Report On

Digital Watermarking to Hide Text

Submitted in partial fulfillment of the requirements of the Mini project in Semester V of Third Year Artificial Intelligence & Data Science

by

Yash Patil (Roll No. 19)
Chetan Sapkal (Roll No. 39)
Shubhamkar Patra (Roll No. 37)

Mentor
Prof. Neha Raut

University of Mumbai

Vidyavardhini's College of Engineering & Technology

Department of Artificial Intelligence & Data Science

(A.Y. 2022-23)

Vidyavardhini's College of Engineering & Technology

Department of Artificial Intelligence & Data Science

CERTIFICATE

This is to certify that the Mini Project entitled **"Digital Watermarking to Hide text"** is a bonafide work of **Yash Patil(19), Chetan Sapkal(39), Shubhamkar Patra(37)** submitted to the University of Mumbai in partial fulfillment of the requirement for the award of the degree of **"Bachelor of Engineering"** in Semester V of Third Year **"Artificial Intelligence & Data Science" .**

_____

Prof. Neha Raut
Guide

_____	_____	_____
Ms. Sejal D'mello	Dr. Vikas Gupta	Dr. H.V. Vankudre
Deputy HOD AI & DS	HOD AI & DS	Principal

Vidyavardhini's College of Engineering & Technology

Department of Artificial Intelligence & Data Science

Mini Project Approval

This Mini Project entitled "**Digital Watermarking to Hide text"** by **Yash Patil(19), Chetan Sapkal(39), Shubhamkar Patra(37)** is approved for the degree of **Bachelor of Engineering** in in Semester V of Third Year **Artificial Intelligence & Data Science.**

Examiners

1……
(Internal Examiner Name & Sign)

2……
(External Examiner name & Sign)

Date:
Place:

Contents

Abstract

Watermarking is utilized to enforce ownership rights on shared data. Watermarks are primarily used for copyright protection and content authentication. Many digital watermarking methods are proposed recently to protect rights of owner along with recovering original data. Proposed system uses a fragile watermarking technique based on Robust Reversible Watermarking and sharing of image with motivation to maintain quality of image. Watermarked data is embedded into the image using LSB algorithm. This algorithm uses Random key generator to encrypt data using binary XOR and both watermark image with secret key. Results indicate that proposed watermarking scheme reduces image distortion and preserves ownership right.

Acknowledgments

This whole project has been developed by three of us i.e **19-Yash Patil, 39- Chetan Sapkal , 37- Shubhamkar Patra** under the guidance of our guide **Prof . Neha Raut** as well as we also express our special thanks to our guide who gave us this opportunity to do this project on the topic **Digital Watermarking to Hide text**, which also helped us in doing a lot of research, to know about many new things and help us in increasing our knowledge and skills. Further I would like to appreciate the efforts made by all of us in completing this project.

1.INTRODUCTION

1.1 INTRODUCTION

Digital image watermarking is simply the digital watermarking of an image, which provides an alternative solution for ensuring tamper-resistance, the ownership of intellectual property, and reinforcing the security of multimedia documents. Any digital content, such as images, audio, and videos, can hide data. Digital content can easily be illegally possessed, duplicated, and distributed through a physical transmission medium during communications, information processing, and data storage. Digital image watermarking is a technique in which watermark data is embedded into a multimedia product and, later, is extracted from or detected in the watermarked product. These methods ensure tamper-resistance, authentication, content verification, and integration of the image. It is not very easy to eliminate a watermark by displaying or converting the watermarked data into other file formats. Therefore, after an attack, it is possible to obtain information about the transformation from the watermark. To discern the difference between digital watermarking and other technologies such as encryption is essential. Digital-to-analog conversion, compression, file format changes, re-encryption, and decryption can also be survived through digital image watermarking techniques. These tasks make it an alternative (or complementary) to cryptography. The information is embedded in the content and cannot be removed by normal usage.

1.2 PROBLEM STATEMENTS & OBJECTIVES

Problem Statement:

Steganography hides the very existence of a message so that if successful it generally attracts no suspicion at all. While Cryptography is more popular than steganography but in cryptography the encrypted letter could be seen by anyone i.e. cipher text. we proposed a LSB algorithm of an image steganography system to hide a digital text of a secret message. The main goal of this method, is to hide a text of a secret message in the pixels of the image in such a manner that the human visual system is not able to distinguish between the original and the stego-image.

