ADVANCED AUDIO WATERMARKING WITH MULTIPLE IMAGE EMBEDDING FOR ENHANCED SECURITY

Major Project - II report

Submitted in partial fulfillment of the requirements

For the award of the degree of

MASTER OF TECHNOLOGY

in

COMPUTER SCIENCE & ENGINEERING

by

Raghwendra Pratap Singh
(2K22/CSE/16)

Under the supervision of
PROF. MANOJ KUMAR

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi- 110042
May,2024

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

DELHI TECHNOLOGICAL UNIVERSITY

(Formerly Delhi College of Engineering)
Bawana Road, Delhi-110042

CANDIDATE'S DECLARATION

I, **Raghwendra Pratap Singh, Roll No. 2K22/CSE/16** student of M. Tech. (Computer Science and Engineering), hereby declare that the Project Dissertation titled "**Advanced Audio Watermarking With Multiple Image Embedding For Enhanced Security**" which is being submitted by me to the **Department of Computer Science & Engineering, Delhi Technological University, Delhi**, in partial fulfilment of requirements for the award of the degree of **Master of Technology** in **Computer Science and Engineering** , is original and not copied from any source without proper citation. This work has not previously formed the basis for the award of any Degree, Diploma Associateship, Fellowship or other similar title or recognition.

Place: Delhi RAGHWENDRA PRATAP SINGH
Date: (2K22/CSE/16)

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of
Engineering) Bawana Road, Delhi-
110042

CERTIFICATE

I, hereby certify that the Project titled "**Advanced Audio Watermarking With Multiple Image Embedding For Enhanced Security",** which is submitted by **Raghwendra Pratap Singh**, **Roll No. 2K22/CSE/16**, **Department of Computer Science & Engineering, Delhi Technological University**, Delhi in partial fulfilment of the requirement for the award of degree of **Master of Technology** in **Computer Science And Engineering**, is a record of the project work carried out by the student under my supervision. To the best of my knowledge this work has not been submitted in part or full for any Degree or Diploma to this University or elsewhere.

Place: Delhi **PROF. MANOJ KUMAR**
Date: **SUPERVISOR**

ABSTRACT

Digital audio watermarking has gained a lot of popularity in the research community. Watermarking is a technique that uses several approaches (such as spatial domain, transform domain, machine learning, and deep learning) to conceal information signals into digital form Through the use of an audio file known as a watermark, the owner's identity can be concealed. Thus, digital audio watermarking is the technique of adding all of the data to the audio file without affecting the audio's audibility. This study describes a novel audio steganography approach based on paying a cryptographic hashing of audio samples in order to improve perceptual invisibility and security in the embedding procedure through a secret key. The suggested method uses a secret key to hash the most significant bit (MSB) of the audio samples for picking only certain samples for modulo embedding. The selection technique applied in this scheme by hashing the samples makes the watermark imperceptible to the unauthorized and reduces the probability of statistical detection by a huge amount. The bits of the different picture’s data are placed carefully into the LSB of the selected audio samples. Because of the careful placement of the watermark in the least significant byte (LSB) of the audio samples, the extracted watermark was found intact. A noticeable improvement in the quality of audio after the extraction process was observed.

ACKNOWLEDGEMENT

I am extremely grateful to my project guide, Dr. Manoj Kumar, Professor, Department of Computer Science and Engineering, Delhi Technological University, Delhi for providing invaluable guidance and being a constant source of inspiration throughout my research. I will always be indebted to him for the extensive support and encouragement he provided. I am highly indebted to the panel faculties during all the progress evaluations for their guidance, constant supervision and for motivating me to complete my project work. They helped me throughout by giving new ideas, providing necessary information and pushing me forward to complete the project work.

Raghwendra Pratap Singh
(2K22/CSE/16)

CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

The rapid advancement of digital multimedia technology has led to the sharing of vast amounts of multimedia content online, making it easier to manipulate and clone content. This has led to a pressing global concern for copyright. Digital watermarking technologies have been used to resolve copyright issues, including author's name, serial number, company name, and important content. These technologies are used in copyright management, content authentication, tamper detection, and protection. Hackers often alter original programs or use them for profit without providing credit where credit is due. To protect risky users, protection mechanisms must be effective, reliable, and distinctive. Watermarking has various uses, including ownership protection, authentication evidence, air traffic monitoring, medicinal applications, and the music industry. Digital information, especially audio, is difficult to safeguard, making it difficult for developers to uphold copyrights. Digital watermarking encapsulates copyright information into a host signal, making it undetectable and resistant to attacks. There are certainly many advantages to digital audio materials such as: easy editing and copying, and safe storage etc. Nevertheless, there are also some problems regarding intellectual property rights. Apparently, steganography – especially audio steganography – would be a good way to solve those issues. We could conceal invisible, hidden information into an audio recording in a way to enhance data integrity and security without the quality loss of the sound which is the original audio. Anyway, since its beginning, the concept of hiding information inside digital media has gone through considerable evolutionary changes. At its early stage, indeed, time-domain techniques have been the mainstay of early research in this area, whereas other, more complicated, techniques are mathematically derived due to blooming digital watermarking technology, in which main approaches mostly focus on the transform domain, utilizing algorithms (e.g. Singular Value Decomposition: SVD [1], Discrete Fourier Transform: DFT [2],Discrete Cosine Transform: DCT[3], Discrete Wavelet Transform: DWT [4], Discrete Fourier Transform: DFT) to increase the probability of resilience against attacks, and improve performance. However, otherwise, there are still few surveys that tackle the topic of the use of these technologies in audio files that are not musical. This work is purported to present an innovative procedure of audio steganography, in which bits inside the sound files are selectively changed based on pre-determined criteria related to audio sample values; it significantly improves the conventional least significant bit (LSB) method. Therefore, this approach allows the possibility of illicit erasure or change of hidden information to be increased, while the likelihood of detection would be diminished.

1.1 Watermarking Procedure

Digital watermarking encapsulates copyright information into a host signal, making it undetectable and resistant to attacks. The embedding block Fig.1 uses a key to improve security, while the extraction block Fig.2 uses the same inputs, including the embedded object, key, and sometimes the watermark, to create the embedded signal or watermarked data.

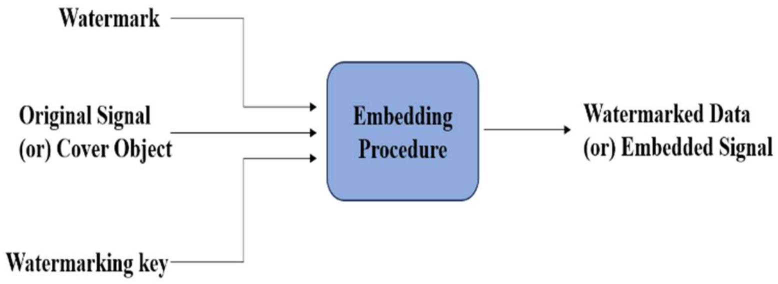

Watermark
Original Signal (or) Cover Object
Watermarking key
Embedding Procedure
Watermarked Data (or) Embedded Signal

Fig.1 Embedding process

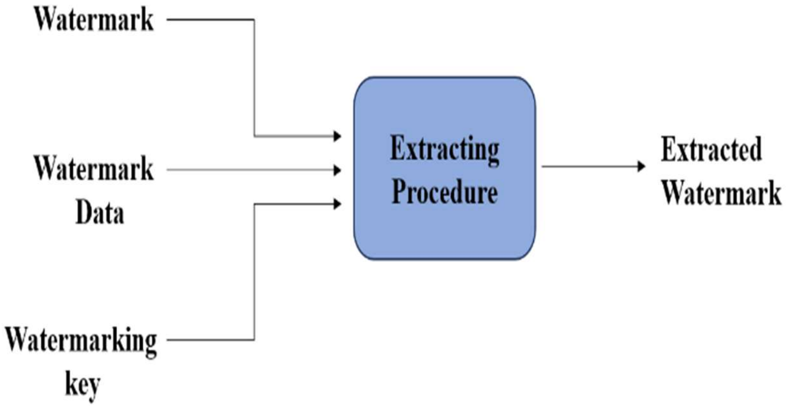


Fig.2 Extracting watermark

1.2 Characteristics Of Watermarking

There are several types of features that a watermark algorithm should have. These are briefly described below, and can be observed from Fig. 3.

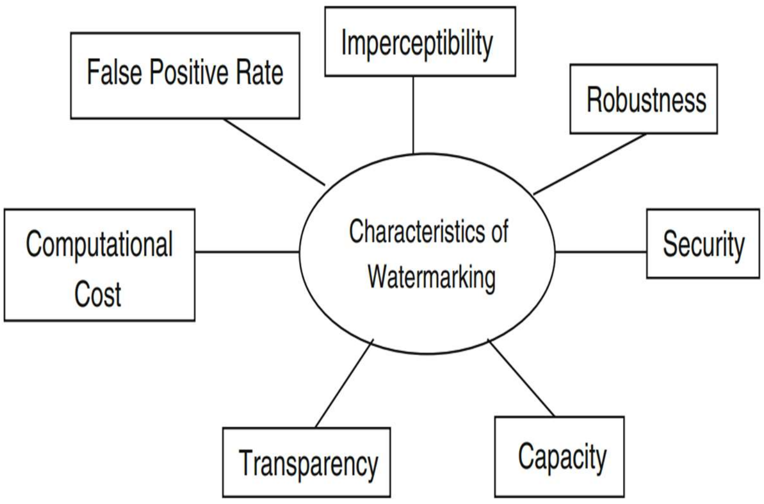


Fig.3 Characteristics of watermarking

1.2.1 Robustness

The watermark, hence, has to be robust against the different types of attacks that the host audio or image signal can suffer, such as processing operations, Digital-to-Analog (D/A), and Analog-to-Digital (A/D) conversions, filtering, linear, nonlinear, data compression, MP3, JPEG, and others, etc. It will ensure robustness by surviving various sorts of modifications and yet still remaining identifiable.It must also survive geometrical distortions such as scaling, rotation, cropping and all others that the signal may encounter through transmission or storage. The good robustness of a watermark implies that, besides surviving intentional tampering, it should also accidentally alter the content by incidental changes that may take place during normal media handling procedures.

1.2.2 Imperceptibility

This has to be done in a way that the host image or audio perceptual quality is not degraded, which means this has to be made imperceptible. For a watermark in an image, this would appear that the watermark must be unseen by human eyes. For an audio signal, it should be rode so human ears can not find degradation with respect to some of the original quality of the audio. Sophisticated schemes, such as embedding the watermark into areas of the signal that are less perceptible, like high-frequency components or low-contrast regions in images, make sure that when achieved, the watermark becomes imperceptible. However, this must be counterbalanced by robustness, as a high-strength watermark can be detectable and a low-strength watermark won't have the ability to survive most attacks.

1.2.3 Security

Security of the watermark means that the message content embedded in a watermark cannot be visually read or accessed in an easy-to-read manner for malicious reasons, nor can it be destroyed. This is done by encrypting the message content of the watermark such that during embedding, the only possible entity who can read the information is one who holds the proper key. Some of the techniques enclosed in the likes of Arnold's transform—which uses a secret key and screws the watermark in an intricate, reversible manner—are more secure methods of securing watermarks.The watermark should be secure so that an adversary will not detect and/or modify; therefore, the watermark should remain in-tact and confidential even under sophisticated attacks. In most cases, very important to their integrity because, acting as evidence, they are of ownership or authenticity.

1.2.4 Capacity

The term 'capacity' refers to the ability of information that can be embedded in a host signal without degrading its quality. This is where the trade-off exists when one tries to cross the limits of total embedded data. Here the imperceptibility of the signal and robustness get degraded. Good watermarking algorithms would, therefore, optimize the capacity so they could embed enough data but still offer the same quality of the original and remain robust to attacks. This is clearly very important in those applications where descriptive details - for instance, serial numbers, or user identification - must be embedded without changing the host signal, at least discretely. Also, a larger capacity has an effect on the watermark's detectability and resistance to a number of signal processing operations.

1.2.5 Transparency

This conveys that the watermarking process should lend transparency to not degrading the quality of the host media. The watermarked image can look as close as possible to the original one, in the case of images, with a minimum of visual artifacts. The audio watermark should not be heard with embedded information. This is important in terms of user acceptance, particularly in applications in which quality problems are critical, for instance, digital media distribution. Techniques like the embedding of a watermark in HSV regions help to achieve transparency. Transparency attains the quality where the watermark is invisible in normal use but visible if special means of extraction are applied.

1.2.6 Computational Cost

The computational cost of a watermarking algorithm refers to the time and resources it requires for embedding and extracting a given watermark. An ideal watermarking scheme is taken as one that imposes least computational overhead so that it becomes practical for real-world applications. This optimizes the algorithm in such a way that it does not increase computational time, while still maintaining other important characteristics, e.g., robustness and imperceptibility.Low computational cost is an applied feature, especially for real-time processing applications in digital content protection, such as live streaming. Furthermore, a decrease in computational complexity ensures that watermarking becomes feasible for devices with very low processing residuals, for example, mobile phones and embedded systems.

1.2.7 False Positive Rate

The false positive rate FPR in watermarking is the probability associated with a media file that will be inaccurately detected as holding a watermark, while in truth, there is really no watermark at all. A high FPR leads to contention in content ownership and substantially diminishes the dependability of a system. Effective watermarking algorithms aim at reducing FPR by employing robust detection and hybrid methodologies amalgamating SVD with other methodologies to achieve high accuracy. Reducing the FPR ensures credibility in the watermarking system, thus reducing misuse by attackers trying to falsely claim ownership of content. A low FPR ensures the integrity of the watermarking process, where genuine watermarks are correctly identified without a problem of false detection.

