DAYANANDA SAGAR UNIVERSITY
DEPT. OF COMPUTER SCIENCE AND ENGINEERING
SOFTWARE REQUIREMENT SPECIFICATION
TOPIC:BIOMETRIC SIGNATURE FOR IMAGE AUTHENTICATION

5TH SEMESTER - 3RD YEAR
MINOR PROJECT

TEAM MEMBERS:
MUSKAAN GOEL(ENG18CS0177)
LYSETTI LAKSHMI POOJITHA(ENG18CS0150)
MEGHANA SHREE M(ENG18CS0165)
MUSKAAN SINHA(ENG18CS0178)

GUIDE: PROF. BHARGAVI MOKASHI
(DEPT. OF COMPUTER SCIENCE AND ENGINEERING)

DAYANANDA SAGAR UNIVERSITY

CERTIFICATE

This is to certify that the Mini project report entitled "_____" being submitted by_____ to Department of Computer Science and Engineering , Dayananda Sagar University, Bangalore, for the 5th Semester B.Tech C.S.E. of this University during the academic year 2020-2021.

Date: _____ _____

Signature of the Faculty Incharge

_____

Signature of the Chairman

Declaration

We **Lysetti Lakshmi Poojitha [ENG18CS0150], Meghana Sree [ENG18CS0165], Muskaan Goel [ENG18CS0177],Muskaan Sinha [ENG18CS0178]** students of 5th semester B.Tech in Computer Science and Engineering, Dayananda Sagar University, Bengaluru, hereby declare that titled''**BIOMETRIC SIGNATURE FOR IMAGE AUTHENTICATION**" submitted to the Dayananda Sagar University during the academic year 2020- 2021, is a record of an original work done by me under the guidance of Dr.Viraj kumar, Associate professor, Department of computer science engineering, Dayananda Sagar University, Bengaluru. This project work is submitted in partial fulfilment for the award of the degree of Bachelor of Technology in Computer Science. The result embodied in this thesis has not been submitted to any other university or institute for the award of any degree.

TEAM MEMBERS
MUSKAAN GOEL(ENG18CS0177)
LYSETTI LAKSHMI POOJITHA(ENG18CS0150)
MEGHANA SHREE M(ENG18CS0165)
MUSKAAN SINHA(ENG18CS0178)

Acknowledgement

We are pleased to acknowledge Dr. Viraj Kumar, Department of Computer Science & Engineering for his invaluable guidance, support, motivation and patience during the course of this mini- project work.

We extend our sincere thanks to Dr. SANJAY CHITTNIS , Chairman, Department of Computer Science & Engineering who continuously helped us throughout the project and without his guidance, this project would have been an uphill task.

We have received a great deal of guidance and co-operation from our friends and we wish to thank one and all that have directly or indirectly helped us in the successful completion of this mini-project work.

TEAM MEMBERS
MUSKAAN GOEL(ENG18CS0177)
LYSETTI LAKSHMI POOJITHA(ENG18CS0150)
MEGHANA SHREE M(ENG18CS0165)
MUSKAAN SINHA(ENG18CS0178)

Abstract

In a modern, civilized and advanced society, reliable authentication and authorization of individuals are becoming more essential tasks in several aspects of daily activities and as well as many different important applications such as in financial transactions, access control, travel and immigration, healthcare etc. In some situations, when individual equipment is required for confirmation of one's identity to other groups of people in order to make use of services or to achieve access to physical places, it is always necessary to declare self-identity and to prove the claim. Traditional authentication methods, which are based on knowledge (password-based authentication) or the utility of a token (photo ID cards, magnetic strip cards and key-based authentication), are less reliable because of loss, forgetfulness and theft. These issues direct substantial attention towards biometrics as an alternative method for person authentication and identification.

The word 'biometric' has been derived from the Greek words "Bio-metriks", "Bio" which means life and "metriks"which means measures. Therefore a biometric is the measurement and statistical analysis of unchanging biological characteristics. Biometrics evaluate a person's unique physical or behavioural traits to authenticate their identity. As biometric identifiers are unique to persons, they are more reliable in verifying identity than token-based and knowledge-based methods. In the last few years, substantial efforts have been devoted to the development of biometric-based authentication systems.