Objectives:

- Hiding the message in another median so that nobody will notice.
- Hidden message is imperceptible to anyone.
- Confidentiality and Authentication security.
- Communicate securely

1.3 SCOPE

Digital image watermarking using various techniques has been applied as an important tool for image authentication, integrity verification, tamper detection, copyright protection, and the digital security image.

Use of the proposed system is in medical, military or many other regions where focus is on image more than hidden information. Many times, hidden data can be secret text or used for authentication.

This project could be further be advanced with email facility for medium of exchanging data globally i.e., medium to communicate and exchange most confidential data**.**

2. LITERATURE SURVEY

2.1 SURVEY OF EXISTING SYSTEM/ SRS

- Basically, the purpose of cryptography and steganography is to provide secret communication. However, steganography is not the same as cryptography. Cryptography hides the contents of a secret message from a malicious people, whereas steganography even conceals the existence of the message.
- steganography does not alter the structure of the secret message, but hides it inside a cover-image so it cannot be seen. A message in cipher-text, for instance, might arouse suspicion on the part of the recipient while an invisible message created with steganographic methods will not. In other word, steganography prevents an unintended recipient from suspecting that the data exists.

2.2 LIMITATION EXISTING SYSTEM /RESEARCH GAP

- In cryptography, the structure of a message is scrambled to make it meaningless and unintelligible unless the decryption key is available.
- It makes no attempt to disguise or hide the encoded message.

2.3 MINIPROJECT CONTRIBUTION

- It provides a secure communication in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data.
- Secret message is encoded in such a manner that the very existence of the information is concealed.

3. PROPOSED SYSTEM (New Approach of data summarization)

3.1 INTRODUCTION

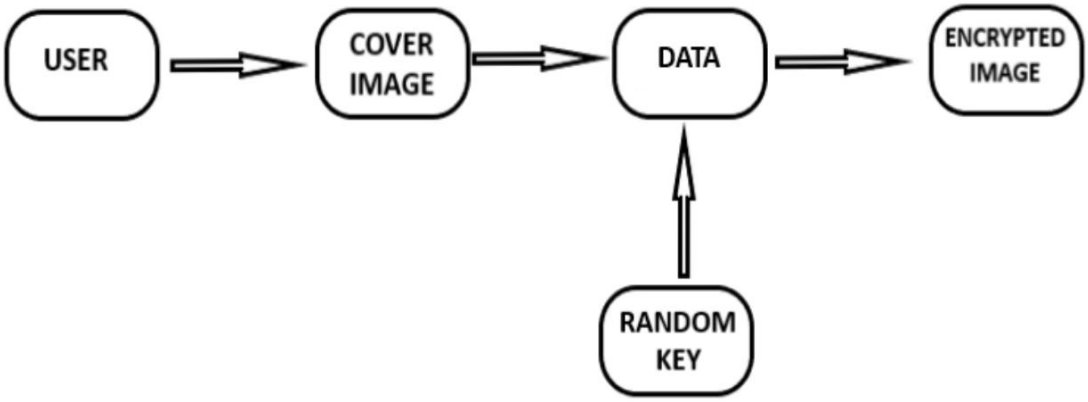
Digital watermarking, which is one of the main tools in the repertoire of DRM, is widely used to protect the copyright of digital content.

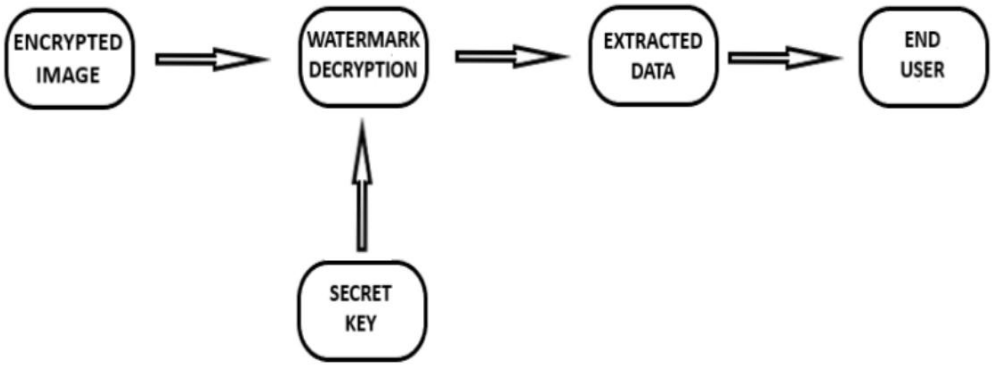
Through this system, individuals can hide a secret message within a cover-media in such a way that others cannot discern the presence of the hidden message. This is a technique for allowing two or more people to silently communicate with each other by hiding any secret message on a media cover. Files used as media can be text and image. The secret message embedded in the media cover using the appropriate algorithm and demanding the steno file itself to be sent to the receiver.