1.3 Performance Measure

Any watermarking purpose algorithm's performance is calculated by performance measures or matrices. It may be in terms of how robust the algorithm is against attacks, the quality of an image used, the watermarked capacity, time taken by the algorithm for embedding and extraction, and many other aspects. Some of the performance measures have been used to prove the quality of researchers' technique according to their needs. This article explains some of these performance measures that are used in watermarking fields.

1.3.1 Mean Square Error (MSE)

The Mean Square Error (MSE) calculates the average variance between the host and watermarked picture. Equation illustrates how an increased value reduces the quality of the image

$$MSE = \frac{1}{M*N} \sum_{x=1}^{M} \sum_{y=1}^{N} [C(x,y) - WC(X,Y)]^2 \tag{1}$$

$$MSE(color) = \frac{\sum_{Z=1}^{3} \sum_{x=1}^{M} \sum_{y=1}^{N} [C(x,y) - WC(X,Y)]^2}{3*M*N} \tag{2}$$

$C(x,y)$: pixel x, y is the host image. $WC(x,y)$: Watermarked image at pixel x, y. Z indicate number of planes in image. M, N: The host image’s dimensions.

1.3.2 Peak Signal Noise Ratio (PSNR)

This metric assesses how well a picture is either watermarked or stego. A higher PSNR value corresponds to greater watermarked picture quality. A PSNR of more than 27 dB is regarded as good. PSNR equation is shown in Eq.

$$PSNR = 10 * log \frac{255^2}{MSE} \tag{3}$$

1.3.3 Normalized Correlation (NC)

NC evaluates the similarity of vectors or pictures in watermarking to ascertain the relationship between the original and extracted picture. A process with a higher NC value indicates a stronger and more robust match.

$$NC(W,W') = \frac{\sum_{X=0}^{M} \sum_{Y=0}^{N} [W(x,y) W'(x,y)]}{\sqrt{\sum_{X=0}^{M} \sum_{Y=0}^{N} W'(x,y)} \sqrt{\sum_{X=0}^{M} \sum_{Y=0}^{N} W(x,y)}} \tag{4}$$

1.3.4 Bit Error Rate (BER)

The bit-error rate (BER) displays the variation between the recovered watermark image and the original. which is a measurement of the error rate in the transmission system, especially in watermarking.

$$BER(W, W') = \frac{number\ \ of\ errors}{Total\ number\ of\ bits} \tag{5}$$

1.3.5 Structural Similarity Index (SSIM)

A closer score denotes a higher degree of structural resemblance between the original cover photos and the inserted watermark pictures, as determined by SSIM. It attests to the watermarking method imperceptibility.

$$SSIM(C, WC) = \frac{\sum_{X=0}^{M} \sum_{Y=0}^{N} C(x,y) WC(x,y)}{\sum_{x=0}^{M} \sum_{y=0}^{N} [C(x,y)]^2} \tag{6}$$

In the case of color pictures, SSIM (C, WC) is equal to the product of the RGB components of the original and watermarked images.

1.4 Watermarking Attacks

Watermarking schemes are vulnerable to various types of attacks aimed at removing, altering, or detecting the watermark. These attacks can be classified into several categories, including image processing attacks, geometric attacks, cryptographic attacks, protocol attacks, and others.

1.4.1 Image Processing Attacks

Filtering Attacks:

- Sharpening Filter: Enhances the edges of the image, which may either strengthen or weaken the watermark depending on its embedding strategy.
- Smoothing Filter: Reduces noise and details in the image, potentially distorting or removing the watermark.
- Median Filter: Replaces each pixel's value with the median value of its neighbors, often used to reduce noise, which can blur or distort the watermark.
- Mean Filter: Uses the average of the surrounding pixels' values, similar to smoothing filters, and can reduce watermark visibility.
- JPEG-2000 Compression Attack: JPEG-2000 is a wavelet-based image compression standard that achieves high compression ratios and reduces

blocky artifacts common in DCT-based JPEG compression. The high compression can significantly alter the embedded watermark, making it difficult to detect or extract.

1.4.2 Geometric Attacks

- Image Scaling: If the size dimensions of the image are reduced and increased, then the watermark can be distorted to the destructive point where it is no longer recognizable. For example, reducing an image in half and then resizing it back up to its original size can achieve very poor results in maintaining the integrity of the watermark.
- Rotation Attack: In this attack, one can rotate the watermarked image by an addition of angle and then crop it so that the watermark will only reveal itself to a person who has prior information about the added angle.
- Image Clipping: If regions of an image identified by the watermark have been clipped, then those regions no longer contain the watermark. Typically, the clipped image needs the original cover image in order to estimate what was cut away for watermark recovery.

1.4.3 Cryptographic Attacks

- Key Extraction Attack: Here the attacker tries to extract the watermark key using cryptographic analysis. After the retrieval of the key, a miscreant can tamper with the watermark or insert a new watermark in the cover image.

1.4.4 Protocol Attacks

- Copy Attack: The watermark from part of the image is extracted in this attack and then it is embedded in another part of the images so that there becomes some ambiguity. This attack does not remove any watermark but rather uses it to create confusion regarding the removed authenticity of location of the artifact.

1.4.5 Simple Attacks

- Manipulation of Watermark Data: An attack that attempts to damage the watermark itself, embedded in a signal, by manipulating all data of the watermark, such as noise addition or re-encoding of the signal.

1.4.6 Detection Disabling Attacks

- Breaking the watermark detection: This research tries to break the relationship between the watermark and the detector, which means that the watermark should be undetectable. Techniques used are modifications of synchronization points and embedding patterns.

1.4.7 Ambiguity Attacks

- Watermark and Host Data Analysis: This method tries to separate the watermark data from host data, such that it is not possible to determine the parts that belong to the watermark or the original information.

1.4.8 Watermark Copy Attack

- Estimation and Filtering: The watermark estimation in the spatial domain is replaced by some other place inside the image to sow confusion.

1.4.9 Time Stretch and Pitch Shift

- Stretch and Shrink: Time stretching changes the length of the audio signal without affecting its pitch; pitch shifting changes the pitch without altering the length. Either change might cause distortion in the watermark embedded.

1.4.10 Dynamic Attacks

- Amplitude Modulation and Reduction: In this method, the amplitude of the audio signal is altered in order to suppress or lower the watermark. This could be done through dynamic range compression, amongst other types of amplitude altering methods.

1.4.11 Removable Attacks

- Publication Removal: Attacks with this aim remove the watermark from the host signal completely. Such an attack is possible since, in most cases, the watermarks are just additive noise signals.

1.4.12 Low Pass Filtering Attacks

- Noise Filtering: A low pass filter can be superimposed on the watermarked signal that reduces high-frequency components. It may either make the watermark far less visible or eliminate it entirely if it relies on high-frequency information.

1.4.13 Forgery Attacks

- Object Insertion and Deflection: Insertion of new objects or deflection of existing ones in the signal to change a scene, background changes and so on may render the watermark unidentifiable.

1.4.14 Active Attacks

- Deliberate Watermark Removal: In these active attacks, a copyright violator directly removes the watermark or makes it imperceptible, hence seriously threatening the copyright protection.

1.4.15 Passive Attacks

- Detection Without Removal: Such attacks are not giving effort to remove the watermark but just to detect its existence. Maybe it is important in a secret communication environment that even knowing a watermark exists is damaging.

1.5 Application Of Watermarking

Audio watermarking has numerous applications in the large number of fields. Here are the main applications classified by the specific uses and goals:

1.5.1 Copyright Protection

- These are, therefore used as a proof of possession by watermarking them within audio recordings. There a dispute in copyright, the watermark is extracted to determine ownership. To be effective watermarks have to be imperceptible to the copyright owner and must survive common audio processing yet be recoverable.
- Proof of ownership: In all cases of copyright infringement, an embedded watermark extracted from the disputed audio can be used to assert actual ownership. The in-built information acts as an undisputable item of evidence within a court of law that assures no unauthorized claim over the contained content will be made.

1.5.2 Copy Protection

- Copy Control Watermarking can enforce policy information regarding copy control and access. It will detect unauthorized copying of digital audio files. To prevent illegal duplication of the CDs and DVDs and other digital audio technologies. That way, the watermark ensures only an authorized user will do a copy, offering protection from piracy of the content.
- Content Filtering: Watermarking is used in the access control of multimedia content with set-top boxes and other interactive devices. The content provider can, therefore, use content embedding by watermarking to ensure that the distribution agreement is observed and viewing is limited to only legitimately interested parties.

1.5.3 Validation of Genuineness

- Authentication: Watermarking can be used for authenticating audio content: A digital signature embedded as a watermark ensures that any change in the audio results in changes in the watermark, which ultimately helps to detect the change in the audio content and confirm its source.
- Tamper Detection: Fragile watermarks are used, which allow the detection of quality in the original data. In the event of alteration on the audio signal, the fragile watermark will be destroyed, showing tampering. This is crucial in order to maintain the audio content's integrity.

1.5.4 Broadcast Monitoring

- Tracking Broadcasts The embedded watermarks in audio signals broadcast could potentially enable tracking and real-time monitoring of the broadcast. From time to time, the computer system recognizes the watermark in a broadcast for verification and logging information about compliance with copyright and other concerns.

1.5.5 Forensic Analysis

- Follow the Flow: Agencies might insert forensic watermarks that trace the route of distribution of audio files. This is helpful for red-flagging redistributors who download and redistribute content illegally. The information is further extracted to ascertain the source of unauthorized redistribution.

1.5.6 Fingerprinting

- Unique Identity: Watermarking watermarking techniques can be used to embed unique identification into each copy of an audio file, which enables tracking of the individual recipients. This is very useful in identifying end users who break license agreements by copying illegally or redistributing the content again.

1.5.7 Airline Traffic Monitoring

- Airline Traffic Monitoring Safe Communication: In air traffic control, watermarks are enabled to embed flight numbers and other critical information within voice communications between a pilot and ground control. This makes it secure from unauthorized interception and tampering of the communication signals.

1.5.8 Medical Applications

- Bi Patient Identification: The detail of the patient's information can be embedded into medical pictures through watermarking techniques, such as radiographs and MRI images, making it possible to accurately link the details of the patient's medical record with the patient and avoiding confusions so that the treatment is accurate.

1.5.9 Information Carrier

- Information Carrier Metadata broadcasting Watermarks, therefore, may be used in the embedding of more information in audio files in the form of metadata while respecting the need for their use within such applications where supplementary information is to be carried alongside main audio content, hence increasing the data-carrying capacity of an audio file.

CHAPTER 2

LITERATURE SURVEY

2.1 Classification Of Watermarking Techniques

watermarking techniques are commonly categorized into three domains: Spatial, Frequency, and Hybrid. This section provides a comprehensive review of various audio watermarking methods, including LSB replacement, spread-spectrum, echo hiding, patchwork, as well as transformations like DWT, DFT, DCT, DWT-SVD[5], DCT-SVD[6], and DCT-DWT[7].

2.1.1 Spatial Domain

Spatial domain techniques embed the watermark directly into time domain with absolutely no transformation. The methods are simple and computationally efficient but offer no robustness. Several techniques used in this domain include least significant bit replacement, echo hiding, phase coding and spread spectrum, among others. Sadasivam Subbarayan et al.[8] proposed an audio watermarking using LSB in which the watermark is encrypted with RSA to make it more robust. The increment of robustness of a watermark due to encryption before embedding ensures better security of information embedded in data under consideration. Cvejic et al. [9] proffered an LSB audio watermarking scheme for stereo audios that disseminate watermark bits over the left and right channels, to enhance invariance to distortion. There is some signal of this kind used to embed the watermark in both channels, thus reducing the effect of distortion caused by the nature of the specific channel; meanwhile, it may interfere with the message payload. This is one way toward better perceptual quality.Hyoung Joong Kim et al. [10] proposed an echo-hiding algorithm with a new forward and backward kernel for blind audio watermarking. The embedding capacity in the proposed technique could be 10 bps. Echo hiding ensures more robust been making without requiring the original audio for extraction, hence lending itself very well to practical applications.Darko Kirovski [11] and Henrique Malvar have done work on the audio watermarking scheme that can withstand desynchronization attacks while adhering to all the requirements posed by the perceptual and 10^-6 error probability. The watermark is embedded in a spread spectrum manner. The spread spectrum-based watermarking retains its indiscernibility because it keeps the watermark hidden from human perceptions.The watermarking algorithm proposed by Moumita Saha et al. in [12] employs non-blind RSA-based embedding with LSB substitution, making the embedded watermark more robust and secure against possible manipulations. The RSA encryption does guarantee the embedded watermark to be very secure and robust to unauthorized extraction or tampering, hence ensuring the security of the content to be watermarked. Anu Binny et al. [13] worked on the hiding of text information in audio signals based on LSB and achieved very good SNR at different bit rates. The use of LSB embedding has hidden the text information, making the method very simple to implement for embedding textual information into audio files for secret communications or metadata embedding. Sathiamoorthy et al. [14] advanced the LSB embedding and echo hiding technique one step further with T-codes, which provided improved robustness to attacks compared to just LSB embedding. The use of echo hiding plus the LSB embedding technique will obtain higher resilience against the most usual signal processing attacks to ensure the integrity and security of the embedded information.

In this direction, Nedeljko Cvejic [15] demonstrated a new method for audio watermarking that has much greater robustness than conventional watermarking methods when attacked by low-pass filtering and resampling. It enhances the reliability of watermarking detection for integrity under tough environments through characterization and mitigation of such common signal processing attacks.Extended LSB Replacement Techniques Researchers have worked in the domain of traditional LSB replacement and proposed advanced methodologies toward higher levels of robustness and security. For example, Liang Xiao et al. [16] put forward a novel reversibility data hiding method for enlarging the prediction error in the case of LSB substitution; such a method can support reversible data embedding with the key property that the embedded watermark is not perceptible.

