.
- [2] P. Zheng and Y. Zhang, "A robust image watermarking scheme in hybrid transform domains resisting to rotation attacks," *Multimedia Tools and Applications*, 2020.
- [3] O. P. Singh, G. Srivastava, N. Kumar and A. Singh, "Image watermarking using soft computing techniques: A comprehensive survey," *Multimedia Tools and Applications*, 2020.
- [4] Z. Xia, X. Wang and L. Zhang, "A Privacy-Preserving and Copy-Deterrence Content-Based Image Retrieval Scheme in Cloud Computing," *IEEE Transactions on Information Forensics and Security*, vol. XI, no. 11, pp. 2594 - 2608, 2016.
- [5] J. m. Zain and L. Chongmin, "Robust Image Watermarking Theories and Techniques: A Review," *Journal of Applied Research and Technology*, vol. XII, no. 1, pp. 122-138, 2015.
- [6] P. Pandey, S. Kumar and S. K. Singh, "A robust logo watermarking technique in divisive normalization transform domain," *Multimedia Tools and Application*, 2013.
- [7] R. Mehta, K. gupta and A. K. Yadav, "An adaptive framework to image watermarking based on the twin support vector regression and genetic algorithm in lifting wavelet transform domain," *Multimedia Tools and Application*, 2020.
- [8] R. Thanki and S. Borra, "Fragile watermarking for copyright authentication and tamper detection of medical images using compressive sensing (CS) based encryption and contourlet domain processing," *Multimedia Tools and Applications*, 2018.
- [9] A. Anand and A. K. Singh, "An improved DWT-SVD domain watermarking for medical information security," *Computer Communication*, 2020.
- [10] E. H. Rachmawanti and H. A. Santoso, "A non-blind robust and impercept watermarking using discrete cosine transform and discrete wavelet transform and discrete wavelet transform," *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control Journal homepage*, vol. 6, pp. 69-76, 2021.
- [11] D. Ariatmanto and F. Ernawan, "Adaptive scaling factors based on the impact of selected DCT coefficients for image

- watermarking," Journal of King Saud University –Computer and Information Sciences, 2020.
- [12] Suresh and R. Kishore, "A Novel and Efficient Blind Image Watermarking In Transform Domain," *Procedia Computer Science*, vol. 167, pp. 1505-1514, 2020.
- [13] J. Wang and W. Wen, "A novel attention-guided JND Model for improving robust image watermarking," *Multimedia Tools and Applications*, vol. 79, 2020.
- [14] Baser, P. ., Jatinderkumar R. Saini, & Baser, N. . (2023). Gold Commodity Price Prediction Using Tree-based Prediction Models. *International Journal of Intelligent Systems and Applications in Engineering*, 11(1s), 90–96. Retrieved from <https://ijisae.org/index.php/IJISAE/article/view/2481>
- [15] F. N. Al-Wesabi, K. Mahmood and N. NEMRI, "A zero watermarking approach for content authentication and tampering detection of Arabic text based on fourth level order and word mechanism of Markov model," *Journal of Information Security and Applications*, 2020.
- [16] J. Y. Li and C. Z. Zhang, "Blind watermarking scheme based on Schur decomposition and non-subsampled contourlet transform," *Multimedia Tools and Applications*, p. 30007–30021, 2020.
- [17] A. Dwivedi, A. Kumar, M. K. Dutta, R. Burget, and V. Myska, "An Efficient and Robust Zero-Bit Watermarking Technique for Biometric Image Protection," 2019 42nd International Conference on Telecommunications and Signal Processing (TSP), Budapest, Hungary, 2019, pp. 236-240, doi: 10.1109/TSP.2019.8768881.
- [18] A. Kumar, A. Dwivedi, and M. K. Dutta, "A Zero watermarking Approach for Biometric Image Security," 2020 International Conference on Contemporary Computing and Applications (IC3A), Lucknow, India, 2020, pp. 53-58, doi: 10.1109/IC3A48958.2020.233268.
- [19] Ólafur, J., Virtanen, M., Vries, J. de, Müller, T., & Müller, D. Data-Driven Decision Making in Engineering Management: A Machine Learning Framework. *Kuwait Journal of Machine Learning*, 1(1). Retrieved from <http://kuwaitjournals.com/index.php/kjml/article/view/108>
- [20] A. Singh, A. Kumar and M. K. Dutta, "DWT, DCT and PBFO based Approach for Biometric Image Security," 2020 International Conference on Contemporary Computing and Applications (IC3A), Lucknow, India, 2020, pp. 298-303, doi: 10.1109/IC3A48958.2020.233317.
- [21] Kumar, A., Singh, A., Prakash, S., & Singh, V. (2021). A novel approach towards audio watermarking using FFT and CORDIC-Based QR Decomposition. *AI and IoT-Based Intelligent Automation in Robotics*, 323-338.
- [22] Singh, A., Kumar, A., Dutta, M. K., Travieso-González, C., & Esteban-Hernández, L. (2020, January). Perspective Approach for Security of Biometric Image. In *Proceedings of the 3rd International Conference on Applications of Intelligent Systems* (pp. 1-7).