Biometrics provide an expected and successful solution to the authentication problem, as it offers the construction of systems that can identify individuals by the analysis of their physiological or behavioural characteristics . In fact, the field of biometrics is the science of using digital technologies and the intention of biometric systems is to perform the recognition or authentication of people based on some biological characteristics that are intrinsically unique for each individual. The effectiveness of a biometric system is measured mainly by the distinguishing attributes that are used to verify the identity. A large number of biometric traits have been investigated and some of them are nowadays used in several applications. Common physical traits include fingerprints, ear, hand or palm geometry, vein, retina, iris and facial characteristics. Behavioural traits include voice, signature, keystroke pattern and gait.

Table of Contents

Table of Figures

1. INTRODUCTION

Biometric systems are playing a key role in the multitude of applications and placed at the center of debate in the scientific research community. Among the numerous biometric systems, handwritten signature verification has got keen interest over the last three decades. Handwritten signature verification is the behavioral bio- metric system that discriminates the genuine signature from the pre-stored known signatures. It has been researched in the number of application areas like banking, financial and business transactions, cheque processing, access control and e-business etc. In this project, a detailed background of signature verification system along with the available datasets are presented comprehensively. At the end, we presented the most notable challenges towards the current trends and future directions of the domain.Digital image watermarking techniques provide a way to secure the rights of the content owner and help in establishing the ownership of the digital images. These techniques add some valuable information in the image in such a way that the perceptual quality of the image remains intact. Various techniques have been proposed to achieve this purpose. Images are watermarked either at pixel level or transformed into some other transform domains such as Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and DWT, etc. Some techniques use hybrid combinations of these transforms to achieve improved results.

1.1 PROBLEM STATEMENT:

A watermarking scheme should achieve higher values of three major quality parameters, i.e. robustness, imperceptibility and embedding strength of watermark information, which are non-commensurable in nature. Increase in one dimension may result in decrease in another dimension. The watermarking technique should suitably satisfy all the three constraints. Applicability of a technique also depends upon the objective of the watermarking for the particular application on hand. DWT is a popular signal processing technique, nowadays used in various image processing applications. DWT of an image results in four different sub images named as Approximate, Horizontal, Vertical and Diagonal sub-bands. They are also represented as LL, LH, HL and HH frequency bands respectively, where L represents low frequency components and H represents high frequency components.

2.LITERATURE SURVEY

The basic model of any Digital watermarking consists of two parts first the watermark embedding and the watermark extraction but with different methods used for embedding and extraction.

Embedding method : These are mostly classified into type according to the domain in which embedding is done, first is spatial domain and other is frequency domain.

Spatial domain techniques directly deal with image pixels.the pixels value are manipulated to achieve desired enhancement.

Spatial techniques are particularly useful for directly altering the gray level values of individual pixels.

Frequency domain- When it comes to the frequency domain in image processing, it represents the changes in pixels values of the image. Any change in frequency means there is a change in the image geometry.

Any Image enhancement technique can be easily applied to the normal images. Still, frequency domain conversion of the images can lead to better enhancement. Why do we need to view images or apply enhancements in frequency domain when they can be easily used in spatial-domain?

Frequency domain Over Spatial Domain

- ➔ Frequency domain gives you control over the whole image, where you can enhance(e.g. edges) and suppress (e.g. smooth shadow) different characteristics of the image very easily.
- ➔ Frequency domain has an established suite of processes and tools that are borrowed directly from signal processing in other domains.
- ➔ Some tools used for even image recognition such as correlation convolution etc are much simpler and computationally cheaper in frequency domain.

Reasons for using DWT over DFT

- Time and frequency information
- A lot of flexibility - there are many different types of DWT bases, whereas the DFT is just based on cos and sin of different frequencies (or equivalently, complex exponentials of different frequencies).
- Because data is shattered into more components, it becomes much easier to filter in or filter out a given non stationary waveform.

- DWT is a multi-resolution representation method and it can represent local information in addition to global information.

REASONS FOR USING DWT OVER DCT

- It has multi resolutional characteristics and is hierarchical.
- Is effective also in structural attacks.
- Good localization both in time and frequency domain.
- While DCT does not work in scaling attacks.
- DCT destroys the invariance properties of the system.Certain higher frequency components tend to be suppressed during certain quantization steps.