2.2 Frequency Domain

The audio watermark is directly embedded in the frequency domain by modifying the respective domain without any transformation. Although the transformed domain is usually computationally more compared to other domains and increases robustness, it provides various techniques embeddings of watermarks in the digital audio signal, which includes FFT, DCT, DWT, and SVD.FFT-based Watermarking by Xiumei Wen et al. [17]. The scheme embeds watermark information in the phase coefficient of the audio signal using Fast Fourier Transform. If the embedded intensity value is equal to 0.1, then the algorithm attains an inaudible SNR of 43.5 dB and remains highly robust against several different kinds of signal processing attacks.SVR Watermarking [18] by Wang and associates: Wang and his team have designed an adaptive, blind digital audio watermarking algorithm involved in the

SVR. Watermark information gets embedded in original audio signal through an adaptive form of quantization. By using the 64x64 bit binary image as watermark, the PSNR of the algorithm is very high at 50.445 dB, while its normalized cross-correlation reaches 1.00, which is very robust and practical.Additive Watermarking Algorithm Based on DWT by B. Charmchamras, et al.[19]: The DWT algorithm executes audio watermarking with the assistance of Additive Binary Images. The performances in this algorithm show robustness against a variety of attacks because its average Normalized Cross-Correlations are beyond 85%, even under low-pass filter attacks, AWGN, and re-sampling attacks. Furthermore, the adaptively modulating the scaling parameter is based on the SNR.Wavelet Domain Watermarking: A blind audio watermarking using wavelet domain decomposition to embed a watermark image into the audio signal was proposed by Kaengin et al. [20]. These normalised correlation values were in the range of 0.8578-1, which showed a very good SNR of 49.44 dB with such a technique and proved to be robust against AWGN, resampling, requantisation, low-pass filtering, and MP3 compression attacks.Watermarking in the Time Domain Based on NDFT by Ling Xie et al. [21]: A secure audio watermarking scheme was reported to be based on non-uniform discrete Fourier transform by Xie et al. The coupled chaotic sequences adopted in the scheme are used for watermark embedding. The SNR is kept in the range from 33.7254 to 34.5542 under different attacks, indicating the robustness of this algorithm to MP3 compression, resampling, low-pass filtering, and re-quant. Self-Synchronization Watermarking. Shaoquan Wu et al. [22] described a self-synchronization algorithm in an audio watermarking scheme based on Haar wavelet transformation. The self-synchronization has enabled robustness of the algorithm leading to zero BER and to the aforesaid imperceptibility, even at a bit error rate of 0.07% under MP3 compression (96 Kbps) with 172 bps of payload.Watermarking Schemes QIM Following Work by Nima Khademi et al.[23] : Based on the work of Khademi et al., a blind audio watermarking technique in the frequency domain was proposed employing a QIM approach. The algorithm shows robustness and reliability with a BER of 0 at an SNR of 12.5 dB in the presence of various attacks that would occur in normal signal processing.The system proposed by Charfeddine Maha et al. in [24] embeds inaudible information within digital audio using the Human Psychoacoustic Model, Discrete Wavelet Transform, Neural Networks, and Error Correcting Codes. Using Neural Networks with memorization for securing the system and Hamming ECC for robustness, the method allows one to achieve invisible watermarking and hence blind watermarking for the system.SVD in MCLT Domain Watermarking: Zezula et al. [25] introduce digital audio watermarking with the Singular Valued Decomposition method in Modulated Complex Lapped Transform domain. This is a blind watermarking technique which falls into the category of methods insensitive to some of the more common attacks in audio signal processing. Imperceptibility was quantified by means of SNR measurements over a number of music genres.Biometric-based watermarking of Kaur et al. [26]: Kaur et al. proposed a high-payload watermarking approach for digital audio signals. Here, the watermark was imbibed using biometric features out of the iris images. High payloads can be implanted at the third level of decomposition with QR decomposition, robust against processing signal attack while being perceptually transparent.Blind Wavelet Domain Watermarking: Arashdeep Kaur et al. [27] Kaur et al. addressed a blind audio watermarking algorithm in the wavelet domain with emphasis on high embedding capacity and robustness against common signal processing attacks. This has been shown to work effectively in music from various genres, maintaining high perceptual transparency by showing low SNR values of 33.1806 dB to 44.2179 dB.These techniques demonstrate the possible diversity and effectiveness in audio watermarking, based on the frequency domain, especially through robustness to arbitrary signal processing attacks, inaudibility, and transparency to high payloads, as well as perceptual transparency.

2.3 Hybrid Domain

Watermarking: The above scheme of embedding a watermark, using DWT-SVD-based watermarking by Krishna Rao Kakkirala et al. [28], is a blind audio watermarking approach which inserts all bits of the watermark into the Eigen values of audio frames. This technique is valid against the known formats of compression, changes in sampling rate, and attacks commonly performed in the processing of signals, with an accuracy rate of up to 99.6 under Gaussian noise.Audio watermarking using DCT-SVD by Suresh et al. [29] presents a blind audio watermarking method in the frequency domain using DCT and SVD. It makes a comparative summary in this paper between the methods, while on PSNR, MOS, and PCC, this DCT-SVD method is very nice compared to DWT-SVD, which is efficient but has a moderate PSNR.QIM-based Watermarking Hwai-Tsu Hu et al. [30] proposed a blind audio watermarking scheme for energy compensation using QIM to rectify the limitations of the DWTDCT. The developed scheme exhibited high robustness and invisibility, to the extent that users could hardly make any differences between the compensated and uncompensated schemes.Watermarking using SVD with dither modulation with differential evolution: audio

In the technique presented above, good visible watermarking has been achieved, although the imperceptibility and robustness of the method required improvement. The results were indicative that the proposed method showed a very fine imperceptibility and was becoming highly robust. SVD-DCT-based Watermarking by Pranab Kumar Dhar et al.[31] : It proposes an audio watermarking system with SVD and DCT, injecting the watermark information into the largest singular value. Some very unique schemes have been adopted, such as an embedding tool using variable strength. The method is robust to attacks of low error probability.The comparison of the DCT-SVD and DWT-SVD methods was further in Watermarking by N. V. Lalitha et al. [32] where a scheme for efficient, inaudible audio watermark embedding in the frequency domain was introduced. It then formulated good imperceptibility and robustness against such a large set of attacks as the DWT-SVD did.Watermarking Scheme Based on SVD-DCT by Bai Ying Lei et al.[33]: A blind watermarking scheme for audio is proposed, which is robust against most common signal processing attacks to a low error probability rate of occurrence. In tests, it showed good imperceptibility with high SNR, MOS, and SegSNR values.Watermarking by SVD-DWT by Vivekananda Bhat K et al. [32]: This is a scheme for blind adaptive audio watermarking in the DWT domain on the basis of SVD with synchronization code. In this case, the expected properties are robustness against attacks on signal processing and high payload capacity, especially against MP3 compression.SVD-DWT-based Watermarking by Huan Zhao et al.[34] proposed a new blind audio watermarking in SVD with DWT, inserting the watermark into approximate components extracted from the DWT decomposition through that. Effective robustness against common operations of audio signal processing with excellent imperceptibility.SVD-LPT-DCT-Based Watermarking: Dhar et al. [35] presented an audio watermarking method using the entropy property, SVD with LPT, and DCT-based data embedding in the components with maximum entropy value. The experiment shows better performance than existing watermarking methods, showing high SNR and MOS values.SVD-DCT-WNN-based Watermarking by Alka Singh et al.: A hybrid technique for digital watermarking is proposed in this research by using the concepts of SVD-DCT and WNN to make a robust scheme for audio watermarking. This scheme embeds the watermark by SVD and DCT; WNN was used in the scheme for additional supportive security.DWT-DCT-SVD-based watermarking: The hybrid watermarking technique is introduced in related works in the area of audio watermarking, where a signal decomposition using DWT is performed. Besides, there is the need for an energy compaction spectral representation in the

DCT and embedding of the watermark in the SVD to render it resistant to various signal processing operations. These techniques are usually robust, imperceptible, and optimizable for capacity in the hybrid domain, by combining strengths in various FD methods in order to tackle different signal processing attacks and perceptual constraints.

Table.1 categorizes techniques into Spatial or Transform domains, focusing on robustness, imperceptibility, security, and data capacity. It outlines experiment types, sizes, and results, noting constraints and observations.

TABLE.1 Analysis of various watermarking

Sr. No	*Analysis of various watermarking*				
	Techniques	***Purpose***	***Image and Watermark Image Dimension***	***Outcomes***	***Limitations/Observation***
1.	DWT,DCT, RCNN [36]	Resilience & Invisibility	COCO/4*4 Dataset	Peak-signal-noise-ratio = 49.1052, SSIM = 0.9985, Normalized Correlation =1	Bits are embedded 15 times, improving redundancy by blind watermarking depending on ROI.
2.	PCA,RDWT, IGWO[37]	Resilience & Invisibility	Grayscale (8 - bit)	Peak-signal-noise-ratio = 67.87, Normalized Correlation = 0.995, SSIM = 0.9997	A suggested better watermarking system is based on PSAs. Color photos are amenable to enhancement.
3.	Dual Tree CWT [38]	Resilience & Invisibility	Color 512*512, Binary 128*128	Peak-signal-noise-ratio = 41.23	Since no attack is carried out, robustness is not verified.
4.	DWT, SVD, Pixel position [5]	Resilience, Security & Invisibility	Both Gray 512*512, 32*32	Peak-signal-noise-ratio = 42.63, Normalized Correlation=1	The result was verified without any attacks, demonstrating good robustness and imperceptibility.
5.	Encryption, Discrete Wavelet Transform [4]	Resilience & Invisibility	Both Gray 228*228, 90*90	Peak-signal-noise-ratio =55, Normalized Correlation = 0.9749	Geometrical attacks are not Compared.
6.	DWT-Singular Value Division, IDWT-Singular value division, RDWT-SVD [39]	Resilience, Privacy & Invisibility	256*256, binary LOGO	Peak-signal-noise-ratio =54.51, Normalized Correlation=0.9993, SSIM = 0.999	Less Stability

Sr. No	***Analysis of various watermarking***				
	Techniques	***Purpose***	***Image and Watermark Image Dimension***	***Outcomes***	***Limitations/Observation***
7.	DWT,DCT, Discrete Fractional Random Transform [DFRT] [40]	Resilience & Invisibility	512*512, 256*256	NC = 0.9940, SSIM = 0.9740	For host pictures, coefficients are utilized often.
8.	DCT, DWT, SVD, Arnold Transform [6]	Resilience & Privacy	512*512, 256*256	Peak-signal-noise-ratio = 34.68, NC = 0.9973	SPIHT (SetPartitioni in HierarchicalTrees) used for compressed watermarking.
9.	Quaternion Hadamard transform, Schur decomposition [41]	Resilience& Invisibility	RGB, 512*512*24, 64*64*2	SSIM = 0.9917, Normalized Correlation=1	Lesser Complexities
10.	DWT, SVD, DC Coefficients [42]	Resilience	512*512, 32*32	Normalized Correlation = 0.9724	Used together, SVD and DWT
11.	DWT and Cuckoo search [43]	Resilience& Invisibility	256*256, 128*128/64*64	Peak-signal-noise-ratio = 38.03, NC = 0.9613	Watermark conflicting factor balance.
12.	DWT, SVD, Arnold map [44]	Sturdiness, Invisibility of Privacy, & Capacity for Payload	Both Color 512*512, 512*512	Peak-signal-noise-ratio = 77.48, SSIM = 0.9940, NC > 0.9	Superior in capability and defense against intrusions and NC outcomes. Better in security against attacks.
13.	DWT, SVD, Block selection scheme [45]	Resilience & Privacy	Color 512*512, Binary 50*20	Peak-signal-noise-ratio = 61.75 SSIM = 0.9999	Adjustments are required for fidelity, false positive rate (FPR), and active attacks
14.	Reinforcement ML, WMnet [46]	Resilience & Invisibility	Boss Base Dataset, color 512*512	Peak-signal-noise-ratio = 40, NC = 1	Better than QIM
15.	TSDL, YUV Space [47]	Imperceptibility & Robustness	Dataset COCO	Peak-signal-noise-ratio = 63.4	Decent Watermark Output

Sr. No	***Analysis of various watermarking***				
	Techniques	***Purpose***	***Image and Watermark Image Dimension***	***Outcomes***	***Limitations/Observation***
16.	DCT, DWT, Arnold Transform [3]	Security & Invisibility& Robustness	Grayscale 512*512	Peak-signal-noise-ratio =47.18, Normalized Correlation = 0.1936	Need to keep PSNR and NC in a healthy balance.
17.	DWT, DCT, Arnold Transform, Hamming Code, Arithmetic compression [48]	Resilience, Privacy & Imperceptibility	Gray 256*256, 512*512	Normalized Correlation =0.9888, BER= 0.2174, Peak-signal-noise-ratio =43.88	Poor quality watermarked picture is produced when the gain factor is high.
18.	RDWT (Redundant DWT), SVD [49]	Resilience& Privacy	Grayscale 512*512	Peak-signal-noise-ratio = 53.61	Poor in preventing root attacks .
19.	Entropy, Hadamard transform [50]	Resilience& Privacy	Both Grayscale 512*512, 64*64	Peak-signal-noise-ratio = 47.98, Normalized Correlation = 0.9942	Low resistance to mean filter
20.	DPSO(Dynamic PSO), DWT, SVD [51]	Resilience & Invisibility & Privacy	Color	Peak-signal-noise-ratio = 39.79	Robustness is not checked in this approach
21.	FFT (Fast Fourier Transform), Pixel shuffling [52]	Resilience& Invisibility, Privacy	Gray	Peak-signal-noise-ratio = 44.28, BER = 0, Normalized Correlation = 1	Scheme is effective and safe, it provides no outcome comparison.
22.	Fast RCNN (DCT, DWT)[53]	Robustness, Security & Imperceptibility,	Image Dataset	Peak-signal-noise-ratio = 50.12	RCNN used to increase the Speed.
23.	DCT, Arnold [2]	Copyright protection	Both Gray 512*512, 19*12/64*64	Peak-signal-noise-ratio = 61.28, Normalized Correlation > 0.9, SSIM = 0.9998	Because the middle component is utilized for concealment, robustness is bad.

Sr. No	***Analysis of various watermarking***				
	Techniques	***Purpose***	***Image and Watermark Image Dimension***	***Outcomes***	***Limitations/Observation***
24.	QDWT,DCT, Arnold [3]	Resilience& Privacy	Color 512*512, Binary 64*64	Peak-signal-noise-ratio = 49.61, Normalized Correlation > 0.9	The middle part is hidden, thus toughness is not ideal.
25.	DWT, Chaotic DCT [54]	Invisibility	Gray 512*512	Cor = 0.9697	Implementing this process against a multimedia application is difficult.
26.	DCT, 2D LDA[55]	Invisibility	Color 512*512,32*25	Peak-signal-noise-ratio = 44.49, BER =0	Easy to implement

CHAPTER 3

METHODOLOGY

3.1 Theoretical Structure Of The Algorithm

This proposed method to hide image in audio file (.wav) as shown in Fig.4.

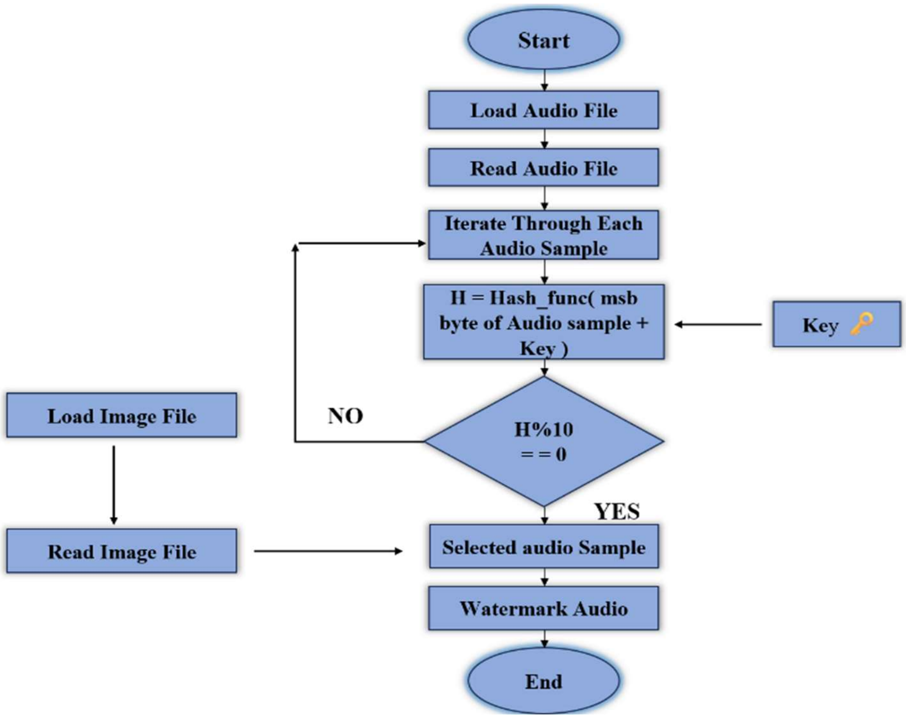


Fig.4 Flow diagram of proposed techniques

This section explicates the theoretical framework of our innovative steganographic approach, divided into three main phases: 'Embedding Technique', 'Embedding Procedure', and 'Extraction Procedure'.

3.1.1 Embedding Technique

Our method exploits the properties of digital audio to embed a grayscale image within a host audio file, utilizing the 16-bit depth of audio samples. This depth allows for bit-level manipulation that is imperceptible in audio playback, ensuring the steganography remains undetectable. By strategically embedding information within these samples, we enhance the security by making the pattern of modifications unpredictable and thus more resistant to steganalysis.

3.1.2 Embedding Procedure

- **Audio and Image Preparation:**

  The host audio file is loaded into the array and if it is stereo then only the first channel is used in order to make a consistent processing template.

  First of all each images are in the form of grayscale, then it converted to a binary bitstream. For a pixel, a bitstream is unpacked from grayscale values, in which it takes 8 bits for one pixel.

- **Selective Audio Sample Criteria:**

  Perform a loop through the audio samples, which are in the form of 16-bit integers. Selection of the samples is done by the pre-defined criterion, which warns away from the uncertainty principle and hence guarantees better security. The criterion is defined by the MSB byte of every 16-bit audio sample:

  - **Hashing MSB with Secret Key:**

    Here, for each sample, the upper byte in the 16-bit sample is taken out. The byte is then concatenated with a key and is hashed with a secure hash function, such as SHA-256. The hash is then converted to an integer towards such an operation of modulo.

  - **Sample Selection**

    Perform a modulo operation on the integer hash value. Select the audio sample for embedding if the result of the modulo operation is a specific value e.g. hash value % 10 == 0 . This selection process is illustrated in the updated Fig.5. and ensures that only a subset of samples is used, preserving audio quality and enhancing security through unpredictability.

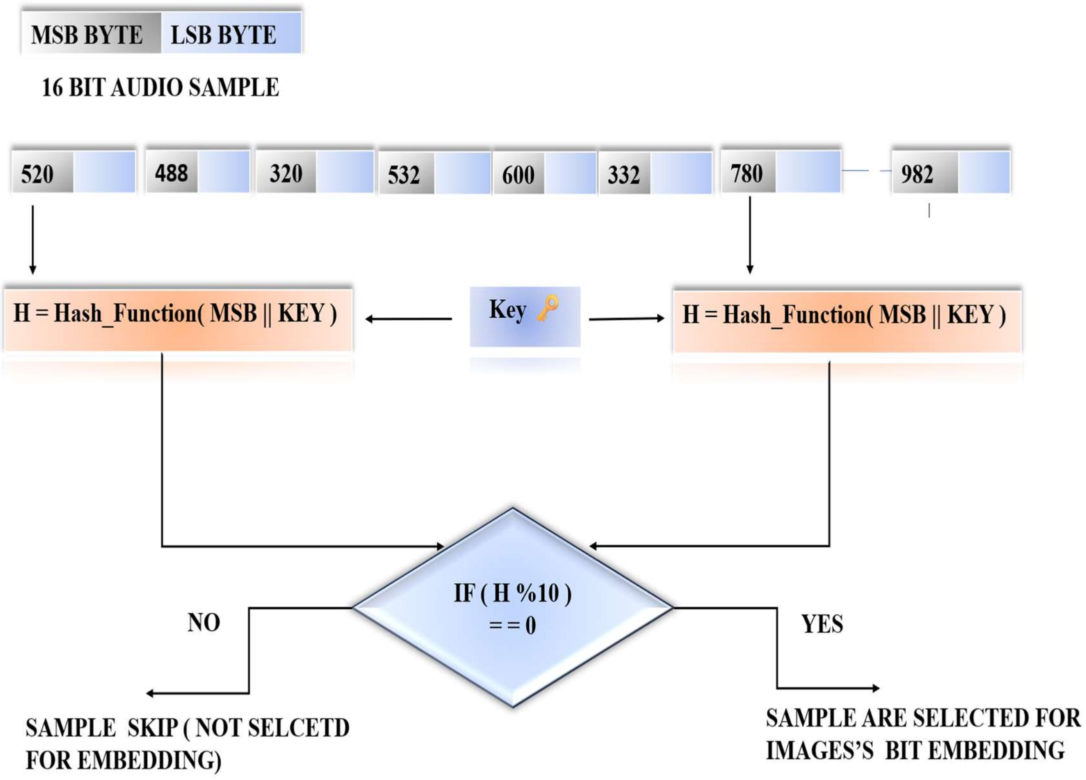

MSB BYTE
LSB BYTE
16 BIT AUDIO SAMPLE
520
488
320
532
600
332
780
982
H = Hash_Function(MSB || KEY)
Key
H = Hash_Function(MSB || KEY)
IF (H %10) = = 0
NO
YES
SAMPLE SKIP (NOT SELCETD FOR EMBEDDING)
SAMPLE ARE SELECTED FOR IMAGES'S BIT EMBEDDING

Fig.5 Selecting sample for embedding bit

- **Embedding Image Bits into Audio Samples:**

  For each selected audio sample, bits from multiple images binary bitstreams are embedded at specific bit positions Fig.6 within the LSB byte of the selected audio sample to minimize perceptual audio distortion.

  This embedding uses bitwise operations to set or clear bits of LSB byte of selected sample at positions such as the 1st, 3rd and 5th bits of the sample(Embed Image 1's bit at the least significant bit position (b0) , Embed Image 2's bit at position b3,and Embed Image 3's bit at position b5), The target bit positions are first cleared, and then the bits from the images are embedded into these positions. This careful embedding ensures that each selected audio sample contains bits from all three images in specified positions, maintaining the integrity of the audio while embedding the watermark data.

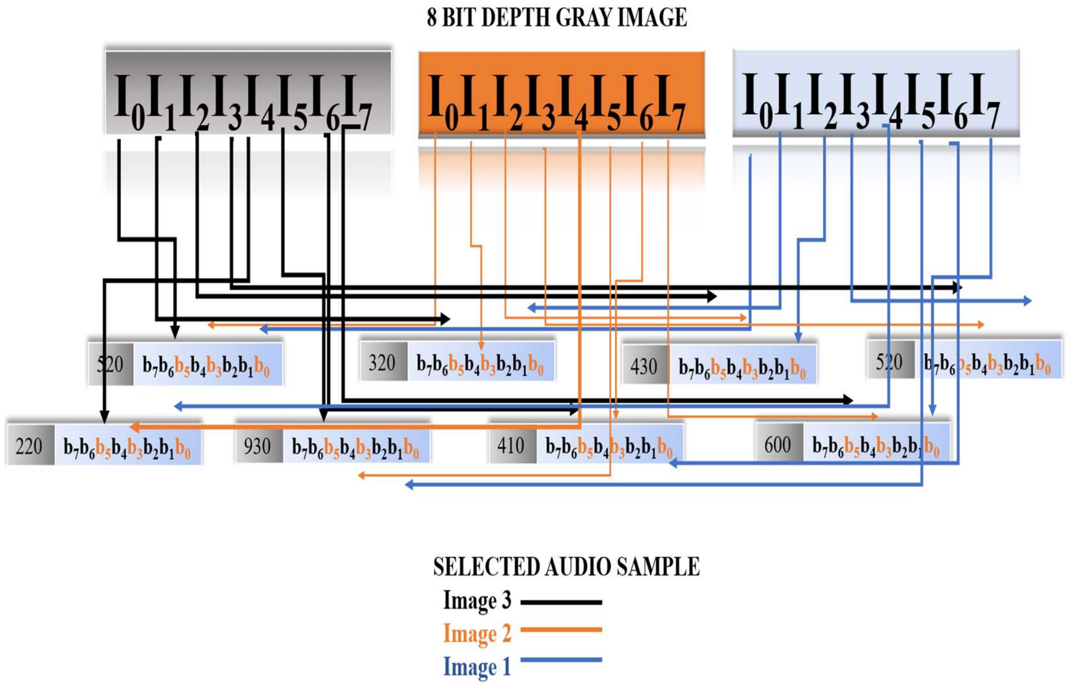

8 BIT DEPTH GRAY IMAGE
$I_0I_1I_2I_3I_4I_5I_6I_7$
$I_0I_1I_2I_3I_4I_5I_6I_7$
$I_0I_1I_2I_3I_4I_5I_6I_7$
520 $b_7b_6b_5b_4b_3b_2b_1b_0$
320 $b_7b_6b_5b_4b_3b_2b_1b_0$
430 $b_7b_6b_5b_4b_3b_2b_1b_0$
520 $b_7b_6b_5b_4b_3b_2b_1b_0$
220 $b_7b_6b_5b_4b_3b_2b_1b_0$
930 $b_7b_6b_5b_4b_3b_2b_1b_0$
410 $b_7b_6b_5b_4b_3b_2b_1b_0$
600 $b_7b_6b_5b_4b_3b_2b_1b_0$
SELECTED AUDIO SAMPLE
Image 3
Image 2
Image 1

Fig.6 Embed images bit on each selected audio sample

- **Writing the Modified Audio:**

  After embedding the image data, the modified array of audio samples is written back to a new audio file.

3.1.3 Extraction Process

- **Retrieving the Watermarked Audio**

  Load the watermarked audio file, again extracting only the first channel if the file is stereo, to align with the embedding process.

- **Extracting Embedded Image Bits**

  Hashing and Sample Identification: Traverse the audio samples, Apply the same hashing and modulo operation with the secret key to identify the audio samples that contain embedded image bits.

- **Bitstream Recovery**

  For each identified sample, the bits from the designated LSB positions are extracted. These bits correspond to the binary bitstreams of the multiple images embedded earlier.

- **Reconstructing the Image**

  Collect the extracted bits sequentially until enough bits are gathered to reconstruct the entire image, compensating for any missing bits with zeros if necessary due to errors or modifications during the audio's lifecycle. The bits are then repacked into bytes and reshaped into the original dimensions of the image using array manipulation tools from the NumPy library and image handling capabilities of the PIL library.

- **Output the Reconstructed Image**

  The reconstructed grayscale image is saved to an output file for visual verification against the original, demonstrating the effectiveness of the embedding and extraction processes.