General application of include broadcast monitoring, owner identification, transaction tracking, content authentication, copy control and many more.

3.2 ARCHITECTURE/FRAMEWORK /BLOCK DIAGRAM

DESIGN:





3.3 PROCESS DESIGN

The entire project is created using the Python. In proposed system LSB with Binary XORed is used. The basic reason of using this technique is to reduce image distortion. As in this technique watermarked data is stored only in 3 bits of each pixels maintaining transparency of image. Then binary XORed operation is performed on both data and secrete key. This provides stronger authentication or security as there are total 2^{256} permutation and combinations are required to break this encryption**.**

3.4 DETAILS OF HARDWARE AND SOFTWARE

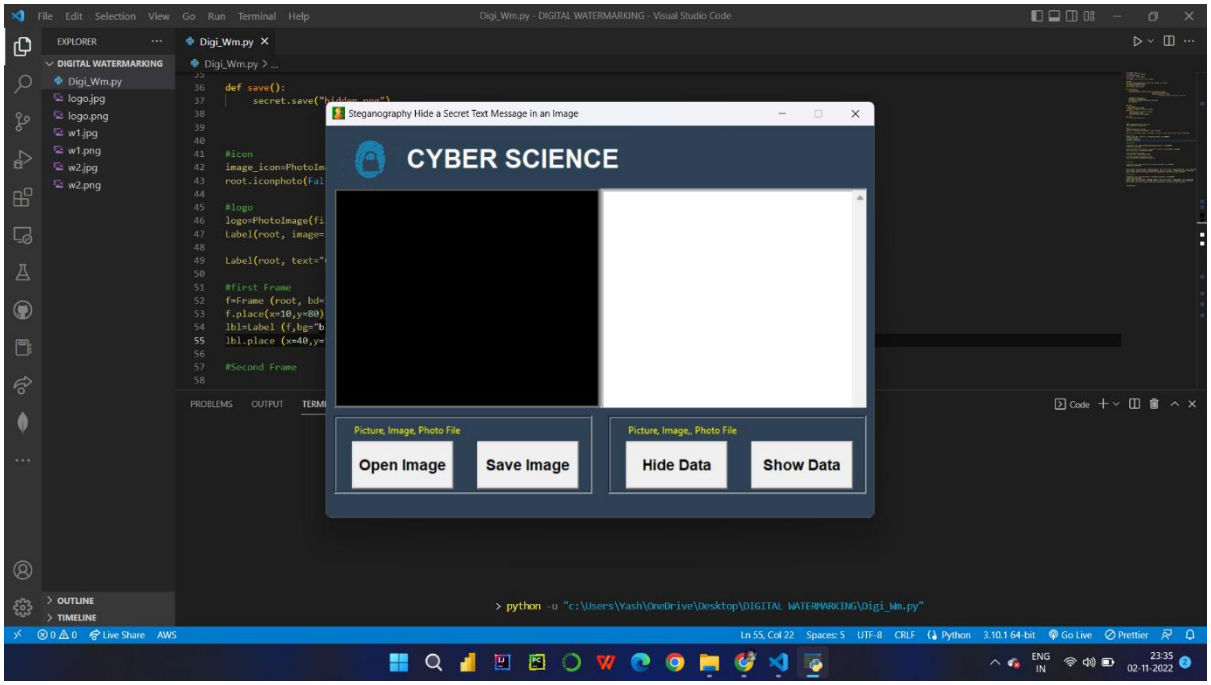
Hardware Requirement:

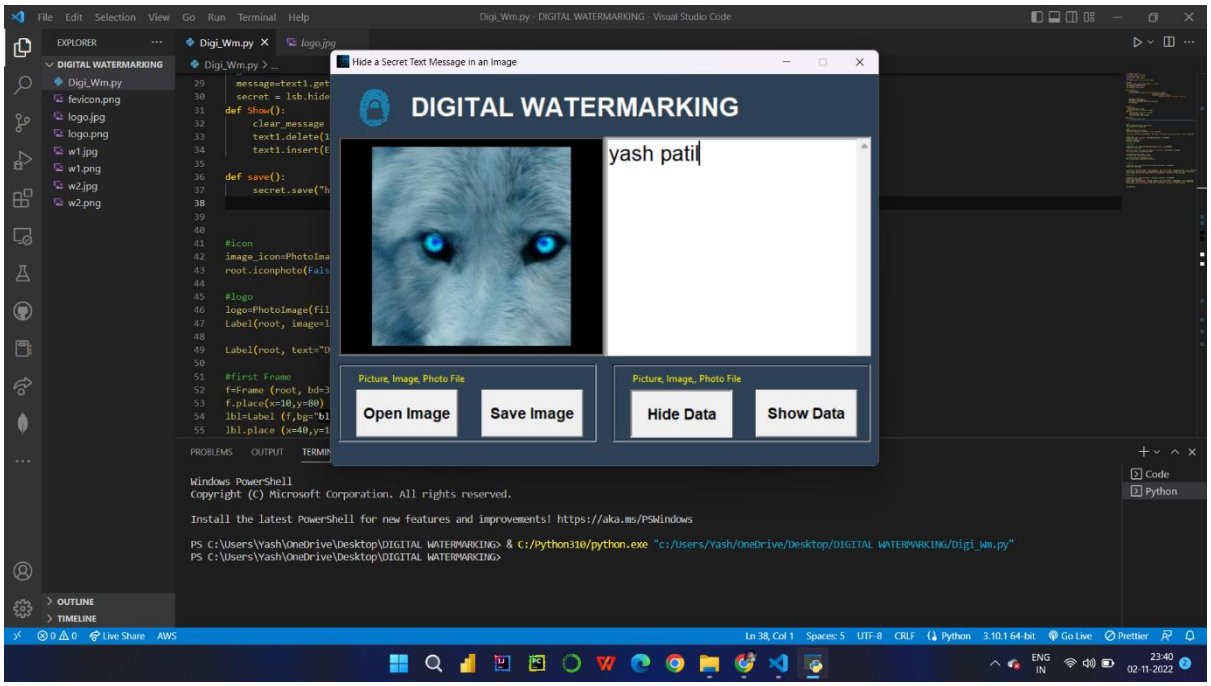
- I3 Processor Based Computer or higher
- Memory: 2 GB RAM
- Hard Drive: 50 GB
- Internet Connection

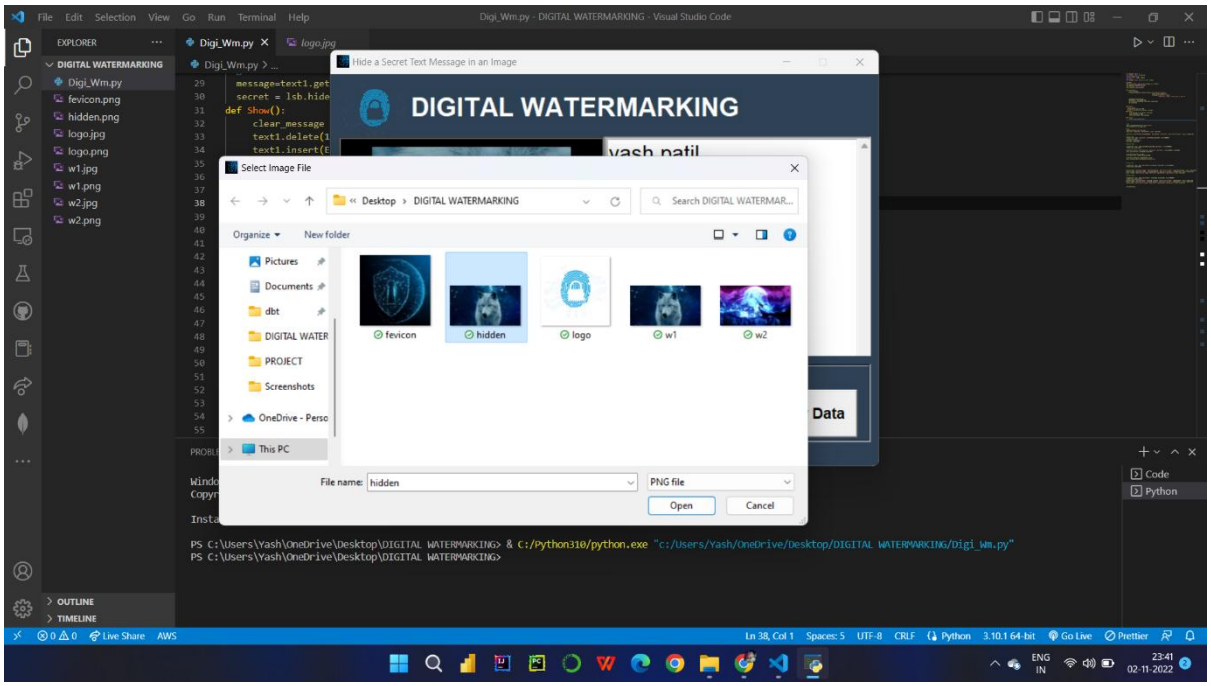
Software Reqquirement:

- Windows (OS)
- Language: Python
- VS Code
- Technology used: Steno , Tkinter

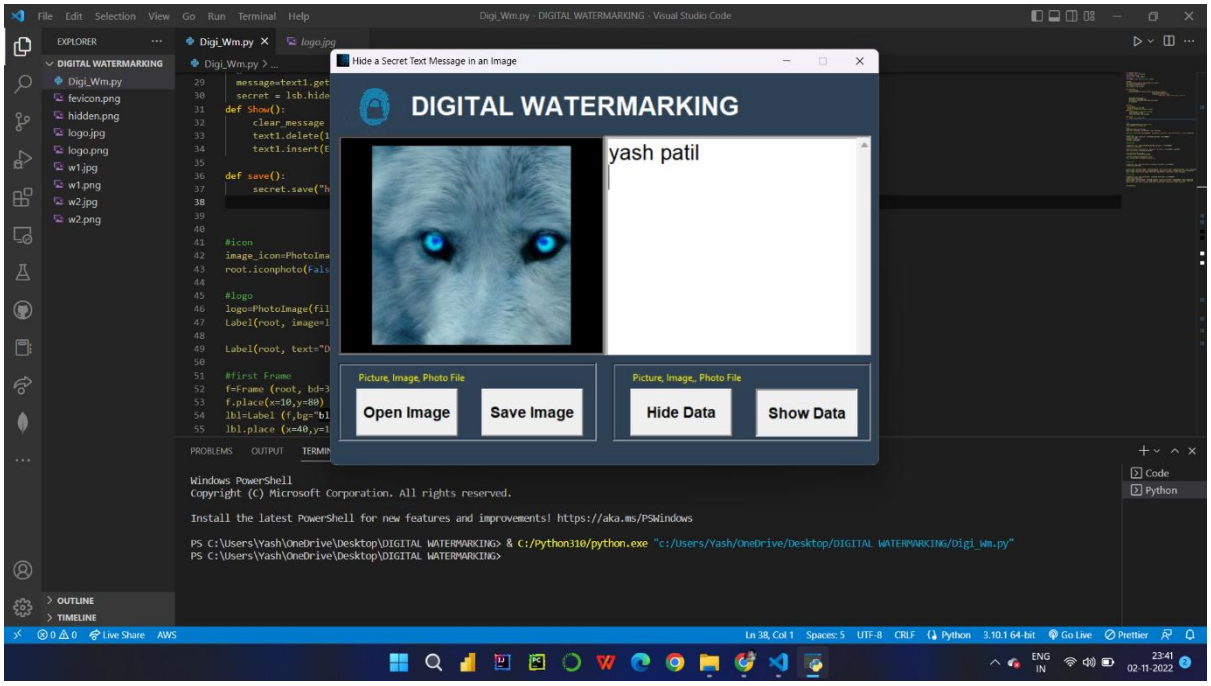
3.5 EXPERIMENT AND RESULT FOR VALIDATION AND VERIFICATION






Hide a Secret Text Message in an Image
DIGITAL WATERMARKING
Select Image File
Desktop › DIGITAL WATERMARKING
Search DIGITAL WATERMAR...
Organize
New folder
Pictures
Documents
dbt
DIGITAL WATER
PROJECT
Screenshots
OneDrive - Perso
This PC
fevicon
hidden
logo
w1
w2
File name: hidden
PNG file
Open
Cancel
Data
PS C:\Users\Yash\OneDrive\Desktop\DIGITAL WATERMARKING> & C:/Python310/python.exe "c:/Users/Yash/OneDrive/Desktop/DIGITAL WATERMARKING/Digi_Wm.py"
PS C:\Users\Yash\OneDrive\Desktop\DIGITAL WATERMARKING>

Result:


Hide a Secret Text Message in an Image
DIGITAL WATERMARKING
yash patil
Picture, Image, Photo File
Open Image
Save Image
Picture, Image, Photo File
Hide Data
Show Data
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\Users\Yash\OneDrive\Desktop\DIGITAL WATERMARKING> & C:/Python310/python.exe "c:/Users/Yash/OneDrive/Desktop/DIGITAL WATERMARKING/Digi_Wm.py"
PS C:\Users\Yash\OneDrive\Desktop\DIGITAL WATERMARKING>

3.6 ANALYSIS

In proposed system, it maintains the quality of image, as here it gives equal importance to data as well as image**.** System assures secret and safely transfer of confidential data with watermarked image and secret key. At receiver side, recovery of original data from watermarked image is done along with minimum image distortion.

3.7 CONCLUSION AND FUTURE WORK

Conclusion:

- Watermarking is a method to protect the data and to authenticate the digital content. Watermarking is required due to the emergence of usage of internet in one's day to day life. As the usage of digital content is growing rapidly, there are many instances where data is insecure. Watermarking is a process to hide data for authorization purpose. Watermarking is the best way to secure the digital content.
- In Proposed system, mainly focused on Image distortion and Data recovery. To achieve this parameter, we using least significant Bit algorithm. Concentrating on image quality as equal importance is given to data as well as cover image. At receiver side original data is extracted without image distortion.

Future Work:

- This Project will be added with an Email facility.
- Most and widely used platform for information exchange i.e., the email, providing this facility in system so that user can communication and transfer confidential data through email in secure way.

REFERENCES

[1] H. Lee, "Reversible Watermarking Exploitation Differential Histogram Modification with error Pre-compensation", in *International Conference on Electronics, Information, and Communication (ICEIC)*, 2018.

[2] S. Yi, Y. Zhou, "Adaptive code embedding for reversible data hiding in encrypted images", *IEEE International Conference on Image Processing (ICIP)*, 2017.

[3] D. Hu, D. Zhao, S. Zheng, "A New Robust Approach for Reversible Database Watermarking With Distortion Control", in *IEEE Transactions On Knowledge And Data Engineering*, 2018.

[4] S. A. Parah, G. M. Bhat, "Fragility evaluation of intermediate significant bit embedding (ISBE) based digital image watermarking scheme for content authentication", in *International Conference on Advances in Electronics Computers and Communications*, 2014.

[5] B.Sridhar, Dr.C.Arun, "A Wavelet based Image Watermarking Technique using Image Sharing Method", in *International Conference on Information Communication and Embedded Systems (ICICES)*, 2013.

[6] A. Kurapawork, M. Sahare, "A Robust Fractal Code and LSB based Image Watermarking", in *International Journal of Computer Applications (0975 – 8887) Volume 160 – No 9*, February 2017.

[7] A. Badr, M. Talal, "A novel Digital watermarking technique based on STD (standard division)",in *International Journ al of Scientific & Engineering Research, Volume 6, Issue 4*, April-2015.

[8] A. Singh, M. K. Dutta, “A blind & fragile watermarking scheme for tamper Detection of medical images preserving ROI”, in *International Conference on Medical Imaging, m-Health and Emerging Communication Systems (MedCom),* 2014.

[9] A. Bajaj, “Robust & reversible digital image watermarking technique based on RDWT-DCT-SVD”, in *IEEE International Conference on Advances in Engineering & Technology Research (ICAETR)*, 2014.

[10] S. Kiatpapan, T. Kondov, “An image tamper detection & recovery method based on self-embedding dual watermarking”, May 25, 2015.

Plagiarism Report: