

**School of Electronics Engineering**

DIGITAL SIGNAL PROCESSING – FINAL REPORT

**REPORT TITLE**

**WATERMARKING AN IMAGE INTO AN AUDIO FILE**

**USING LEAST SIGNIFICANT BIT METHOD**

**Registration Number Name**

17BEC0524 Anshul Goyal

17BEC Sabasachi

**Under the guidance of:**

Prof. Prakasam P

**ACKNOWLEDGEMENT**

We would like to take this opportunity to thank all the people who have helped in completion of this project. Their constant support and guidance enabled me to complete my project. We would like to show my greatest gratitude towards Prof. Prakasam P for helping us during this project.

**Abstract**

In recent times it has grown to be important to protect the digital media content like audio, video, images from getting illegally copied and distributed without copyright owner’s knowledge. It has been observed that the digital media are hacked and its copyright is being misused to their own, even if it is the work of others. To protect from this malicious use, we are proposing the digital audio watermarking content. . In our proposed work we aim at embedding a unique image file called watermark into and audio file. Multiple copies of copyrighted material are produced with a unique watermark which can be extracted from the file and matched with the original file to backtrack the person responsible for leaking the file. The technique used in this project is least significant bit technique which makes minimal changes to original content but still watermarks very effectively.

**Introduction**

Illegal copying, modifying, tampering and copyright protection have become very important issues with the rapid use of internet. Hence, there is a strong need of developing the techniques to face all these problems. Digital watermarking emerged as a solution for protecting the multimedia data. Digital Watermarking is the process of hiding or embedding an imperceptible signal (data) into the given signal (data). This imperceptible signal (data) is called watermark or metadata and the given signal (data) is called cover work. The watermark should be embedded into the cover work, so that it should be robust enough to survive not only the most common signal distortions, but also distortions caused by malicious attacks. This cover work can be an image, audio or a video file. A watermarking algorithm consists of two algorithms, an embedding and an extraction (or detection) algorithm. The idea of watermarking first appeared hundreds of years ago. Watermarking technology was used to mark information authenticity by many different means. Watermarking technology has been used in computer as well. Most of the work on computer watermarking technology was for embedding a watermark into images, audio, and video files. Media watermarking research is a very active area and digital image watermarking became an interesting protection measure and got the attention of many researchers since the early 1990s. The extraction procedure allows us to extract the content but the file is being still protected. There are about some properties that satisfy the need for effective watermarking applications. These are

**Inaudible**- The digital watermark is embedded into audio data as it should not be audible to human ear. Security- A system is believed to be protected if the cracker cannot take away the watermark applied without having the knowledge of embedded algorithm, detector and composition of watermark. Only the authorized users can access it.

**Verifiability**- It can be used to check the object is protected i.e. copyright-protected and identify the authenticity and control of illegal copying

**Robustness**- It is the capability to deal with the copyright information of digital works; the embedded watermark can refuse to accept the common editing process, processing the image and lossy compression. Also after attacks the watermark cannot be damaged and can be still detected to offer certification. For example, filtering, noise, compression, cropping, A/D-D/A conversions, geometrical or non-geometrical attacks etc.

**Fragile**- Fragile watermarking is used for mainly integrity protection which is very sensitive to the changes of the signal. We can determine tampered data in accordance with the state of fragile watermarking. Semi fragile- It is proficient in managing changes made to watermarked image such as addition of lossy compression (i.e. noise).

**Constant** **Bit**-**rate**- The amount of watermark data may be securely embedded within the host signal per unit space or time. For solving the data security, the watermarking techniques are introduced to provide security of information. In recent years the watermarking techniques have been introduced to focus on images and video clips but audio watermarking is more complicated that video and image watermarking.

**Theory**

**Algorithms**

***Embedding Algorithm***

* Step 1: Read the audio file you want to use for embedding.
* Step 2: Read the message image you want to hide in the audio signal.
* Step 3: Conversion of message image into double.
* Step 4: Rounding of values after operation (message/256).
* Step 5: Conversion into uint8 values.
* Step 6: Determine the size of audio signal used for embedding.
* Step 7: Determine the size of message object to embed.
* Step 8: Set the MSB or 8st bit of cover object (ii,jj) to the value of the MSB of watermark (ii,jj).
* Step 9: Write to file the two images.
* Step 10: Display watermarked image.

***Extraction Algorithm***

* Step 1: Read the watermarked audio signal to be used for recovering.
* Step 2: Determining size of audio signal.
* Step 3: Use the LSB of audio signal to recover watermark.
* Step 4: Scaling the recovered watermark by converting the image into double.
* Step 5: Scaling and displaying the recovered image.