3.2 Mathematical Implementation Of Algorithm

For the embedding and extraction process, it is useful to describe the operations mathematically to give clarity to the process and justify the selection criteria and manipulation techniques used.

3.2.1 Embedding Process

- **Audio Sample Selection**

  The MSB byte extracted from each sample is then hashed together with a secret key to determine if the sample should be used for embedding.

$$MSB = \left((S_i \gg 8)\&0xFF\right) \tag{1}$$

$$H_i = SHA\_256(MSB \oplus Key) \tag{2}$$

$$Select\, S_i\, if \quad H_i\%10 == 0 \tag{3}$$

Where:

H_i: Is the hash output

Key: Is the secret key

S_i: Selected audio sample

MSB: Is the most significant byte extracted from the Audio sample.

$\oplus$: Denotes the concatenation of the MSB and key.

- **Bit Embedding**

  Clears at specific positions (eg. b_0, b_3, b_5) of the LSB byte of the selected audio sample S_i and sets them with bits (I_1, I_2, I_3) from the images' binary bitstreams, creating the new sample S_i'.

$$S_i' = S_i \& \sim ((1 \ll 0) \mid (1 \ll 3) \mid (1 \ll 5) \mid (I_1 \ll 0) \mid (I_2 \ll 3) \mid (I_3 \ll 5) \tag{4}$$

S_i': Watermarked sample (modified audio sample)

b_0 , b_3 , b_5: are the bit positions where image data is embedded.

I_1, I_2, I_3: are the bits from the images' binary bitstreams.

3.2.2 Extraction Process

- **Identifying samples containing embedded bits**
  - Identifies samples S_i' that likely contain embedded bits.

    $$MSB = \left((S_i' \gg 8) \& 0xFF\right) \tag{5}$$

  - Using the same secret key, we compute the hash:

    $$H_i = SHA\_256(MSB \oplus Key) \tag{6}$$

- **Apply election criteria**

  $$Select\ S_i' = \left((H_i\ \%10) == 0\right) \tag{7}$$

- **Extracting bits**

  Retrieves image bits I_1, I_2, I_3 embedded during the embedding process from the bit positions b_0, b_3, b_5.

  $$I_1 = (S_i' \gg 0) \& 1 \tag{8}$$

  $$I_2 = (S_i' \gg 3) \& 1 \tag{9}$$

  $$I_3 = (S_i' \gg 5) \& 1 \tag{10}$$

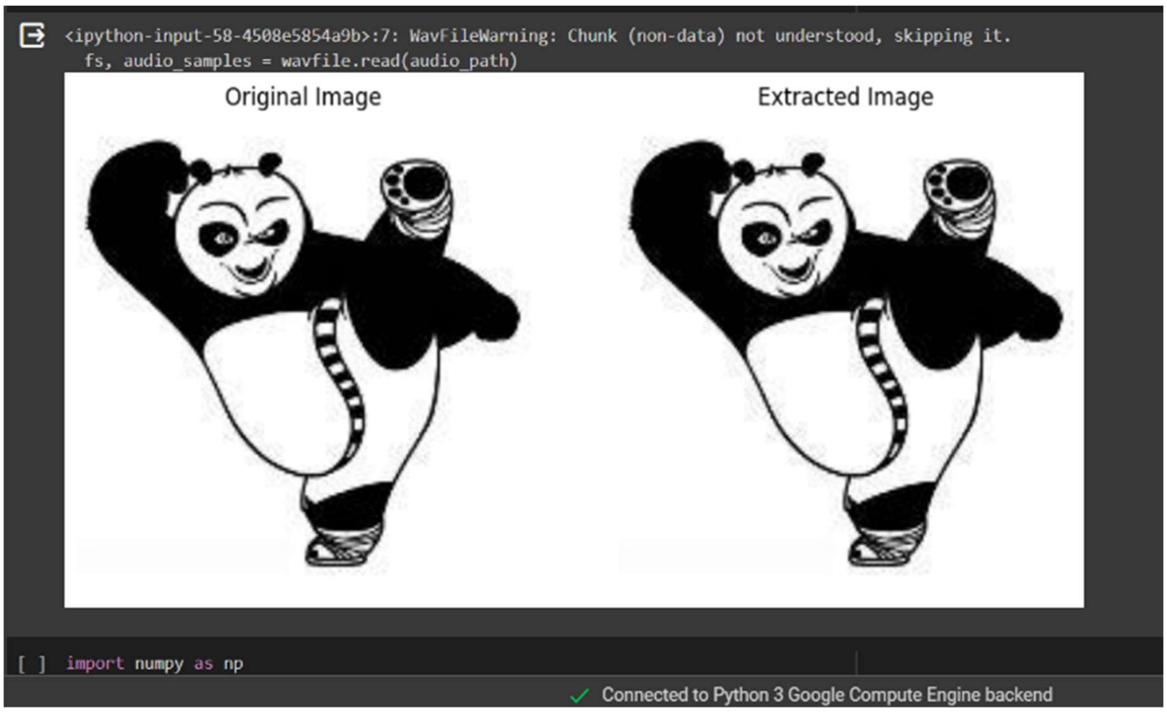
CHAPTER 4

RESULT AND ANALYSIS

This section presents the experimental results obtained by applying our novel steganographic algorithm to two different watermark images: a grayscale image of an athlete and a binary image of a panda. The results are assessed based on various metrics, including Normalized Correlation (NC), Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), Structural Similarity Index Measure (SSIM), and Bit Error Rate (BER). We also analyze the robustness of our algorithm under common signal processing attacks.

4.1 Visual Performance Assessment

To visually demonstrate the effectiveness of our steganographic technique, “Fig 7” and “Fig 8” compare the original images with their corresponding extracted versions after the application of our algorithm.



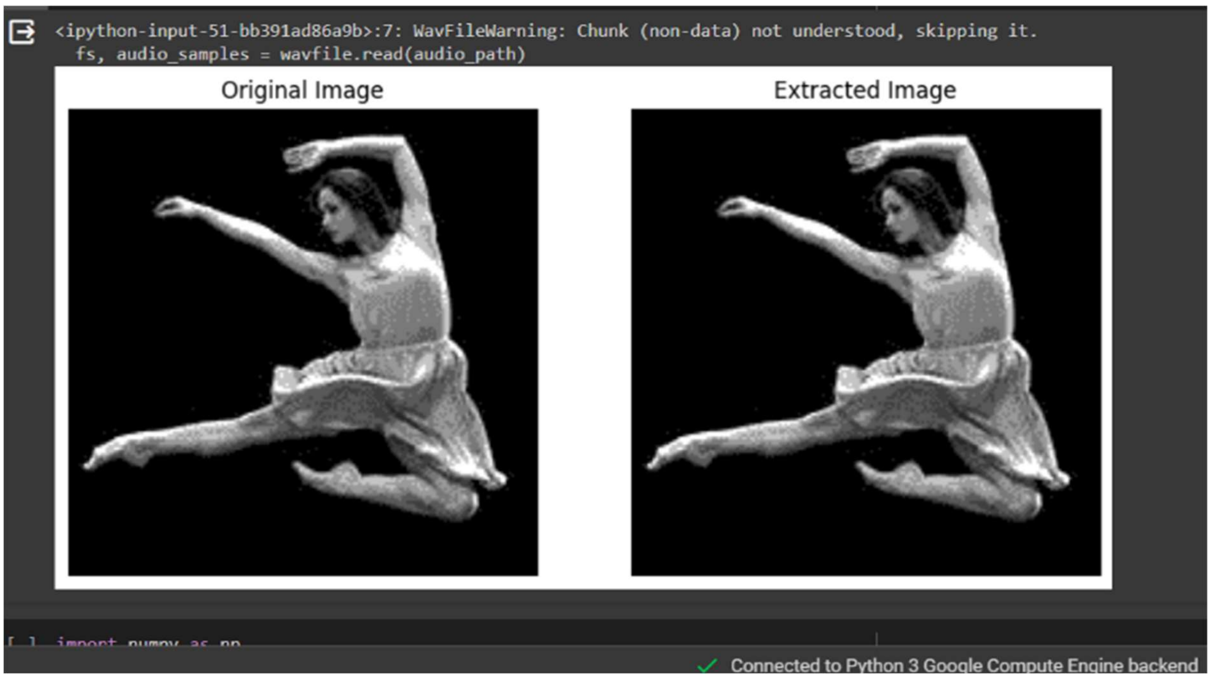
```
<ipython-input-58-4508e5854a9b>:7: WavFileWarning: Chunk (non-data) not understood, skipping it.
  fs, audio_samples = wavfile.read(audio_path)
```

```
[ ]  import numpy as np
```

✓ Connected to Python 3 Google Compute Engine backend

Fig.7 Comparison of Original and Extracted Images for Watermark 1

The left image shows the original binary watermark featuring a popular animated character, while the right image depicts the watermark extracted post-steganography. The extracted image displays remarkable similarity, with no discernible loss in quality, which is also supported by our quantitative metrics.



```
<ipython-input-51-bb391ad86a9b>:7: WavFileWarning: Chunk (non-data) not understood, skipping it.
  fs, audio_samples = wavfile.read(audio_path)
```

```
[ ] import numpy as np
```

Fig.8 Comparison of Original and Extracted image for watermark 2

4.2 Quantitative Metrics Evaluation

The original and extracted images for both the athlete and panda were compared to evaluate the performance of our watermarking algorithm. The extracted images show a high degree of fidelity, as evidenced by the metrics outlined below.

TABLE.2 Performance Metrics for Watermarked Images

Sr. No	**Performance Metrics for Watermarked Images**					
	Watermark image	***NC***	***PSNR***	***MSE***	***SSIM***	***BER***
1.	PANDA	1.00	Inf	0.00	0.997	0.01
2.	Athelete	1.00	Inf	0.00	1.00	0.00

for both images demonstrate that our method can extract watermarks without any loss of information or quality. These results validate the efficacy of the embedding technique, confirming that the watermark remains entirely imperceptible and undistorted, even post-extraction.

4.3 Analysis On Different Attacks

TABLE.3 Robustness against signal processing attacks

Sr. No	Robustness against signal processing attacks		
	Attack type	***Athlete image***	***Panda image***
1.	Low pass filtering	NC: 0.9999	NC: 0.9998
2.	Random noise	NC: 0.9997	NC: 0.9995
3.	Cropping	NC: 0.7580	NC: 0.7580
4.	Resampling	NC: 0.9998	NC: 0.9996

The results indicate a high level of robustness, with the NC values for both images remaining close to 1, even after attacks. This underscores the resilience of the embedding technique, although a slight degradation is observed, particularly with the cropping attack, which presents opportunities for further algorithmic refinement.

4.4 Comparative Analysis

4.4.1 Structure comparison in table form

TABLE.4 Comparative Analysis with Existing Techniques

Sr. No	Comparative Analysis With Existing Techniques					
	Techniques	***Domain***	***Primary techniques***	***Key strength***	***Limitations***	***Ideal Use-case***
1.	Traditional LSB (Least Significant Bit) [56]	Audio / Image	LSB Embedding	Simple to implement, Low computational cost	Vulnerable to lossy compression and noise	Simple covert communications
2.	DCT (Discrete Cosine Transform)[57]	Image	Transform-based Embedding	Resilient to JPEG compression	Susceptible to geometric attacks	Digital media watermarking
3.	DWT (Discrete Wavelet Transform)[58]	Image	Transform-based Embedding	Multi-resolution capabilities, Robust against scaling	Complex, High computational cost	Robust watermarking in multi-media
4.	CNN/RNN (Convolutional/Recurrent Neural Networks)[36]	Image/Audio	Deep Learning-based	High accuracy, Adaptability	Requires large datasets, Intensive training	Secure and adaptive steganography

Sr. No	Comparative Analysis With Existing Techniques					
	Techniques	***Domain***	***Primary techniques***	***Key strength***	***Limitations***	***Ideal Use-case***
5.	SVD (Singular Value Decomposition)[59]	Image	Algebraic manipulation	Robust to common image processing attacks	Computationall y intensive	High-security applications needing robustness
6.	Improve LSB[60]	Image	LSB Embedding with encrypted image	Security	Vulnerable to lossy compression and noise	Used where information is crucial
7.	DCT, Arnold[61]	Image	Transform-based Embedding	Security, Imperceptibility	Secure with Arnold transform	Ownership
8.	**Proposed Algorithm**	**Image /Audio**	**Cryptographic Hashing with LSB**	**High imperceptibility, Low computational overhead, Security, Robustness**	**Vulnerable to cropping, resampling**	**Secure audio communications , DRM systems, Copyright**

4.4.2 Comparison In Narrative Form

- **Traditional LSB Techniques**

  For both graphics and audio, traditional LSB embedding is simple and efficient. However, it is typically less resistant to complex assaults and is readily undermined by straightforward changes like filtering or compression. Its main benefits stem from its ease of use and low processing overhead.

- **Modern Techniques (DCT, DWT, CNN/RNN, SVD)**

  DCT and DWT [5], [7] are appropriate for contexts where typical transformations like scaling and compression are expected because they are both resistant to these kinds of modifications. Because they may include data into the perceptually important parts of the carrier media, they are frequently utilized in digital watermarking applications. CNNs and RNNs [8] bring machine learning to steganography, providing a dynamic method of data embedding that may change according on the properties of the input media. Their great effectiveness is due to their versatility, but it comes at the expense of requiring a large amount of computer power and training data. Strong security at a high computing cost is provided by

SVD, which is employed because of its mathematical resilience in maintaining key data properties even with large changes.

- **Proposed Technique**

  By using cryptographic hashing, the suggested approach improves on classical LSB embedding and greatly boosts embedding security. By using the audio data itself and a secret key, the hashing algorithm establishes the embedding placements, making it impossible for unauthorized parties to detect or modify without sacrificing audio quality. When it comes to secure audio transfers, this technique works especially well since data integrity and imperceptibility are crucial. Outperforming numerous current steganographic techniques, the results show greater imperceptibility and resilience, particularly in maintaining a lower BER and higher SSIM.

4.4 Conclusion And Future Scope

This paper explores a new concept to achieve the process of audio steganography providing enhanced data embedding using secret keys and cryptographic hashing, selectively embedding visual information into the audio files to have high quality and ensure extra protection to it. The proposed method shows perfection in integrity and invisibility outperforming classical metrics in terms of performance, by applying cryptographic concepts our proposed work enhances steganographic process and secure the embedded data from unauthorized access. Our future work variations and applying the method for real practical situation which paves the way for illegal interaction hidden in the invisible world. Applying all the metrics, a null BER, a perfect SSIM, a unity NC, zero MSE, an infinite PSNR and perfect SSIM which guarantees full integrity and invisibility of the embedded information in sense of be identical to original one. Enhance audio quality and reinforced protection against any kind of unauthorized discovery and extraction of information are the induced outcomes by applying this novel technique. Encouraged results from the experiment provide new standard in digital steganography where would encourage more research in method resistance towards audio modifications and applying the technique to practical secure communication area.

REFERENCE

[1] C.-C. Chang, P. Tsai, and C.-C. Lin, “SVD-based digital image watermarking scheme,” *Pattern Recognit. Lett.*, vol. 26, no. 10, pp. 1577–1586, Jul. 2005, doi: 10.1016/j.patrec.2005.01.004.

[2] M. Hamidi, M. E. Haziti, H. Cherifi, and M. E. Hassouni, “Hybrid blind robust image watermarking technique based on DFT-DCT and Arnold transform,” *Multimed. Tools Appl.*, vol. 77, no. 20, pp. 27181–27214, Oct. 2018, doi: 10.1007/s11042-018-5913-9.

[3] A. M. Joshi, S. Gupta, M. Girdhar, P. Agarwal, and R. Sarker, “Combined DWT–DCT-Based Video Watermarking Algorithm Using Arnold Transform Technique,” in *Proceedings of the International Conference on Data Engineering and Communication Technology*, S. C. Satapathy, V. Bhateja, and A. Joshi, Eds., Singapore: Springer, 2017, pp. 455–463. doi: 10.1007/978-981-10-1675-2_45.

[4] S. P. Ambadekar, J. Jain, and J. Khanapuri, “Digital Image Watermarking Through Encryption and DWT for Copyright Protection,” in *Recent Trends in Signal and Image Processing*, S. Bhattacharyya, A. Mukherjee, H. Bhaumik, S. Das, and K. Yoshida, Eds., Singapore: Springer, 2019, pp. 187–195. doi: 10.1007/978-981-10-8863-6_19.

[5] P. Jain and U. Ghanekar, “Robust Watermarking Using DWT and Weighted SVD,” in *2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, Mar. 2018, pp. 302–307. doi: 10.1109/ICECA.2018.8474680.

[6] Z. Zhang, C. Wang, and X. Zhou, “Image watermarking scheme based on Arnold transform and DWT-DCT-SVD,” in *2016 IEEE 13th International Conference on Signal Processing (ICSP)*, Nov. 2016, pp. 805–810. doi: 10.1109/ICSP.2016.7877942.

[7] A. K. Abdulrahman and S. Ozturk, “A novel hybrid DCT and DWT based robust watermarking algorithm for color images,” *Multimed. Tools Appl.*, vol. 78, no. 12, pp. 17027–17049, Jun. 2019, doi: 10.1007/s11042-018-7085-z.

[8] S. Subbarayan and S. K. Ramanathan, “Effective Watermarking of Digital Audio and Image Using Matlab Technique,” in *2009 Second International Conference on Machine Vision*, Dec. 2009, pp. 317–319. doi: 10.1109/ICMV.2009.33.

[9] N. Cvejic and T. Seppanen, “Increasing robustness of LSB audio steganography using a novel embedding method,” in *International Conference on Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004.*, Apr. 2004, pp. 533-537 Vol.2. doi: 10.1109/ITCC.2004.1286709.

[10] H. J. Kim and Y. H. Choi, “A novel echo-hiding scheme with backward and forward kernels,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 885–889, Aug. 2003, doi: 10.1109/TCSVT.2003.815950.

[11] D. Kirovski and H. Malvar, “Spread-spectrum audio watermarking: requirements, applications, and limitations,” in *2001 IEEE Fourth Workshop on Multimedia Signal Processing (Cat. No.01TH8564)*, Oct. 2001, pp. 219–224. doi: 10.1109/MMSP.2001.962737.

[12] M. Saha, M. Kedia, and I. Gupta, “A robust digital watermarking scheme for media files,” Dec. 2007, pp. 1–4. doi: 10.1109/TENCON.2007.4429141.

[13]A. Binny and M. Koilakuntla, “Hiding Secret Information Using LSB Based Audio Steganography,” in *2014 International Conference on Soft Computing and Machine Intelligence*, Sep. 2014, pp. 56–59. doi: 10.1109/ISCMI.2014.24.

[14] S. Manoharan and S. Mitra, “Message recovery enhancements to LSB embedding and echo hiding based on T-Codes,” *2009 IEEE Pac. Rim Conf. Commun. Comput. Signal Process.*, pp. 215–220, Aug. 2009, doi: 10.1109/PACRIM.2009.5291371.

[15] N. Cvejic and T. Seppänen, “Spread spectrum audio watermarking using frequency hopping and attack characterization,” *Signal Process.*, vol. 84, no. 1, pp. 207–213, Jan. 2004, doi: 10.1016/j.sigpro.2003.10.016.

[16] C. C. Islamy, T. Ahmad, and R. M. Ijtihadie, “Reversible data hiding based on histogram and prediction error for sharing secret data,” *Cybersecurity*, vol. 6, no. 1, p. 12, Jun. 2023, doi: 10.1186/s42400-023-00147-y.

[17]X. Wen, X. Ding, J. Li, L. Gao, and H. Sun, “An Audio Watermarking Algorithm Based on Fast Fourier Transform,” in *2009 International Conference on Information Management, Innovation Management and Industrial Engineering*, Dec. 2009, pp. 363–366. doi: 10.1109/ICIII.2009.95.

[18]X.-Y. Wang, P.-P. Niu, and W. Qi, “A new adaptive digital audio watermarking based on support vector machine,” *J. Netw. Comput. Appl.*, vol. 31, no. 4, pp. 735–749, Nov. 2008, doi: 10.1016/j.jnca.2007.10.001.

[19]B. Charmchamras, S. Kaengin, S. Airphaiboon, and M. Sangworasil, “Audio watermarking technique using binary image in wavelet domain,” in *2007 6th International Conference on Information, Communications & Signal Processing*, Dec. 2007, pp. 1–3. doi: 10.1109/ICICS.2007.4449600.

[20]S. Kaengin, S. Airphaiboon, and S. Pathoumvanh, “New technique for embedding watermark image into an audio signal,” *2009 9th Int. Symp. Commun. Inf. Technol.*, pp. 29–32, Sep. 2009, doi: 10.1109/ISCIT.2009.5341291.

[21]L. Xie, J. Zhang, and H. He, “Robust Audio Watermarking Scheme Based on Nonuniform Discrete Fourier Transform,” in *2006 IEEE International Conference on Engineering of Intelligent Systems*, Apr. 2006, pp. 1–5. doi: 10.1109/ICEIS.2006.1703157.

[22]S. Wu, J. Huang, D. Huang, and Y. Q. Shi, “Efficiently Self-Synchronized Audio Watermarking for Assured Audio Data Transmission,” *Broadcast. IEEE Trans. On*, vol. 51, pp. 69–76, Apr. 2005, doi: 10.1109/TBC.2004.838265.

[23]N. Khademi, M. A. Akhaee, S. M. Ahadi, M. Moradi, and A. Kashi, “Audio Watermarking based on Quantization Index Modulation in the Frequency Domain,” *2007 IEEE Int. Conf. Signal Process. Commun.*, pp. 1127–1130, 2007, doi: 10.1109/ICSPC.2007.4728522.

[24]M. Charfeddine, E. Maher, and C. Ben Amar, “A blind audio watermarking scheme based on Neural Network and Psychoacoustic Model with Error correcting code in Wavelet Domain,” Apr. 2008, pp. 1138–1143. doi: 10.1109/ISCCSP.2008.4537396.

[25]R. Zezula and J. Misurec, “Audio Digital Watermarking Algorithm Based on SVD in MCLT Domain,” in *Third International Conference on Systems (icons 2008)*, Apr. 2008, pp. 140–143. doi: 10.1109/ICONS.2008.21.

[26]A. Kaur, M. K. Dutta, K. M. Soni, and N. Taneja, “A secure and high payload digital audio watermarking using features from iris image,” *2014 Int. Conf. Contemp. Comput. Inform. IC3I*, pp. 509–512, Nov.

2014, doi: 10.1109/IC3I.2014.7019714.

[27]A. Kaur, M. K. Dutta, K. M. Soni, and N. Taneja, “A high payload audio watermarking algorithm robust against Mp3 compression,” *2014 Seventh Int. Conf. Contemp. Comput. IC3*, pp. 531–535, Aug. 2014, doi: 10.1109/IC3.2014.6897229.

[28]K. R. Kakkirala, S. R. Chalamala, and G. B. M. Rao, “DWT-SVD based blind audio watermarking scheme for copyright protection,” *2014 Int. Conf. Audio Lang. Image Process.*, pp. 180–183, Jul. 2014, doi: 10.1109/ICALIP.2014.7009782.

[29]G. Suresh, N. V. Lalitha, C. S. Rao, and V. Sailaja, “An efficient and simple Audio Watermarking using DCT-SVD,” *2012 Int. Conf. Devices Circuits Syst. ICDCS*, pp. 177–181, Mar. 2012, doi: 10.1109/ICDCSyst.2012.6188699.

[30]H. T. Hu, S. H. Chen, and L. Y. Hsu, “Incorporation of Perceptually Energy-Compensated QIM into DWT-DCT Based Blind Audio Watermarking,” *2014 Tenth Int. Conf. Intell. Inf. Hiding Multimed. Signal Process.*, pp. 748–752, Aug. 2014, doi: 10.1109/IIH-MSP.2014.191.

[31]P. K. Dhar and T. Shimamura, “An SVD-based audio watermarking using variable embedding strength and exponential-log operations,” in *2013 International Conference on Informatics, Electronics and Vision (ICIEV)*, May 2013, pp. 1–6. doi: 10.1109/ICIEV.2013.6572572.

[32]N. V. Lalitha, G. Suresh, and D. V. Sailaja, “Improved_Audio_Watermarking_Using_DWT-SVD,” vol. 2, no. 6, 2011.

[33]B. Y. Lei, I. Y. Soon, and Z. Li, “Blind and robust audio watermarking scheme based on SVD–DCT,” *Signal Process.*, vol. 91, no. 8, pp. 1973–1984, Aug. 2011, doi: 10.1016/j.sigpro.2011.03.001.

[34]H. Zhao, F. Wang, Z. Chen, and J. Liu, “A Robust Audio Watermarking Algorithm Based on SVD-DWT,” *Elektron. Ir Elektrotechnika*, vol. 20, no. 1, Art. no. 1, Jan. 2014, doi: 10.5755/j01.eee.20.1.3948.

[35]P. K. Dhar and T. Shimamura, “Entropy-based audio watermarking using singular value decomposition and log-polar transformation,” *2013 IEEE 56th Int. Midwest Symp. Circuits Syst. MWSCAS*, pp. 1224–1227, Aug. 2013, doi: 10.1109/MWSCAS.2013.6674875.

[36]M. Bagheri, M. Mohrekesh, N. Karimi, and S. Samavi, *Adaptive Control of Embedding Strength in Image Watermarking using Neural Networks*. 2020.

[37]N. Mangal, M. N. Tiwari, K. Atul, Dwivedi, S. Devendra, and Chauhan, “An Efficient Hybrid Algorithm to Enhance Cloud Data Security with Digital Watermarking Technique,” *Int. Res. J. Comput. Sci.*, vol. 11, pp. 161–166, Apr. 2024, doi: 10.26562/irjcs.2024.v1104.54.

[38]L. Zhuang and M. Jiang, “Multipurpose Digital Watermarking Algorithm Based on Dual-Tree CWT,” in *Sixth International Conference on Intelligent Systems Design and Applications*, Oct. 2006, pp. 316–320. doi: 10.1109/ISDA.2006.253853.

[39]N. M. Makbol, B. E. Khoo, and T. H. Rassem, “Security analyses of false positive problem for the SVD-based hybrid digital image watermarking techniques in the wavelet transform domain,” *Multimed. Tools Appl.*, vol. 77, no. 20, pp. 26845–26879, Oct. 2018, doi: 10.1007/s11042-018-5891-y.

[40]N. R. Zhou, W. M. X. Hou, R. H. Wen, and W. P. Zou, “Imperceptible digital watermarking scheme in multiple transform domains,” *Multimed. Tools Appl.*, vol. 77, no. 23, pp. 30251–30267, Dec. 2018, doi: 10.1007/s11042-018-6128-9.

[41]J. Li, C. Yu, B. B. Gupta, and X. Ren, “Color image watermarking scheme based on quaternion Hadamard transform and Schur decomposition,” *Multimed. Tools Appl.*, vol. 77, no. 4, pp. 4545–4561, Feb. 2018, doi: 10.1007/s11042-017-4452-0.

[42]X. Zhou, H. Zhang, and C. Wang, “A Robust Image Watermarking Technique Based on DWT, APDCBT, and SVD,” *Symmetry*, vol. 10, no. 3, Art. no. 3, Mar. 2018, doi: 10.3390/sym10030077.