FUNCTIONAL REQUIREMENTS

WHAT DOES OUR PROJECT DO?

Consequential requisites of the developed system comprised of the following:

- System extracts fingerprint templates into ISO format and raw images.
- System has enrollment functionality of fingerprint templates into system database
- System has verification functionality of saved fingerprints from presented fingerprints.
- System has identification functionality of saved fingerprints from presented fingerprints.
- System does encryption and decryption of users' fingerprint templates.
- System uniquely identifies and verifies users after verification and identification of their presented fingerprints.

3. REQUIREMENTS:

HARDWARE REQUIREMENT

- **System used: Laptop**
- **Operating system: Windows 10.0**

SOFTWARE REQUIREMENT

Software : PYTHON

4. DESIGN MODEL:

4.1 ALGORITHM :

STEP 1: the image is taken first from the system.

STEP 2: image is embedded with the watermarking image.

STEP 3:encoding of image.

STEP4: combine a watermark with a image document.

STEP5: CW=E(CO+W+K).

STEP 6:watermark retrieval.

STEP 7:extracting a sequence referred to as retrieved watermarks.

STEP 8:embedded watermarks are detected.

STEP 9:extraction from a suspected signal of containing watermarks.

STEP 10:extraction of original image.

4.2 SYSTEM DESIGN:

- The requirements for a biometric image authentication system are typically specified in terms of six major design parameters, namely, accuracy, cost, security, privacy and usability.

- In general, biometric image authentication systems consist of seven basic modules that operate sequentially as :

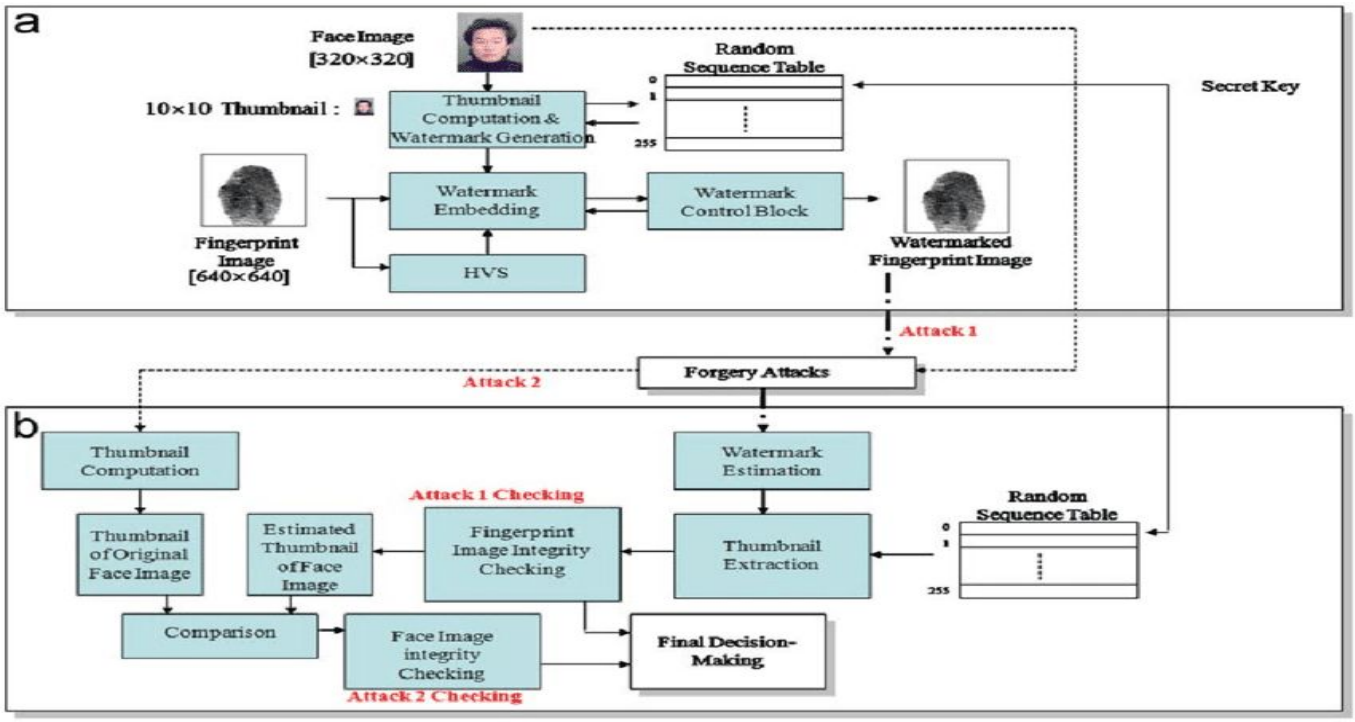
(i) a user interface incorporating the biometric reader or sensor

(ii) a quality check module to determine whether the acquired biometric sample is of sufficient quality for further processing

(iii) an enhancement module to improve the biometric signal quality

- (iv) a feature extractor to glean only the useful information from a biometric sample that is pertinent for the person recognition task

4.3 BLOCK DIAGRAM REPRESENTATION



5.PROJECT BREAKDOWN

➔ Watermark Embedding :

The algorithm to embed a watermark in the original image is summarized as follows:

1- Decompose the original image into four levels .

2- Any binary image with approximately equal number of 0s and 1s is utilized as a watermark image.

3- Map 0– 1 and 1– +1 to generate a pseudo-random binary sequence containing either 1 or +1.

4- The subband pairs (LH3, LH2), (HL3, HL2), and (HH3, HH2) at level 3 and level 2 are selected to calculate the changes made in these middle frequency subbands.

5- Apply the IDWT (Inverse Discrete Wavelet Transform) using the newly updated sub-band values at the level 3 and level 2 to obtain the watermarked image.

➔ Watermark Extraction:

Watermark extraction is accomplished without referring to the original image. The correlations Z between the DWT coefficients and the watermarking sequence to be tested at level 2 and computed by using the watermark embedding algorithm. This correlation is compared to the thresholds T saved in the watermark embedding procedure. The watermark is present if and only if one of the following conditions is true:

$$Z >= T$$

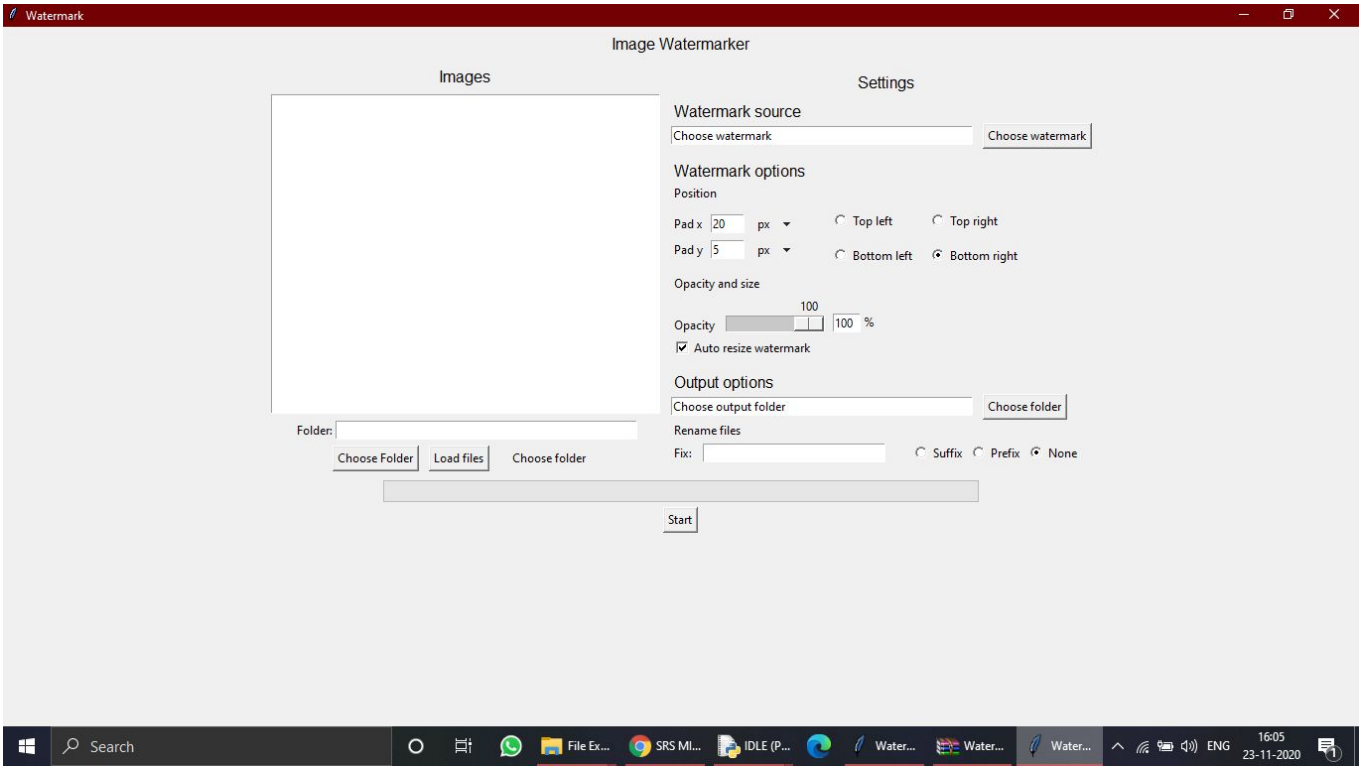
Then watermarking revealed it means watermarked image

$$Z < T$$

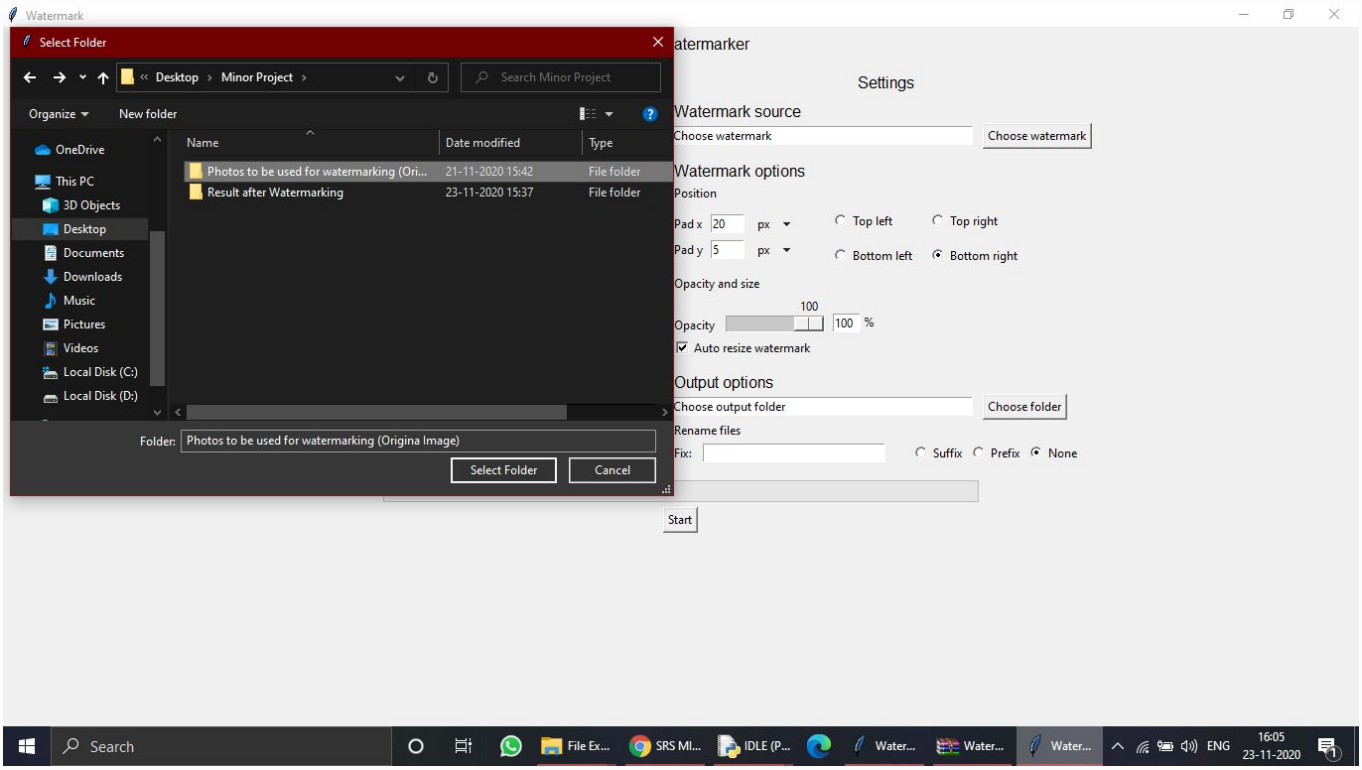
Then watermarking is not revealed; it means non-watermarked image.

6. RESULTS/SCREENSHOTS OF THE OUTPUT:

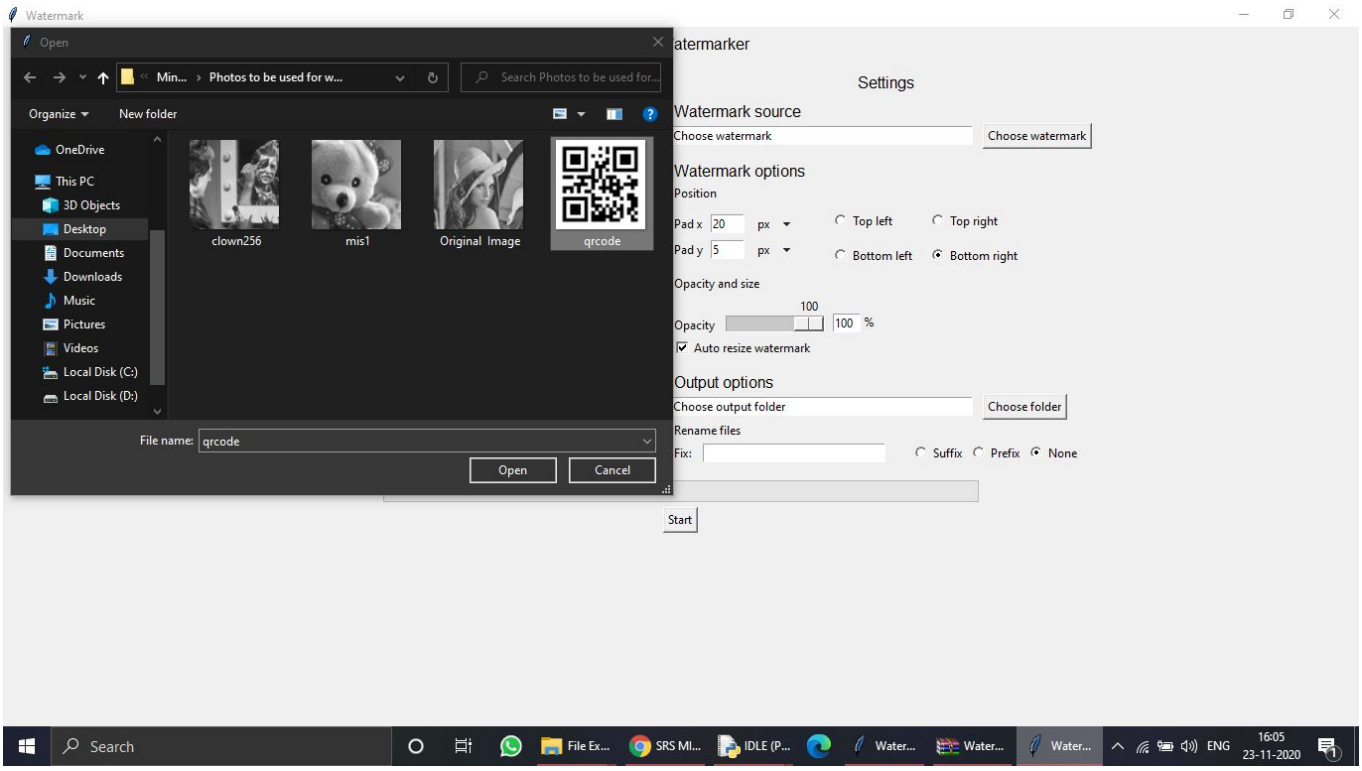
Main window



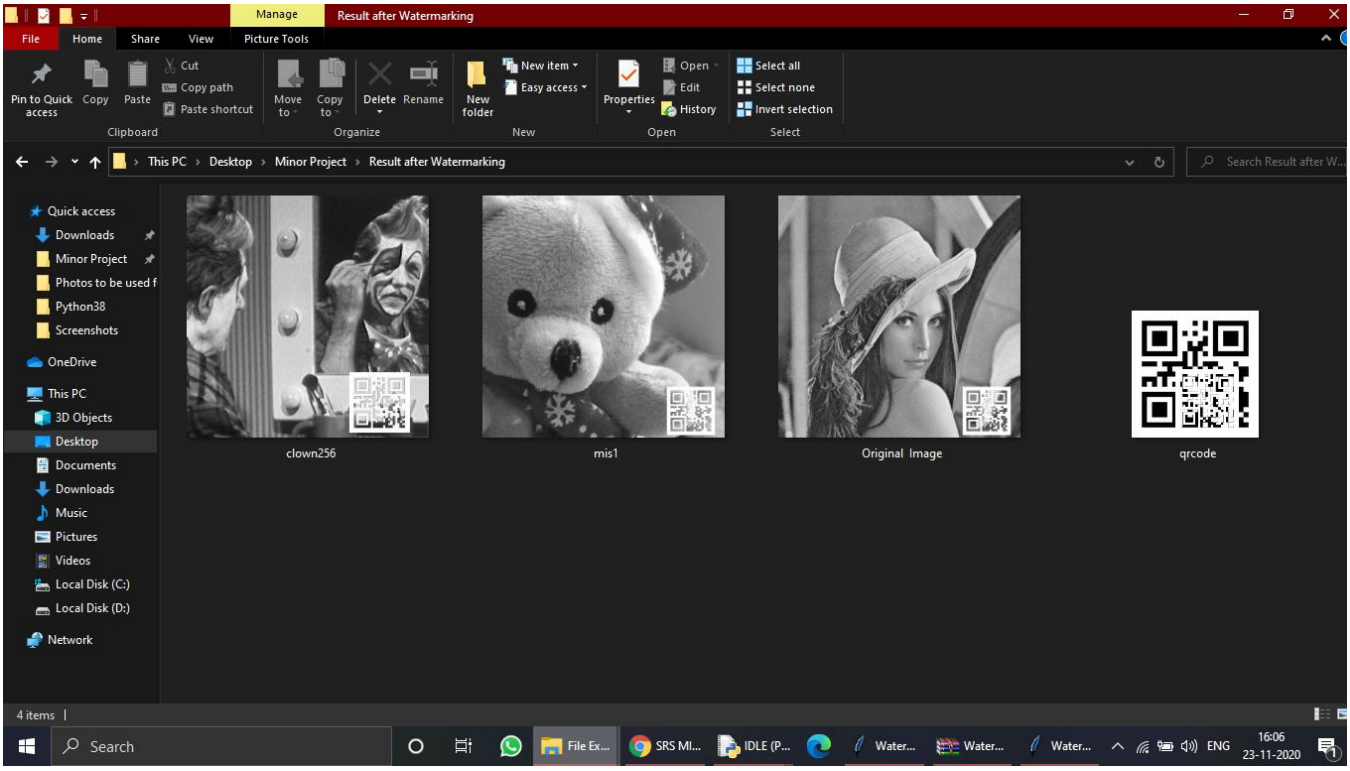
Selecting the photos to be watermarked



Selecting the watermark:



The Result :


Manage
Result after Watermarking
File
Home
Share
View
Picture Tools
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New item
Easy access
New folder
New
Properties
Open
Edit
History
Open
Select all
Select none
Invert selection
Select
This PC › Desktop › Minor Project › Result after Watermarking
Search Result after W...
Quick access
Downloads
Minor Project
Photos to be used f
Python38
Screenshots
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Local Disk (D:)
Network
clown256
mis1
Original Image
qrcode
4 items
Search
File Ex...
SRS Mi...
IDLE (P...
Water...
Water...
Water...
ENG
16:06
23-11-2020

7. References

http://www.ijoart.org/docs/Digital-Image-Watermarking-Technique-Using-Discrete-Wavelet-Transform-And-Discrete-Cosine-Transform.pdf

https://www.ijcsmc.com/docs/papers/May2016/V5I5201601.pdf

https://ieeexplore.ieee.org/document/7509352

https://www.sciencedirect.com/topics/computer-science/digital-watermarking

http://ijsrcseit.com/paper/CSEIT1831188.pdf