***Code***

Embedding code:

function watermarkThis(n)

[host, f] = audioread ('host.wav') ;

host = uint8(255\*(host + 0.5));

watermark="watermark"+n+".png";

wm = imread(char(watermark));

[r, c] = size(wm) ;

wm\_l = length(wm(:))\*8 ;

if length(host) < (length(wm(:))\*8)

disp('your image pixel is not enough')

else

host\_bin = dec2bin(host, 8);

wm\_bin = dec2bin(wm(:), 8);

wm\_str = zeros(wm\_l, 1);

for j = 1:8

for i = 1:length(wm(:))

ind = (j-1)\*length(wm(:)) + i;

wm\_str(ind, 1) = str2double(wm\_bin(i, j));

end

end

for i = 1:wm\_l

host\_bin(i, 8) = dec2bin(wm\_str(i));

end

host\_new = bin2dec(host\_bin);

host\_new = (double(host\_new)/255 - 0.5);

OutputName="SongFile"+n+".wav";

audiowrite(char(OutputName), host\_new, f)

end

Extraction code:

function position=extractThis(file,n)

wm\_sz = 20000;

px\_sz = wm\_sz/8;

im\_sz = sqrt(px\_sz);

SearchFile=file+".wav";

host\_new = audioread (char(SearchFile));

host\_new = uint8(255\*(host\_new + 0.5));

host\_bin = dec2bin(host\_new, 8);

wm\_bin\_str = host\_bin(1:wm\_sz, 8);

wm\_bin = reshape(wm\_bin\_str, px\_sz , 8);

wm\_str = zeros(px\_sz, 1, 'uint8');

for i = 1:px\_sz

wm\_str(i, :) = bin2dec(wm\_bin(i, :));

end

wm = reshape(wm\_str, im\_sz , im\_sz);

for i=1:n

watermark="watermark"+i+".png";

ref= imread(char(watermark));

ref=rgb2gray(ref);

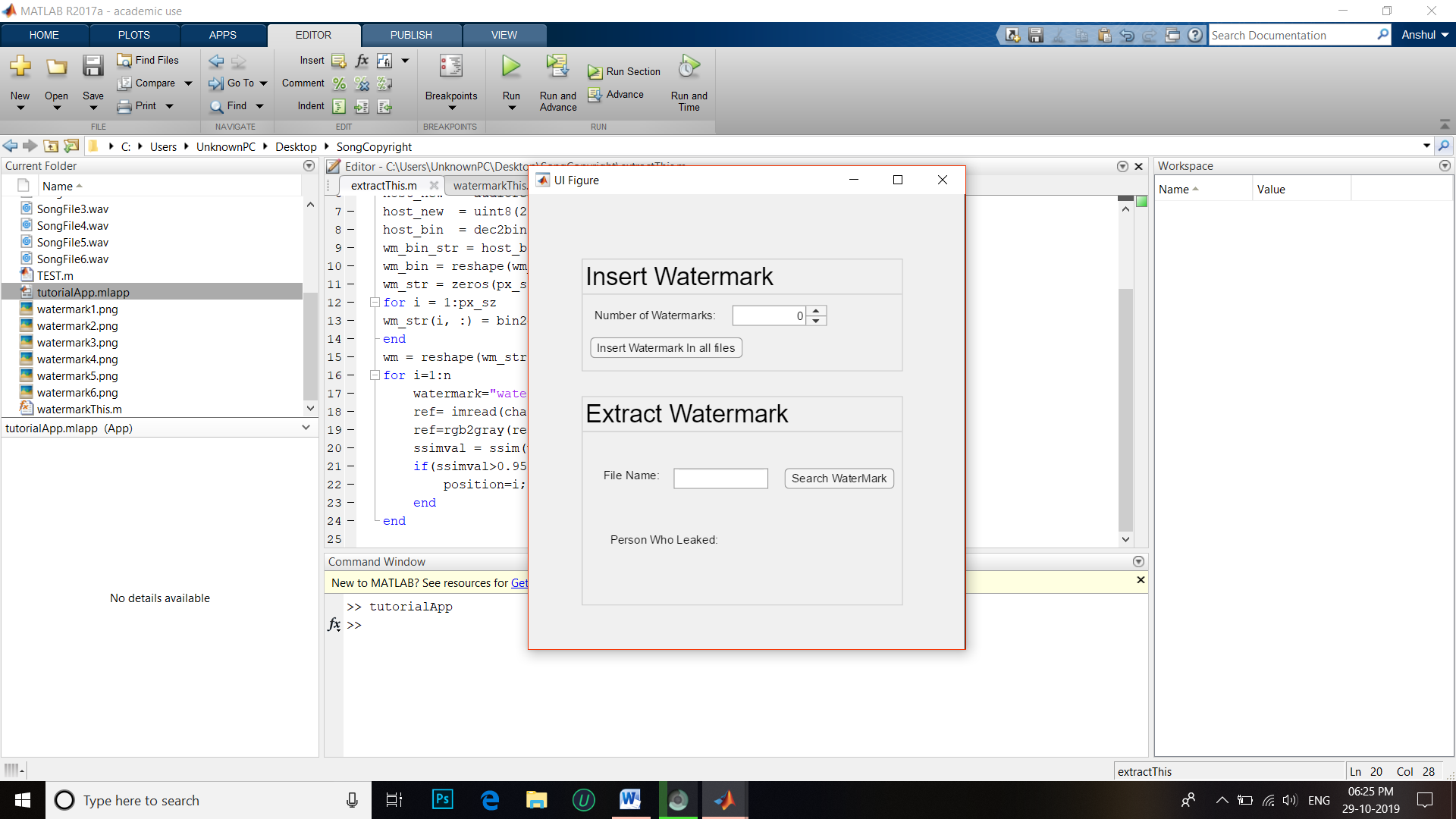
ssimval = ssim(wm,ref);

if(ssimval>0.95)

position=i;

end

end



**CONCLUSION**

In the proposed method the digital audio watermarking is given high security using the LSB and DCT technique which protects form the attacks of the unauthorized users. We have used two procedures for watermarking one is embedded watermarking and extraction watermarking. The Results obtained are compared with previous system. Future work will focus to find the possibility of organizing still more security and improving the results.