[43]M. Ali and C. W. Ahn, “An optimal image watermarking approach through cuckoo search algorithm in wavelet domain,” *Int. J. Syst. Assur. Eng. Manag.*, vol. 9, no. 3, pp. 602–611, Jun. 2018, doi: 10.1007/s13198-014-0288-4.

[44]S. Kamble, V. Maheshkar, S. Agarwal, and V. K. Srivastava, “DWT-SVD BASED ROBUST IMAGE WATERMARKING USING ARNOLD MAP”.

[45]D. G. Savakar and A. Ghuli, “Robust Invisible Digital Image Watermarking Using Hybrid Scheme,” *Arab. J. Sci. Eng.*, vol. 44, no. 4, pp. 3995–4008, Apr. 2019, doi: 10.1007/s13369-019-03751-8.

[46]Y.-P. Chen, T.-Y. Fan, and H.-C. Chao, “WMNet: A Lossless Watermarking Technique Using Deep Learning for Medical Image Authentication,” *Electronics*, vol. 10, no. 8, Art. no. 8, Jan. 2021, doi: 10.3390/electronics10080932.

[47]Y. Liu, M. Guo, J. Zhang, Y. Zhu, and X. Xie, “A Novel Two-stage Separable Deep Learning Framework for Practical Blind Watermarking,” in *Proceedings of the 27th ACM International Conference on Multimedia*, in MM ’19. New York, NY, USA: Association for Computing Machinery, Oct. 2019, pp. 1509–1517. doi: 10.1145/3343031.3351025.

[48]G. Kumar and R. Kumar, “Analysis of Arithmetic and Huffman Compression Techniques by Using DWT-DCT,” *Int. J. Image Graph. Signal Process.*, vol. 13, no. 4, p. 63.

[49]F. Ernawan and M. N. Kabir, “A block-based RDWT-SVD image watermarking method using human visual system characteristics,” *Vis. Comput.*, vol. 36, no. 1, pp. 19–37, Jan. 2020, doi: 10.1007/s00371-018-1567-x.

[50] Z.-M. Ma, L.-Q. Yao, S. Yuan, and H.-Z. Zhang, “Entropic Conditional Central Limit Theorem and Hadamard Compression.” arXiv, Jan. 20, 2024. Accessed: May 17, 2024. [Online]. Available: http://arxiv.org/abs/2401.11383

[51]N. Saxena, K. K. Mishra, and A. Tripathi, “DWT-SVD-Based Color Image Watermarking Using Dynamic-PSO,” in *Advances in Computer and Computational Sciences*, S. K. Bhatia, K. K. Mishra, S. Tiwari, and V. K. Singh, Eds., Singapore: Springer, 2018, pp. 343–351. doi: 10.1007/978-981-10-3773-3_34.

[52]S. Malik and R. R. Kishore, “Fractional Fourier Transform and Position shuffling Based Digital Image Watermarking Scheme and Its Performance Analysis.” Rochester, NY, 2018. Accessed: May 16, 2024. [Online]. Available: https://papers.ssrn.com/abstract=3330016

[53]D. Li, L. Deng, B. Bhooshan Gupta, H. Wang, and C. Choi, “A novel CNN based security guaranteed image watermarking generation scenario for smart city applications,” *Inf. Sci.*, vol. 479, pp. 432–447, Apr. 2019, doi: 10.1016/j.ins.2018.02.060.

[54]Z. Wang, Z. S. Hussein, and X. Wang, “Secure compressive sensing of images based on combined chaotic DWT sparse basis and chaotic DCT measurement matrix,” *Opt. Lasers Eng.*, vol. 134, p. 106246, Nov. 2020, doi: 10.1016/j.optlaseng.2020.106246.

[55]W. Chen, M. J. Er, and S. Wu, “PCA and LDA in DCT domain,” *Pattern Recognit. Lett.*, vol. 26, no. 15, pp. 2474–2482, Nov. 2005, doi: 10.1016/j.patrec.2005.05.004.

[56]N. Cvejic, “Algorithms for audio watermarking and steganography,” jultika.oulu.fi. Accessed: May 16, 2024. [Online]. Available: https://oulurepo.oulu.fi/handle/10024/37393

[57]J. R. Aparna and S. Ayyappan, “Comparison of digital watermarking techniques,” in *International Conference for Convergence for Technology-2014*, Apr. 2014, pp. 1–6. doi: 10.1109/I2CT.2014.7092189.

[58]A. R. Elshazly, M. M. Fouad, and M. E. Nasr, “Secure and robust high quality DWT domain audio watermarking algorithm with binary image,” in *2012 Seventh International Conference on Computer Engineering & Systems (ICCES)*, Nov. 2012, pp. 207–212. doi: 10.1109/ICCES.2012.6408514.

[59]V. Bhat K, I. Sengupta, and A. Das, “An adaptive audio watermarking based on the singular value decomposition in the wavelet domain,” *Digit. Signal Process.*, vol. 20, no. 6, pp. 1547–1558, Dec. 2010, doi: 10.1016/j.dsp.2010.02.006.

[60]D. Hmood, K. Abbas, and M. Altaei, “A New Steganographic Method for Embedded Image In Audio File,” *Int. J. Comput. Sci. Secur.*, vol. 6, p. 135, Apr. 2012.

[61]M. Hamidi, M. E. Haziti, H. Cherifi, and M. E. Hassouni, “Hybrid blind robust image watermarking technique based on DFT-DCT and Arnold transform,” *Multimed. Tools Appl.*, vol. 77, no. 20, pp. 27181–27214, Oct. 2018, doi: 10.1007/s11042-018-5913-9.

PAPER NAME

29Final_Thesis_work _Raghwendra.pdf

WORD COUNT

11555 Words

CHARACTER COUNT

64389 Characters

PAGE COUNT

48 Pages

FILE SIZE

1.6MB

SUBMISSION DATE

May 29, 2024 8:58 PM GMT+5:30

REPORT DATE

May 29, 2024 8:59 PM GMT+5:30

● 10% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

- 7% Internet database
- Crossref database
- 7% Publications database
- Crossref Posted Content database

● Excluded from Similarity Report

- Submitted Works database
- Quoted material
- Small Matches (Less then 10 words)
- Bibliographic material
- Cited material

29Final_Thesis_work _Raghwendra.pdf

My Files

My Files

Delhi Technological University

Document Details

Submission ID

trn:oid:::27535:60273669

Submission Date

May 29, 2024, 8:58 PM GMT+5:30

Download Date

May 29, 2024, 9:03 PM GMT+5:30

File Name

29Final_Thesis_work _Raghwendra.pdf

File Size

1.6 MB

48 Pages

11,555 Words

64,389 Characters

How much of this submission has been generated by AI?

0%

of qualifying text in this submission has been determined to be generated by AI.

Caution: Percentage may not indicate academic misconduct. Review required.

It is essential to understand the limitations of AI detection before making decisions about a student's work. We encourage you to learn more about Turnitin's AI detection capabilities before using the tool.

Frequently Asked Questions

What does the percentage mean?
The percentage shown in the AI writing detection indicator and in the AI writing report is the amount of qualifying text within the submission that Turnitin's AI writing detection model determines was generated by AI.

Our testing has found that there is a higher incidence of false positives when the percentage is less than 20. In order to reduce the likelihood of misinterpretation, the AI indicator will display an asterisk for percentages less than 20 to call attention to the fact that the score is less reliable.

However, the final decision on whether any misconduct has occurred rests with the reviewer/instructor. They should use the percentage as a means to start a formative conversation with their student and/or use it to examine the submitted assignment in greater detail according to their school's policies.

How does Turnitin's indicator address false positives?
Our model only processes qualifying text in the form of long-form writing. Long-form writing means individual sentences contained in paragraphs that make up a longer piece of written work, such as an essay, a dissertation, or an article, etc. Qualifying text that has been determined to be AI-generated will be highlighted blue on the submission text.

Non-qualifying text, such as bullet points, annotated bibliographies, etc., will not be processed and can create disparity between the submission highlights and the percentage shown.

What does 'qualifying text' mean?
Sometimes false positives (incorrectly flagging human-written text as AI-generated), can include lists without a lot of structural variation, text that literally repeats itself, or text that has been paraphrased without developing new ideas. If our indicator shows a higher amount of AI writing in such text, we advise you to take that into consideration when looking at the percentage indicated.

In a longer document with a mix of authentic writing and AI generated text, it can be difficult to exactly determine where the AI writing begins and original writing ends, but our model should give you a reliable guide to start conversations with the submitting student.

Disclaimer
Our AI writing assessment is designed to help educators identify text that might be prepared by a generative AI tool. Our AI writing assessment may not always be accurate (it may misidentify both human and AI-generated text) so it should not be used as the sole basis for adverse actions against a student. It takes further scrutiny and human judgment in conjunction with an organization's application of its specific academic policies to determine whether any academic misconduct has occurred.

Gmail **RAGHWENDRA SINGH <raghwendrapratapsingh01@gmail.com>**

Acceptance Notification 1st IEEE ICAC2N-2024 & Registration: Paper ID 694 @ ITS Engineering College, Greater Noida

1 message

Microsoft CMT <email@msr-cmt.org> Mon, May 13, 2024 at 10:13 PM
Reply-To: "Dr. Vishnu Sharma" <vishnu.sharma@its.edu.in>
To: RAGHWENDRA PRATAP SINGH <raghwendrapratapsingh01@gmail.com>

Dear RAGHWENDRA PRATAP SINGH,
Delhi technological university ,DTU

Greetings from ICAC2N-2024 ...!!!

Congratulations....!!!!!

On behalf of the ICAC2N-2024 organising Committee, we are delighted to inform you that the submission of “Paper ID- 694 “ titled “ Enhancing Audio Steganography: Advancing Audio Steganography with Cryptographic Hashing “ has been accepted for presentation and further publication with IEEE at the ICAC2N- 24. All accepted papers will be submitted for inclusion into IEEE Xplore subject to meeting IEEE Xplore’s scope and quality requirements.

Registration/Fee Payment related details are available at https://icac2n.in/register.

For early registration benefit please pay your fee and complete your registration by clicking on the following Link: https://forms.gle/E7RuvuQQPxPZQnJU6 by 20 May 2024.

You are directed to ensure incorporating following points in your paper while completing your registration:

Comments:
The topic chosen "Enhancing Audio Steganography: Advancing Audio Steganography with Cryptographic Hashing" is interesting and relevant.
Formatting of paper is not proper. Paper must be strictly in IEEE template.
Abstract must be clear and precise.
Add a comparison table with the similar work carried out in this field with latest references.
Conclusion and result section must be more descriptive.
All references must be properly cited in content and should be in proper format.

Note:
1. All figures and equations in the paper must be clear.
2. Final camera ready copy must be strictly in IEEE format available on conference website.
3. Transfer of E-copyright to IEEE and Presenting paper in conference is compulsory for publication of paper in IEEE.
4. If plagiarism is found at any stage in your accepted paper, the registration will be cancelled and paper will be rejected and the authors will be responsible for any consequences. Plagiarism must be less then 15% (checked through Turnitin).
5. Change in paper title, name of authors or affiliation of authors will not be allowed after registration of papers.
6. Violation of any of the above point may lead to rejection of your paper at any stage of publication.
7. Registration fee once paid will be non refundable.

If you have any query regarding registration process or face any problem in making online payment, write us at icac2n.ieee@gmail.com.

Regards:
Organizing committee
ICAC2N – 2024

To stop receiving conference emails, you can check the 'Do not send me conference email' box from your User Profile.

Microsoft respects your privacy. To learn more, please read our Privacy Statement.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Gmail **RAGHWENDRA SINGH <raghwendrapratapsingh01@gmail.com>**

Registration Confirmation 1st IEEE ICAC2N-2024 : Paper ID 694 @ ITS Engineering College, Greater Noida

1 message

Microsoft CMT <email@msr-cmt.org> Wed, May 22, 2024 at 12:16 AM
Reply-To: "Dr. Vishnu Sharma" <vishnu.sharma@its.edu.in>
To: RAGHWENDRA PRATAP SINGH <raghwendrapratapsingh01@gmail.com>

Dear RAGHWENDRA PRATAP SINGH,
Delhi technological university ,DTU

Greetings from ICAC2N-2024 ...!!! Thanks for Completing your registration...!!

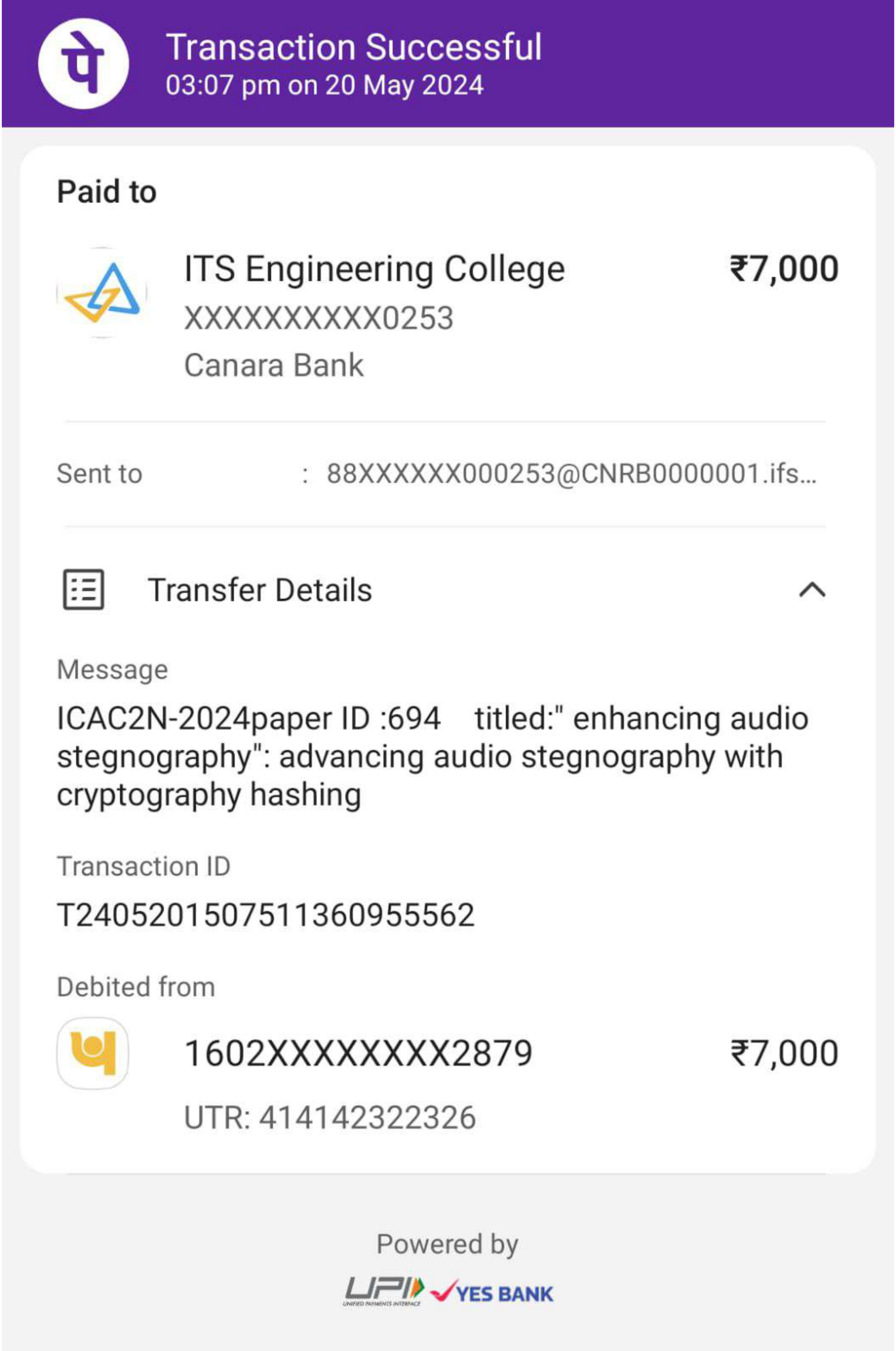
Paper ID- "694 “
Paper Title- “ Enhancing Audio Steganography: Advancing Audio Steganography with Cryptographic Hashing “

This email is to confirm that you have successfully completed your registration for your accepted paper at ICAC2N-2024. We have received your registration and payment details. Further, your submitted documents will be checked minutely and if any action will be required at your end you will be informed separately via email.

For further updated regarding conference please keep visiting conference website www.icac2n.in or write us at icac2n.ieee@gmail.com.

Regards:
Organizing committee
ICAC2N – 2024

Note:
1. Transfer of E-copyright to IEEE and Presenting paper in conference is compulsory for publication of paper in IEEE. (For this you will be informed separately via email well before conference)
2. If plagiarism is found at any stage in your accepted paper, the registration will be cancelled and paper will be rejected and the authors will be responsible for any consequences. Plagiarism must be less then 15% (checked through Turnitin).
3. Change in paper title, name of authors or affiliation of authors is not allowed now.
4. Violation of any of the above point may lead to cancellation of registration.
5. Registration fee once paid is non-refundable.



Transaction Successful

03:07 pm on 20 May 2024

Paid to

ITS Engineering College ₹7,000

XXXXXXXXXX0253

Canara Bank

Sent to : 88XXXXXX000253@CNRB0000001.ifs...

Transfer Details

Message

ICAC2N-2024paper ID :694 titled:" enhancing audio stegnography": advancing audio stegnography with cryptography hashing

Transaction ID

T2405201507511360955562

Debited from

1602XXXXXXXX2879 ₹7,000

UTR: 414142322326

Powered by

PAPER NAME

Paper ID- 694.pdf

WORD COUNT

2883 Words

CHARACTER COUNT

16293 Characters

PAGE COUNT

5 Pages

FILE SIZE

1.0MB

SUBMISSION DATE

May 22, 2024 9:48 AM GMT+5:30

REPORT DATE

May 22, 2024 9:49 AM GMT+5:30

4% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

- 4% Internet database
- Crossref database
- 3% Submitted Works database
- 3% Publications database
- Crossref Posted Content database

Excluded from Similarity Report

- Bibliographic material

Gmail **RAGHWENDRA SINGH <raghwendrapratapsingh01@gmail.com>**

Acceptance Notification 1st IEEE ICAC2N-2024 & Registration: Paper ID 627 @ ITS Engineering College, Greater Noida

1 message

Microsoft CMT <email@msr-cmt.org> Mon, May 13, 2024 at 10:13 PM
Reply-To: "Dr. Vishnu Sharma" <vishnu.sharma@its.edu.in>
To: RAGHWENDRA PRATAP SINGH <raghwendrapratapsingh01@gmail.com>

Dear RAGHWENDRA PRATAP SINGH,
Delhi technological university ,DTU

Greetings from ICAC2N-2024 ...!!!

Congratulations....!!!!!

On behalf of the ICAC2N-2024 organising Committee, we are delighted to inform you that the submission of "Paper ID- 627 " titled " Inaudible Identity: An Exhaustive Survey of Digital Audio Watermarking Methods for Secure Applications " has been accepted for presentation and further publication with IEEE at the ICAC2N- 24. All accepted papers will be submitted for inclusion into IEEE Xplore subject to meeting IEEE Xplore's scope and quality requirements.

Registration/Fee Payment related details are available at https://icac2n.in/register.

For early registration benefit please pay your fee and complete your registration by clicking on the following Link: https://forms.gle/E7RuvuQQPxPZQnJU6 by 20 May 2024.

You are directed to ensure incorporating following points in your paper while completing your registration:

Comments:
The topic chosen "Inaudible Identity: An Exhaustive Survey of Digital Audio Watermarking Methods for Secure Applications" is interesting and relevant.
Formatting of paper is not proper. Paper must be strictly in IEEE template.
Abstract must be clear and precise.
Add a comparison table with the similar work carried out in this field with latest references.
Conclusion and result section must be more descriptive.
All references must be properly cited in content and should be in proper format.

Note:
1. All figures and equations in the paper must be clear.
2. Final camera ready copy must be strictly in IEEE format available on conference website.
3. Transfer of E-copyright to IEEE and Presenting paper in conference is compulsory for publication of paper in IEEE.
4. If plagiarism is found at any stage in your accepted paper, the registration will be cancelled and paper will be rejected and the authors will be responsible for any consequences. Plagiarism must be less then 15% (checked through Turnitin).
5. Change in paper title, name of authors or affiliation of authors will not be allowed after registration of papers.
6. Violation of any of the above point may lead to rejection of your paper at any stage of publication.
7. Registration fee once paid will be non refundable.

If you have any query regarding registration process or face any problem in making online payment, write us at icac2n.ieee@gmail.com.

Regards:
Organizing committee
ICAC2N – 2024

Gmail

RAGHWENDRA SINGH <raghwendrapratapsingh01@gmail.com>

Registration Confirmation 1st IEEE ICAC2N-2024 : Paper ID 627 @ ITS Engineering College, Greater Noida

1 message

Microsoft CMT <email@msr-cmt.org> Wed, May 22, 2024 at 12:16 AM
Reply-To: "Dr. Vishnu Sharma" <vishnu.sharma@its.edu.in>
To: RAGHWENDRA PRATAP SINGH <raghwendrapratapsingh01@gmail.com>

Dear RAGHWENDRA PRATAP SINGH,
Delhi technological university ,DTU

Greetings from ICAC2N-2024 ...!!! Thanks for Completing your registration...!!

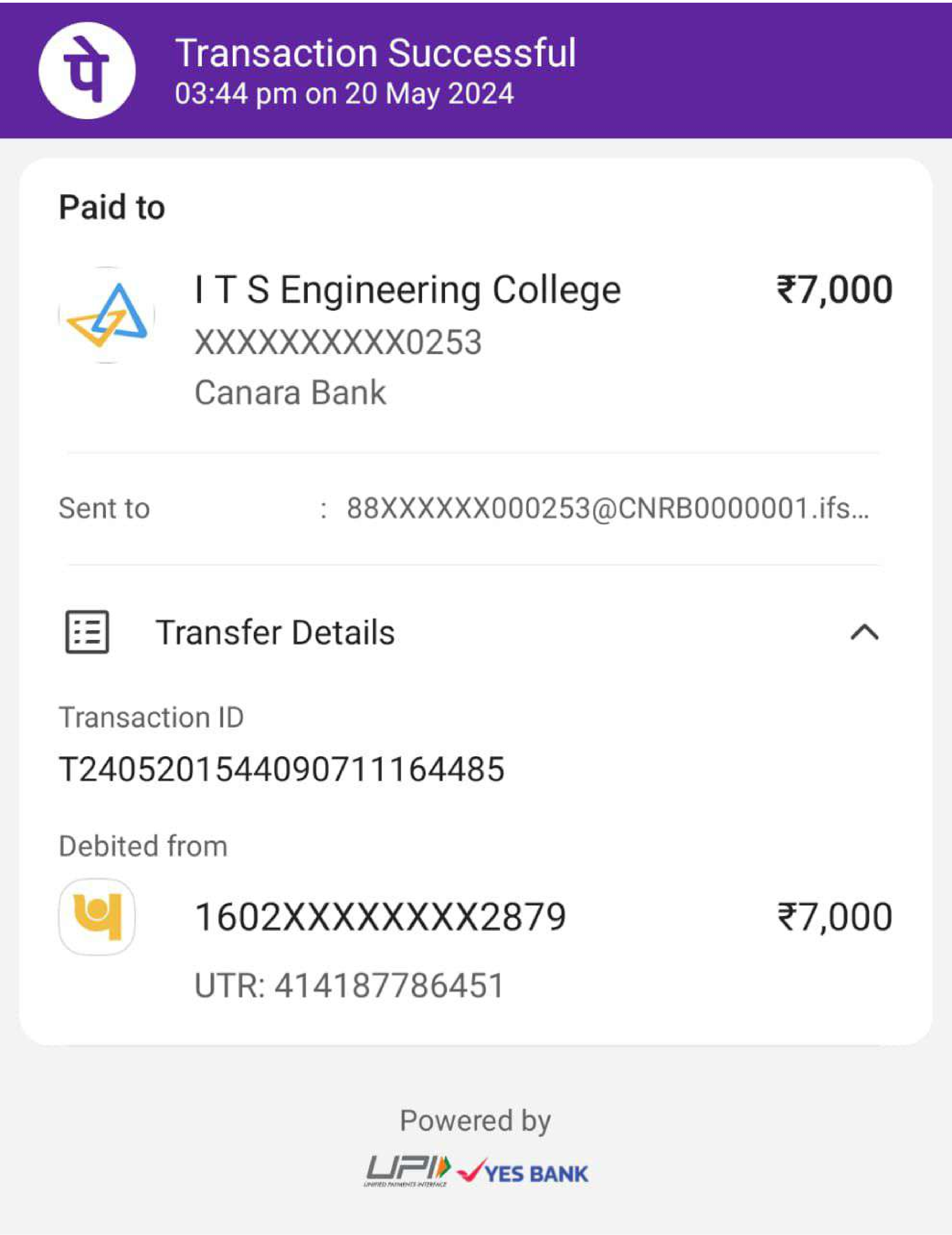
Paper ID- "627 “
Paper Title- “ Inaudible Identity: An Exhaustive Survey of Digital Audio Watermarking Methods for Secure Applications “

This email is to confirm that you have successfully completed your registration for your accepted paper at ICAC2N-2024. We have received your registration and payment details. Further, your submitted documents will be checked minutely and if any action will be required at your end you will be informed separately via email.

For further updated regarding conference please keep visiting conference website www.icac2n.in or write us at icac2n.ieee@gmail.com.

Regards:
Organizing committee
ICAC2N – 2024

Note:
1. Transfer of E-copyright to IEEE and Presenting paper in conference is compulsory for publication of paper in IEEE. (For this you will be informed separately via email well before conference)
2. If plagiarism is found at any stage in your accepted paper, the registration will be cancelled and paper will be rejected and the authors will be responsible for any consequences. Plagiarism must be less then 15% (checked through Turnitin).
3. Change in paper title, name of authors or affiliation of authors is not allowed now.
4. Violation of any of the above point may lead to cancellation of registration.
5. Registration fee once paid is non-refundable.



Transaction Successful

03:44 pm on 20 May 2024

Paid to

I T S Engineering College XXXXXXXXXX0253 Canara Bank	₹7,000

Sent to : 88XXXXXX000253@CNRB0000001.ifs...

Transfer Details

Transaction ID

T2405201544090711164485

Debited from

1602XXXXXXXX2879 UTR: 414187786451	₹7,000

Powered by

UPI YES BANK

Similarity Report

PAPER NAME

Paper ID- 627.pdf

WORD COUNT

4390 Words

CHARACTER COUNT

25144 Characters

PAGE COUNT

7 Pages

FILE SIZE

823.8KB

SUBMISSION DATE

May 28, 2024 12:53 PM GMT+5:30

REPORT DATE

May 28, 2024 12:54 PM GMT+5:30

● 11% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

- 3% Internet database
- Crossref database
- 4% Submitted Works database
- 9% Publications database
- Crossref Posted Content database

● Excluded from Similarity Report

- Bibliographic material
- Small Matches (Less then 10 words)