LOVELY PROFESSIONAL UNIVERSITY

EFFICIENT WATERMARKING TECHNIQUE USING DWT, SVD, RAIL FENCE AND 10's COMPLEMENT APPLIED ON DIGITAL IMAGES

A Dissertation Report Submitted

BY

Kulakarni Shylesh

(11303629)

to

Department of Computer Science

In Partial fulfilment of the Requirement for the

Award of the Degree of

Master of Technology in Computer Science & Engineering

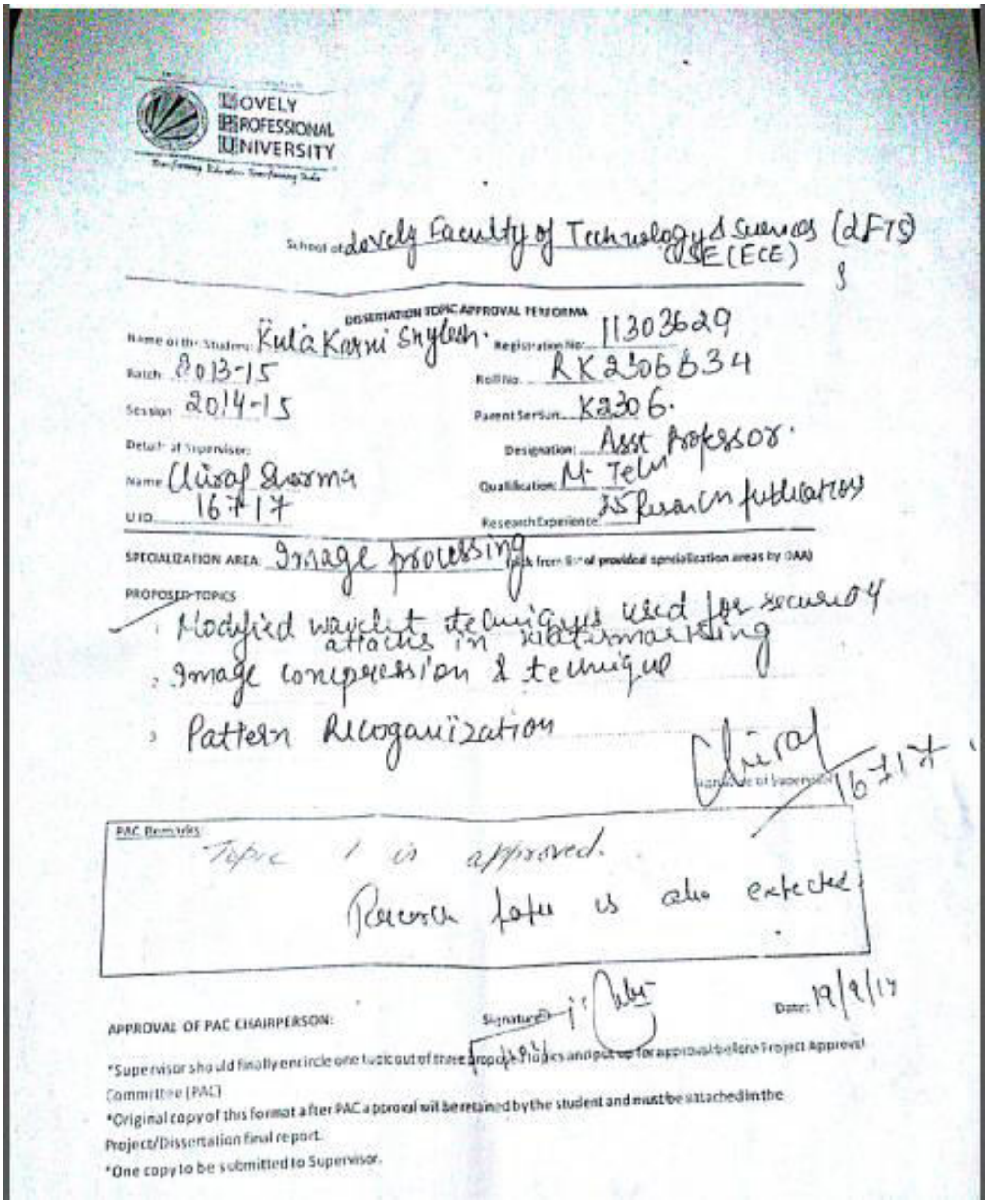
Under the guidance of

Mr. Chirag Sharma

Assistant Professor

(MAY, 2015)

PAC APPROVAL FORM



LOVELY PROFESSIONAL UNIVERSITY

Transforming Education Transforming India

School of: lovely Faculty of Technology & Sciences (LFTS) CSE (ECE)

DISSERTATION TOPIC APPROVAL PERFORMA

Name of the Student: Kula Karni Syleesh. Registration No: 11303629

Batch: 2013-15 Roll No.: RK2306B34

Session: 2014-15 Parent Section: K2306.

Detail of Supervisor: Designation: Asst Professor.

Name: Chirag Sharma Qualification: M. Tech

UID: 16717 Research Experience: 25 Research publications

SPECIALIZATION AREA: Image processing (pick from list of provided specialization areas by DAA)

PROPOSED TOPICS

1. Modified wavelet techniques used for security attacks in watermarking
2. Image compression & technique
3. Pattern Recoganization

Chirag 16717

Signature of Supervisor

PAC Remarks:

Topic 1 is approved.

Research topic is also extended.

APPROVAL OF PAC CHAIRPERSON: Signature: Date: 19/9/14

*Supervisor should finally encircle one topic out of three proposed topics and put up for approval before Project Approval Committee (PAC)

*Original copy of this format after PAC approval will be retained by the student and must be attached in the Project/Dissertation final report.

*One copy to be submitted to Supervisor.

ABSTRACT

This paper presents an efficient watermarking technique based on Discrete Wavelet Transformation (DWT), Singular Value Decomposition (SVD) and Rail Fence methods and which applied on grey scale and Digital colour images. First 10's complement and rail-fence method is applied on watermark image which gives modified watermark image. The singular values of a modified watermark image are embedded in singular values of the LL1 sub-band coefficients of the host image by making use of scaling factors. The proposed method has helped to get the robust watermarking scheme and provides security to the Watermark image. This proposed method will helpful for copyright protection. This approach leads to secure transmission of digital data.

CERTIFICATE

This is to certify that **Kulakarni Shylesh** has completed M.Tech (Computer Science and Engineering) Dissertation titled **“Efficient watermarking technique using dwt, svd, rail fence and 10’s complement applied on digital images”** under my guidance and supervision. To the best of my knowledge the present work is the result of his original investigation and study. No part of the dissertation has ever been submitted for any other degree or diploma.

The dissertation is fit for the submission and the partial fulfilment of the conditions award of M.Tech (Computer Science and Engineering) degree.

Date: ____________

Signature of Advisor

Name: ________________

UID: _________________

ACKNOWLEDGEMET

I am very grateful to my project guide **Mr. Chirag Sharma,** Asst. Prof. in Department of Computer Science & Technology, Lovely Professional University, for his extensive patience and guidance throughout my project work. Without his help i could not completed my work successfully. I would like to thank **Mr. Dalwinder Singh**, Professor and Head, Department of Computer Science and Engineering, Lovely Professional University, for having provided the freedom to use all the facilities available in the department, especially the library. I would also like to thank my classmates for always being there whenever I needed help or moral support. Finally, I express my immense gratitude with pleasure to the other individuals who have either directly or indirectly contributed to my need at right time for the development and success of this work.

DECLARATION

I hereby declare that the dissertation entitled, **“Efficient watermarking technique using dwt, svd, rail fence and 10’s complement applied on digital images”** submitted for the M. Tech Degree is entirely my original work and all ideas and references have been duly acknowledged. It does not contain any work for the award of any other degree or diploma.

Date: _____________

Investigator

Regn. No. _____________

TABLE OF CONTENTS

Sr. No	TOPIC	PAGE
1.	**INTRODUCTION**	**1**
	1. Introduction	1
	1.1 Digital Watermarking	2
	1.2 Techniques used in Digital Watermarking	3
	1.3 Types of Watermarking based on visibility	7
	1.4 Types of Watermarking based on content.	7
	1.5 Applications of Digital Watermarking	8
	1.6 Video Watermarking	9
	1.7 Terminologies used in Digital Watermarking	10
	1.8 Digital Watermarking Security Attacks	10
2.	**LITERATURE SURVEY**	13
3.	**PRESENT WORK**	**17**
	3. Present work	17
	3.1 Scope of the study	17
	3.2 Problem formulation	18
	3.3 Objectives of the study	19
	3.4 Research Methodology	19
4.	**RESULT AND DISCUSSION**	**23**
	4. Result and discussion	23
	4.1 Grey scale images	23
	4.2 Digital colour images	31
	4.3 Extraction of original image	37
5.	**CONCLUSION AND FUTURE SCOPE**	**41**
6.	**REFERENCES**	**44**
7.	**APPENDIX**	**46**
	7.1 Questionnaires	46
	7.2 List of Abbreviations	47

LIST OF FIGURES

FIGURE.NO	TOPIC	PAGE
1.	Brief idea of spatial and frequency domain………………………	3
2.	Encoding process of DWT…...	5
3.	1-level decomposition of an image……………………..…….......	5
4.	Proposed watermark embedding algorithm...……………………..	21
5.	Proposed watermark extraction algorithm………………………..	22
6.	Grey scale watermark image ………………………....................	24
7.	10’s complemented watermark image ……………………….…......	25
8.	Rail-fence encryption on 10’s complemented watermark image....	25
9.	Watermarking image ……………………..................................	26
10.	Extracted watermark image ………………………......................	26
11.	Watermark image (bird) bar chart..	27
12.	Extracted watermark image (bird) bar chart................................	29
13.	Extracted original image ……………………............................	29
14.	Watermark image after extraction (on grey scale)……………….	30
15.	Watermark extraction by attacker (grey scale image)…………...	31
16.	Digital colour watermark image ………………………..............	32
17.	10’s complemented watermark image …………………………....	32
18.	Rail-fence encryption on 10’s complemented watermark image.	33
19.	Original image ……………………..	33
20.	Watermarking image ……………………................................	34

21. Watermark image after extraction process ……………………. 34

22. Original image after extraction ……………………….............. 35

23. Nature original image …………………….......................... 37

24. Extracted original image ……………………….................... 37

25. Watermark image after extraction (on digital colour image)…. 38

26. Watermark extraction by attacker (digital colour image)…….. 38

27. Watermark image bar chart... 39

28. Watermark image bar chart after brute-force attack................ 40

LIST OF TABLES

FIGURE.NO **TOPIC** **PAGE**

1. PSNR and NC (w,w') values (For grey scale images)............ 28

2. PSNR and NC (w,w') values (For digital colour images)..... 36

3. 10's complement results ……………………..……........... 41

4. 10's complement comparison results...…………………….. 42

CHAPTER 1

INTRODUCTION

Introduction

Image processing is acts as an important application for the computer graphics, it mainly focussing on the things like how an image is stored, retrieved, manipulated if necessary. The main goal of digital image processing are we need to store the picture in certain format (eg: jpeg or jpeg 2000), retrieve the image from where you have stored, we needs to manipulate the image if it is necessary and There should be no noise in a picture. So our main goal of this image processing is to store the data in a compressed manner for that we need some technique like data or image compression. If we compress our data then we can send it easily through the network. There are many technologies in image processing such as Digital Watermarking, Image Compression and Gait Recognition. In Digital watermarking the main aim is to secure the digital content by embedding some information that information exist in the form of text, image, audio or video. This Digital watermarking is used in several areas like medical field, military field and Multimedia technology. Image compression is used to compress the large digital content in to small digital content without any loss of data. Advantage of using image compression is to store the digital data in compressed manner; we can send that data through the network in very efficient way and it requires less amount of band-width to transmit the digital content. In Gait recognition the main aim was to recognize the people according to walking style of them. Every person has unique walking style so according to that we will recognize the people. Research work is mainly going under this gait recognition. Face recognition is a part of an image processing which will recognize the people according there facial structure. Facial information of a person is stored in an intelligent system if any person want to communicate with any system or a device then it scans the face using sensors if match found then the person is authorized. We have many recognition like thumb recognition, Ankle Recognition and Behaviour Recognition these all are parts of Biometrics and these all are having one similar application area that is security. Digital watermarking is a technique where we embed some information into the digital content, that information may be in the form of text, image, audio or video. The major reason for using these watermarking techniques is to secure or protect the digital content (image, text, audio or video). Digital watermarking has used in many areas. Digital watermarking is the popular topic for both researches and applications in the last 10 years [9]. Now a day's multimedia technology has been grown very fast and for secure digital data transmission, need some special mechanisms like digital watermarking. Normally user uses the audio and video file's that are exist in the websites at free of cost but the problem comes in case of the protection of that digital content (audio or video file). If any un-authorized user will access that digital content and altering that data is called as attacking against authentication. Use such a watermarking technique that will protect our digital content in such a way that it will give protection during its (watermark) entire lifespan. These watermarking techniques also provide the ownership identity, proof of ownership and they are two important applications of multimedia technology. Digital watermark is added to the legal copy (original file) such that it can protect the copy rights of the digital content. Video watermarking is used to protect the videos in the internet. In video watermarking, embedding the watermark to the frames of the videos and it will give the watermarked video and it acts as legal copy of the digital content. Several mechanisms exists in the digital watermarking, they are: Embedding process has been done in between the digital content and watermark data (image, audio or video) it will give the watermarked digital content and the other side the detection action was performed against the watermarked data, in detection action the inverse action will be performed and they gives digital content. Sometimes the other side attacker also present so provide such a mechanism it will protect the watermarked image in such that it can't be detected and modified by the attacker.

1.1 Digital watermarking

Digital watermarking is a process of embedding some information (text, image, audio) in to the digital content. Encryption process protects the content through the transmission process; but once the content is decrypted the data cant protected but it should protect the identity by using some methodologies such as digital watermarking. Watermarking and encryption should be used as two complimentary techniques.

1.2 Techniques used in watermarking

Watermarking is a method of hiding the digital content by using some secret information (watermark). This hiding process is done by using watermarking extraction algorithm. Our main goal is to use such an algorithm which will give the protection for our digital content i.e which produces the robust and secure watermarking approach. If attacker will know the algorithm then he can easily destroy the digital content or he will remove or manipulate the given digital content.

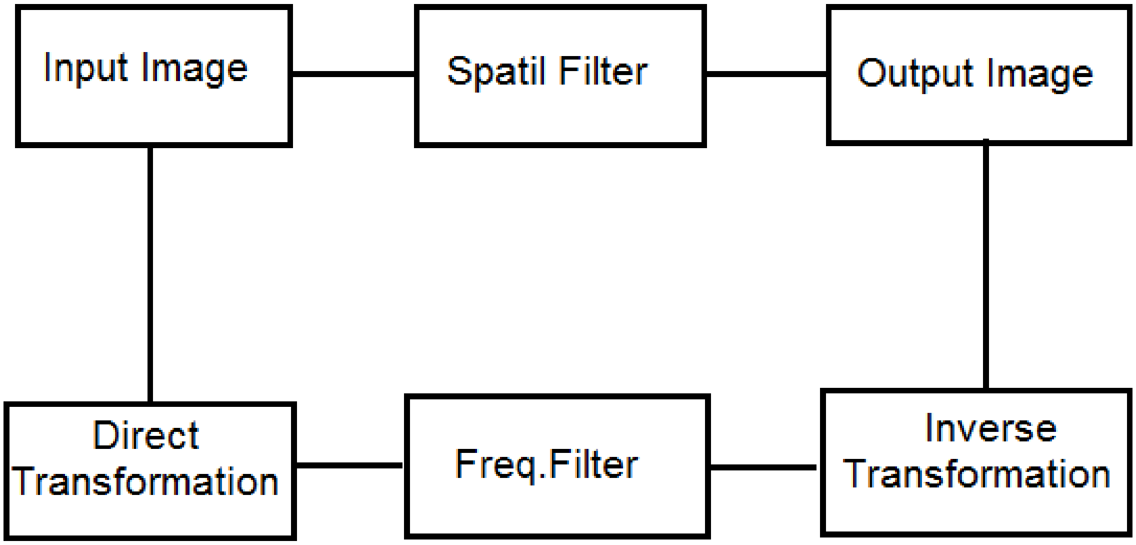


Figure 1: Brief idea of spatial and frequency domain

Above figure is explaining about the spatial domain and frequency domain. In spatial domain we use only spatial filter which will give the output as watermarked image. In these spatial filters the process is directly performing on the pixels and they are sensitive against the attacks. But in frequency domain, before goes in to frequency filter first the transformation has been taken place after that it goes into frequency filter and gives the watermarked image after this it will perform inverse transformation and then it will give the output.

Basic Purpose of Transformation is:

i. The transformation coefficients should have the energy compaction capability. In the sense bulk of energy will be present in the few transformed coefficients in the signal. This will give the efficient compression by truncating the coefficients which will not carrying the significant energy.

ii. The transformed coefficients must be de-correlated to each other. For this we need the orthogonal transformation such as DCT, HAAR wavelets and DWT etc.

I. **Frequency Domain Watermarking:** Compare to spatial domain methods, frequency domain methods are mostly used in many applications. The Embedding process in the frequency domain is performed at the spectral coefficients of the image [5]. Some types of frequency domain watermarking are

a. **DCT (Discrete Cosine Transformation):** It represents the data in terms of frequency space. DCT based watermarking techniques is more robust when compared to spatial domain techniques. The implementation of DCT is more difficult and its week against some geometric attacks. The Computational complexity of DWT is more when it is compared with DCT. DCT provides lossy compression; the important data (watermark image) may be lost some times so this method is not suitable now a days. This issue is solved by using the Wavelet transformation method. This is the formula to calculate DCT value

$S(k1,k2)=(2/N)*c(k1)*c(k2)*\sum_{n1=0}^{N-1}\sum_{n2=0}^{N-1}\cos\left(\frac{\pi(2n1+1)}{2N}\right)*\cos\left(\frac{\pi(2n2+1)}{2N}\right)$

c(k)={1/√2 for k=0 at boundaries and

{1 otherwise.

b. **DWT (Discrete Wavelet Transform):** The Localization property is restricted in DCT. It is the limitation for the DCT method this will be solved by the wavelets. Wavelets are small wave or time limited waves which depend on two parameters such as scaling and shifting. Scaling means at what extent it should be scaled and shifting means at what extend it should shifted. Wavelet transformation is a combination of summation of scaling function and summation of wavelet function. In real word we work on discrete signal not on the continuous signal. Wavelet permits us to transformation and inverse transformation by using two banks of filters such as analysis filter and synthesis filter.

For forward transformation we use the analysis filter and for reverse transformation we use the synthesis filter. When the 2-D signal is going to the analysis signal in case of 1-level of decomposition the signal is become ¼th of the original signal it will give four sub bands (LL, LH, HL and HH) with different resolutions. The transformed signal will go into the synthesis filter and it will give the original signal as the output. We mostly prefer the low pass filter version of an image why because the image at low frequency value will be good quality image. In JPEG 2000 version the experts uses the DWT as the compression scheme.

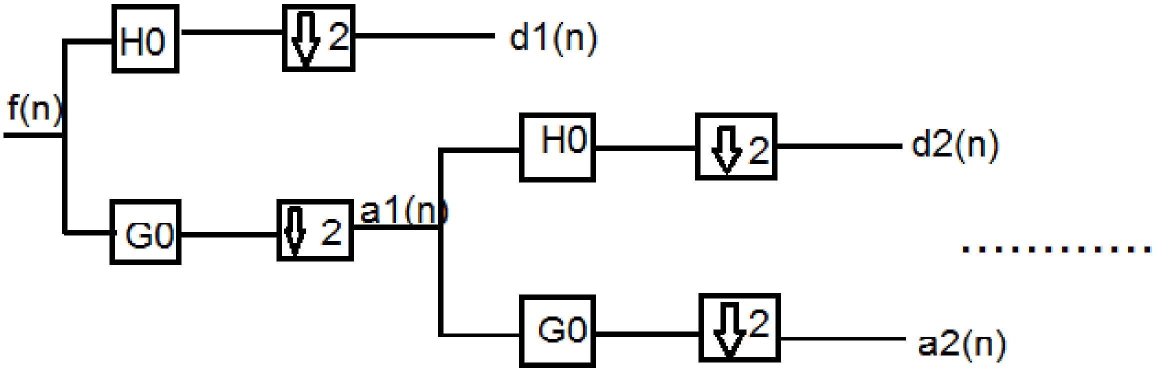


Figure 2: Encoding process of DWT

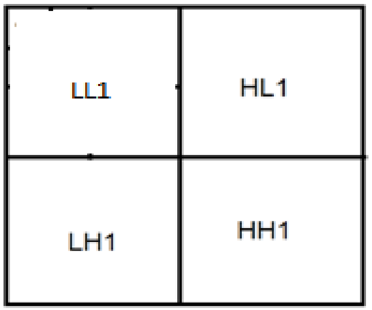


Figure 3: 1-level decomposition of an image

In this above diagram figure 2, it has been observed that the given signal (f(n) which is a combination of both scaling function and wavelet function) is decomposed into several signals by factor of two at the low pass filters side.

Haar wavelet-transform (1-D DWT): The following steps to be performed to calculate the Haar-wavelet transformation: First find the average of each pair of samples, then find the difference between the average and sample, fill the first half part with averages and second part with its differences and repeat the process on the first part until it reaches to end of the part. This process will be considered for the encoding process of the image. This is also be a compression process of the image. After applying inverse of the averaging the difference and we will get the original image. This process is called as de-compression of the image.

c. Singular Value Decomposition (SVD): This is one of the numerical Analysis techniques which is use to decompose the image into Different levels. In the earlier days it will works only on the square images but now technology has improved so now it is useful for the Rectangular images also. SVD method will be used in many Applications such as image watermarking, image hiding, image compression and Noise Reduction. It is also used in the Dimensional Reduction so that it can achieve compressed or optimum Approach.

Consider an image N×N size represented with A and it will decomposed into the following

A= UA*SA* $(VA)^T$ = $\sum_{i=1}^{r} ui * si * (vi)^T$ where UA = [u1, u2, u3….uN]

VA = [v1, v2…….vN]

$$S=\begin{pmatrix} s1 & \cdots & N \\ \vdots & \ddots & \vdots \\ 0 & \cdots & sN \end{pmatrix}$$

UA and VA are the N×N Orthogonal Matrices and S is consists of Singular values from (s1, s2,…sN) and this is in the decreasing order. This method is for the Host image and watermark image.

d. 10's Complement: Normally Calculate the 10's Complement of the Watermark Image Pixel values. This provides some Security to the Watermark image when it is added with Rail fence method.

Example: 10's Complement of 233

(9-2) (9-3) (9-3) = 766

Then add 1 766+1=767 (it is 10's Complement of 233).

e. Rail Fence Method: It is the basic Transposition technique which will be used to Encrypt and Decrypt the given input data without using any key and provide security. By applying Double Rail fence on the given input the security will increases more.

Example: input: she is watching tv, this will be written as follows:

s e s a c i g

h i w t h n

Encrypted data is: sesacighiwthn. These two types of the methods are applied on Watermark image it will increase the security of the Watermark image when it is compare with the Existing System.

1.3 Types of watermark based on visibility of the watermark: Types of watermark based on visibility of watermark are: visible watermark and in-visible watermark

a. Visible Watermark: This type of watermark is embedded in a digital content in such a way that it will visible to human eye. In this case it will show about ownership of the digital content.

b. In-visible watermark: In this type the watermark is embedded into digital content in such a way that it will not visible to human eye. Advantage of using in-visible watermarking is that the watermark is not visible so that the removal of the watermark for attacker is so difficult.

1.4 Types of watermark based on content to be watermark

The types of watermark based on content to be watermark as follows below:

a. Image: The watermark in the form of image in Digital Content. It means that in this case the watermarked data will be present in the form of an image. To protect the digital content this image will be embedded into the digital content (image or video).

b. Text: The watermark in the form of Text in Digital Content. It means that in this case the watermarked data will be present in the form of a text. To protect the digital content this text will be embedded into the digital content (image or video).

c. Audio: This area is the more popular and important due to the large use of internet music and mp3 in our daily life [6]. This audio watermarking will be used to protect the audio files which are there in an internet.

d. Video: in this case the watermark is added to the video sequence to protect the video data. This method will require practical extraction and robustness for compression [6].

e. Graphic watermarking: It embeds the watermark to 2D or 3D computer produced graphics for the copyright [6]. This will helps in indicating the ownership of the digital content by using the graphics and watermarking the data.

1.5 **Application of Digital Watermarking:** The applications of Digital watermarking as given below:

a. **Copy-Right Protection:** It is used to identify and protect the Ownership copy rights. In this case some Digital data is embedded in to the original data. So that it gives the identification of the owner. By providing a robust algorithm which gives the security i.e if any attacker wants to remove the watermark from the original data then it should not be removed and it always remains with the original digital data.

b. **Digital Right Protection:** DRM presents the embedding of some DRM information into the original digital so that it will protect the copy and also owner will easily control and monitor the data by using some mechanisms. If any un-authorized member will access the copy and making duplicate copy of that original copy and he/she will easily traced.

c. **Tampering Proofing:** This is used for authentication purpose of the Digital content. In this the Digital content is embedded with fragile watermark. Digital Content gets destroyed whenever an un-authorized person wants to modify the original digital content.

d. **Broadcast Monitoring:** In this fast market condition knowing broadcast has become very difficult for content owners, copyright holders, distributors and broadcasters. Watermarking techniques are not only useful for secure the ownership details and identification of ownership but also controlling the flow of that unauthorized users and tracking them easily.

e. **Fingerprinting:** This acts as an object which is differentiates another object. This is very important application of copyright protection. It is used for the purpose of authentication and which gives the protection from un-authorized users. For the authentication, hash functions such as SHA algorithms are used.

f. **Access Control**: In this, if a user has legal license then only he/ahe will able to get digital content in the internet. It means if he/she an un-authorized member then the access is denied for them.

g. **Medical Field:** In medical field these watermarking techniques usually used for protecting the patients record and Medical reports. The Medical Reports are used to the treatment for the patient. In the medical field the watermarking techniques are very useful for secure transformation of medical information among the hospitals.

h. **Media forensics:** This application is very useful for a content owner. If any un-authorized member will misuse his/her digital content then he/she will compare that digital content with original content then he/she will able to get the evidence for that crime.

i. **Remote Education:** Now a day's distance education has been grown due to the lack of teaching faculty or some others reasons. The major issue in the distance education is the distribution of content and teacher-student interaction [8]. In this case we will use image watermarking technique so that it will protect the image of the distance learner so that it can store and protect in the university server. In this case we will also use the watermarking techniques for secure transformation.

j. **Health and car insurance companies:** Health and car insurance companies nowadays uses image processing [8]. Health insurance companies stores the scanned copies of the medical images of their clients. They stores these images in the main office server so that it will be useful when any client loss the vehicle.

1.6 Video watermarking

Video watermarking is the process of embedding some information in to the video file to secure or to protect that video from the un-authorized users. That information may be directly inserted in to the raw video or integrated during embedding process or implemented after compression of that specific video file. These video watermarking is used in many fields like medical, film, army and multi-media etc. The embedding or encoding process of video watermarking can be written as:

a. **Process of encoding**: The encoding process can be written as:

$X'=E(X, W, [K])$

Where, X is Original video file

W is watermark that is used insert in to the video file

K is a key

X' is a watermarked video.

b. **Process of decoding** : The decoding process can be written as:

$W'=D(X'', [X], [K])$

c. **Video watermarking is used in**: Video watermarking is used in several areas: internet multimedia, wireless video, personal video recorder, video-on-demand, set-top box, Video Phone and Video Conferencing.

1.7 The terminologies that are used in video watermarking

The following are some terminologies that are using in this video watermarking they are:

a. **Digital video**: This is also called as original video which we want to be watermarked. It is a collection of frames. In these frames only we are embedding the watermark by using embedding algorithm.
b. **Payload**: The amount of information that is stored in a watermark. This is also called as size of the watermarked data that we are embedding in to the frames of the video file. According to the change the scene in the video the embedding process has been completed.
c. **Perceptibility:** The watermark only detected by using some special methods that is applied on it. If the method is not known by the person then it is difficult to view and hear the watermark. The authorized person only accesses the content. These types of approaches are useful for the authentication to the watermark data in the digital content.
d. **Robustness:** Watermark will be always presents with in a video file only. We will use such a robust algorithm that will gives the maximum security it means that if any attacker wants to remove the watermark from the original data(video file) then it cannot be removed and it is always remains with the original digital data.
e. **Security:** It should be always protects the watermark by using some algorithm and that algorithm should be always kept it as public and also we should think about the key algorithm is pubic, so choice of a key has done from a large set of key space.

1.8 Watermarking attacks

There are many types of attacks which affects the robustness of the watermark data. Using some software's in the image processing attacker performs the attack on digital watermarking data. This will affect the robustness and security of the watermarking system. There are some possible attacks in the given below such as:

a. **Geometric attacks**: All changes affect the geometric size of the image such as flipping, rotation and cropping etc. A cropping attack done from the right-hand side and the bottom of the image is an example of this attack.

b. **Low pass filtering attack:** A low pass filtering is performed on the watermarked image and this produces different combinations of the noisy image.

c. **Forgery attack:** this attack produced by inserting any unwanted object in to the content or deleting the important scene background from the image. This attack will damage security of the ownership in digital media.

d. **Security Attack:** generally if the attacker is known the watermarking algorithm, then he/she perform such an attack which will change the entire content in the watermark image [5]. The watermarking algorithm which is said to be secure if the watermarked information may not be deleted from the host data.

e. **Cryptographic attacks:** Cryptographic attack is mainly effects on the security of the watermark image. Brute force is one of the Cryptographic attacks which will performed by entering all possibilities of the key and get the original watermark data. For this need of secure and robust algorithms are mandatory.

f. **Active Attacks:** In this, the attacker purposely trying to remove the watermark from the extracted data and make it as useless data. This is a big issue in copyright protection, fingerprinting or copy control for example. Content modification and replay attack are comes in the active attacks. For this also need of secure and robust algorithms are mandatory.

g. **Passive Attacks:** In this case, the attacker is not trying to remove the watermark but simple he/she will check the existence of the watermark in the original file.

h. **Collusion Attacks:** In this attack normally unauthorized person wants to remove the watermark for that he takes the duplicate copies of the same data and then he inserts the different watermark data in to the copies and produces the several duplicate copies of the original data with different watermark data. This will be very serious problem in the case of the authentication, fingerprinting and proof of the ownership.

i. **Image Degradation:** in this attack first attacker wants to remove the parts of the image then some time there may chance to lose some important information and it affects the robustness of the watermark. Some time there may be chance to lose watermark information so this types of attacks are serious issues for the digital watermarking schemes.

j. **Image Compression:** for the reduce storage space and to transmit the image in the limited bandwidth generally images are compressed by using JPEG and JPEG2000 compression techniques. These lossy compression methods are more damaging as compared with lossless compression methods. Loss less compression methods can extract the watermark information by using inverse operation. By using quantization step in the lossy compression there may be a chance to lose important information about the watermark in the reverse process. So the probability of extracting watermark information is always less in the lossy compression.

k. **Removal attack**: in Removal attacks the attacker intention is to remove the watermark from the watermarked digital content. After this attack the watermark images becomes the noisy image or blur image and which presents in the host image. The problem with this attack will be, there may be chance of loss of important data which will be useful.

CHAPTER 2

LITERATURE SURVEY

Literature survey

Monia Ghobadi (2001) conducted a survey on wavelet-based coding and its application in JPEG 2000, this paper presents the wavelet transform and 1-D Discrete and 2-D Discrete wavelet transformations and also discussed about the Haar wavelet transformation with an example. This paper also presents the applications of the digital watermarking in the present generations. This presented technique is useful for the copyright protection, Copy-Right Protection, Copy Protection, Digital Right Protection, Tampering Proofing, Broadcast Monitoring, Fingerprinting, Access Control, Medical Field, Media forensics and Electronic Distribution. This paper also presents various attacks are performed on the watermarked image which will produce the better results with efficient PSNR values and NC values.

Sukhendu das (2002) conducted lecture on image compression and how DCT (Discrete Cosine Transformation) method is helps to achieve it. In this demonstration he explains with an example so that this topic very easy to understand. This demonstration also presents the applications of the digital image processing. This lecture contains the basic steps that are performed on the image and also explains the techniques that are used in the digital image processing. The major issues that are produced by the quantization table will be the loss of important data. If this method will apply on the watermark image there may be a chance to lose some important information. For the better results of the quality of the image most generally preferred method will be the wavelet transformation.

Prabhishek Singh, R S Chadha (2003) conducted a survey on Digital Watermarking Techniques, Applications and Attacks. This paper presents various types of techniques that are used for the digital watermarking and also contains the applications of digital watermarking (image, audio, text and video). It presents watermarking technique in case of spatial and frequency domain and its difference. It presents the security attacks in the digital watermarking and security issues that are affecting on the digital watermarking. The experiments results of this paper will give the betterment in case of the security of the watermark in the digital data and which is the best approach for the copy right protection and the to protect the distribution rights of the ownership.

Neha singh, Arnab nandi(2003) conducted a survey on digital watermarking mark this technology this paper presents the watermarking techniques in the spatial domain and frequency domain. This also have the brief explanation about the technique that are used in digital watermarking, watermark insertion and watermark detection (watermark embedding and detection).the main drawback of the spatial filter is directly applying the filtering on the pixel intensity values. The un authorized person will easily break the data so this is not robust approach for the image watermarking where as frequency filters are some intelligent techniques which presents the transformation before the filtering process which produce the robust and secure watermarking scheme. This paper mainly presents the difference between this both the filters.

Prabhishek Singh, R S Chadha (2003) conducted a survey on Digital Watermarking Techniques, Applications and Attacks. This paper presents the various types of techniques and applications that are used for the digital watermarking. Some of the applications like Copy-Right Protection, Copy Protection, Digital Right Protection, Tampering Proofing, Broadcast Monitoring, Fingerprinting, Access Control, Medical Field, Media forensics and Electronic Distribution for Digital Watermarking. This paper also presents the various types of the attacks which effects the robustness of the watermark which exist in the digital content and shown the efficient results for the security against many types of the watermarking attacks.

Sourav Bhattacharya, T. Chattopadhyay and Arpan Pal (2006) conducted a Survey on Different Video Watermarking Techniques and Comparative Analysis with Reference to H.264/AVC this paper presents the basics of video watermarking and how the encoding, decoding and detection process will be held and also presents about the terminologies that are used in the video watermarking and also presents the technique that used for video watermarking. This comparative analysis is performed based on various types of robustness algorithms which are applied on the same watermarked image and got the efficient outputs for the various types of attacks are applied on the same watermarked image

Li Hui-fang, Chen Ning, Chen Xiao-ming (2010) conducted a survey on “A study on image digital watermarking based on wavelet transform” this paper presents image digital watermarking process based on wavelet Transformation method. The embedding of the watermark in the selected areas this wavelet transformation method is very helpful. For the Embedding and the Extraction of the watermark this method will provide the efficiency. The quality of the data hiding will be increases by using wavelet transformation and computation complexity also reduced when it will compare with the Discrete Cosine Transformation (DCT). The major advantage of the using this method is the there is no loss of the data while in case of DCT the data will be lost due to the Quantization process.

Z J Xu, Z Z Wang, Q Lu (2011) conducted a survey on “Research on Image Watermarking Algorithm based on DCT” this paper presents DCT/IDCT method which is used for the Image Watermarking Algorithm. The length of the watermark will be decided on the number of rows of the Host Image. This method provides the Embedding and Extraction of the image watermark which gives the robust watermarking scheme. DCT provides lossy compression; the important data (watermark image) may be lost some times so this method is not suitable now a days. This issue is solved by using the Wavelet transformation method.

Baisa L Gunjal and Dr. Suresh N Mali (2012) conducted a survey on Applications of Digital Image Watermarking in Industries. This paper presents the some basics of digital watermarking and also explained about some of the applications, techniques that are widely used in digital watermarking. In case of Digital copyright protection system based on Remote Education and Health and car insurance companies. This paper also presents the various types of the techniques that are used to achieve secure and robust algorithm.

Anurag Mishra , Charu Agarwal , Arpita Sharma, Punam Bedi (2014) conducted a survey on “Optimized gray-scale image watermarking using DWT–SVD and Firefly Algorithm” this paper presents the three methods such as Discrete Wavelet Transformation(DWT), Singular value Decomposition(SVD) and Firefly Algorithm. The singular values Watermark image will be Embed in the singular values of the LL3

Decomposition of the Host Image. This gives the Robust Watermarking method and provides the security to the Watermark in the Host image. This algorithm is useful for the copyright protection. This existing Watermarking technique will be mainly focusing on two terms such as Robustness and Imperceptibility. Normally in digital watermarking the watermark should always remain with the Host image for this the existing system will provide robust algorithm. It can help to get the Robust Watermark Scheme. Digital watermarking contains two types of algorithms they are Embedding Algorithm and Extraction Algorithm.

CHAPTER 3

PRESENT WORK

Present work

i. The work has completed till embedding, extraction of the watermark image and extraction of original image. We worked on the grey scale images and RGB images and got the efficient results in those processes. This process has implemented in the Matlab 8.1.

ii. PSNR and NC values are calculated between watermark image and extracted watermark image for both grey scale images and the digital colour images and got the good PSNR and NC values for different watermark images such as (Bird, Cameraman, Baboon, Peppers, Barbara and Boat) but original image is Nature for every image.

iii. We calculated PSNR and NC values between original image and extracted original image (Nature). Here, we have calculated the results for both grey scale and digital colour images of Nature image. We get the good value of PSNR and NC for grey scale images and digital colour images.

iv. When we extracted the watermark and original image (for both gray scale and digital colour images) then we got original image was same as extracted original image and watermark image was same as extracted watermark image. So from this the data loss is very less after we will perform extraction process.

3.1 Scope of the Study

i. The proposed algorithm presents the two new methods such as rail fence and 10's complement and these will helps to achieve improved security watermarking scheme over the existing method.
ii. This proposed algorithm provides the efficient results on the attacks such as cryptographic attacks, active and passive attacks. This proposed method is useful in many areas such as copy right protection, tampering proofing, fingerprinting and medical fields.

iii. The proposed algorithm presents the WT and SVD methods the advantages of using these methods are there is no loss of the data and which provides robustness against the many watermarking attacks.

iv. The singular values are easily transmitted, so by using SVD method the transmission of data over network has done effectively.

v. This proposed system provides robust and secure scheme which is suitable for the copy right protection and the secure transmission.

3.2 Problem formulation

Digital watermarking has used in many areas. Digital watermarking has been popular topic for both researches and applications in the last 10 years. Now a day's multimedia technology has been grown very fast and for secure digital data transmission, need some special mechanisms like digital watermarking. In this digital watermark we can embed the image, audio, text and video (watermark data) into digital media (image, audio, text and video). The proposed method used the grey scale images (both for original and watermark image) and digital colour images (both for original and watermark image). But the problem with the existing system is, if the attacker known the two algorithms (DWT and SVD) then the watermark image will be easily identified by sometimes. In this case there is no secure algorithm is providing to the watermark before calculate the singular values of it. My problem is a hybrid approach which consist 10's complement and rail-fence methods in it and which provides the security to the image even after applying the brute-force attack on watermark image. In this case we have calculated PSNR and NC values after extraction process and we got good values of watermark image after the extraction process. When hacker performs brute force attack on the encrypted image after the extraction process then he won't able to get the original watermark image exactly and there will be a very huge loss of pixel values of it.

3.3 Objective of the Study

i. To get the robust watermarking scheme which works on images (invisible watermark) and gives the efficient results for the copy right protection (resist the active and passive attacks in transmission).

ii. To focus on a watermarking scheme that provides good quality of the image it has the good PSNR (Peak Signal to Noise Ratio) value. It provides security for the image even after applying image processing attacks on watermarking image.

iii. The existing system uses the DWT and SVD methods for the Embedding and the extraction of the watermark image. Which provide the security against the many attack and this is one of the robust approach.

iv. To improve the more security to the watermark image the proposed algorithm presents other two methods such as 10's complement, rail fence, DWT and SVD. 10's complement and rail fence methods are applied on the watermark image so that it will produce the encrypted image this is used to secure the watermark image from the active and passive attacks during the transmission.

v. Proposed algorithm will helps to secure the watermark image from the cryptographic attacks, active and passive attacks etc.

3.4 Research Methodology

The methodology in this proposal is to achieve the research is the hybrid approach. This approach presents the mixture of descriptive and exploratory methodologies. These two approaches are useful to achieve the good results in the research. The Exploratory approach is used for collecting the information about the techniques which are using in the image digital watermarking. From the above approach the collecting data will help to achieve good image watermarking techniques. Descriptive analysis is used to achieve the problems in the existing system it provides some methodology which help in solving the problems which are defined by the researcher. Descriptive and Exploratory approaches are used to solve the any type of problems which were produced by the researchers in the real world.

I. Proposed Embedding Algorithm

Step 1: First apply the 1-Level DWT method on the Host Image by using the HAAR Filter and obtain the LL1 sub band coefficients of it (Size of m×m).

Step 2: Then apply SVD method on the LL1 Sub band Coefficients of the Host image. To calculate it the formula is: [U, S, V] = SVD (LL1)

Step 3: Apply 10's Complement on the Watermark Image (w).

Step 4: Apply Rail fence method on that 10's Complemented Watermark Image and get the cipher Watermarked Image or Modified Watermark image (wc).

Step 5: Apply SVD method on the Watermark image (wc). To calculate it the formula is: [Uw, Sw, Vw] = SVD (wc)

Step 6: Embed singular values of wc into the singular values of the LL3 sub band (Embed Sw into S). To calculate it the formula is: S'=S+(δ*Sw)

Step 7: Get the Adapted LL1 Sub band coefficients LL1' by using the LL1' = (U * S' $*(V)^T$).

Step 8: Apply the 1- level IDWT method and to get the Watermarked Image.

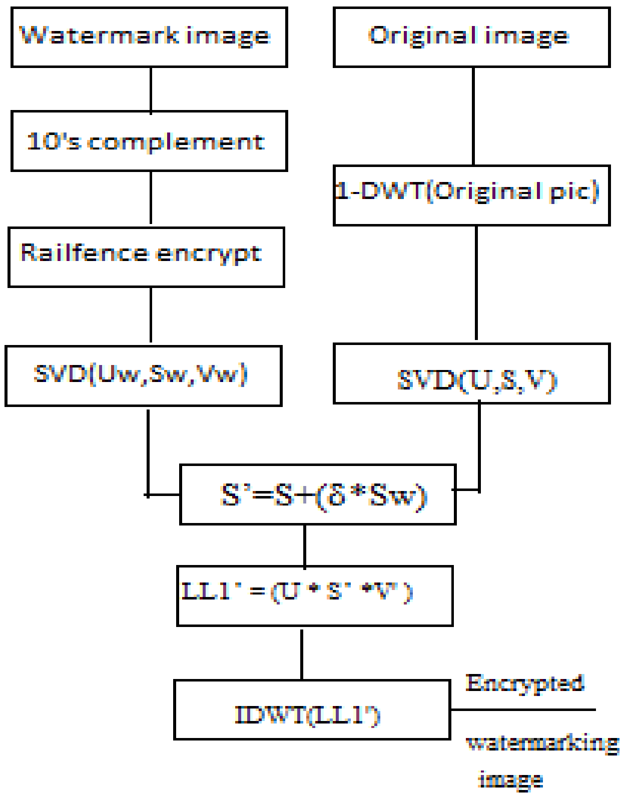


Figure 4: Proposed watermark embedding process

II. Proposed Extraction Algorithm

Step 1: Apply 1-level DWT method using the HAAR Filter on the Host Image i and the watermarked Image i' to get the LL1 and LL1' sub band Coefficients which consists the size of m×m.

LL1=DWT (i) and LL1'=DWT (I')

Step 2: Then apply SVD method on LL1 and LL1' Sub band Coefficients by using the formula:

[U, S, V] = SVD (LL1) and [U', S', V'] = SVD (LL1').

Step 3: Calculate the Singular values of the Watermark Image by Using

Swc' = [S' – S]/δ.

Step 4: Recover or Extract the Watermark by using this Formula:

wc' = Uw * Swc' * $(V)^T$

Step 5: Apply the Decryption of Rail fence to the wc'.

Step 6: Apply the Inverse of 10's to the above one and Extract the Watermark Image w'.

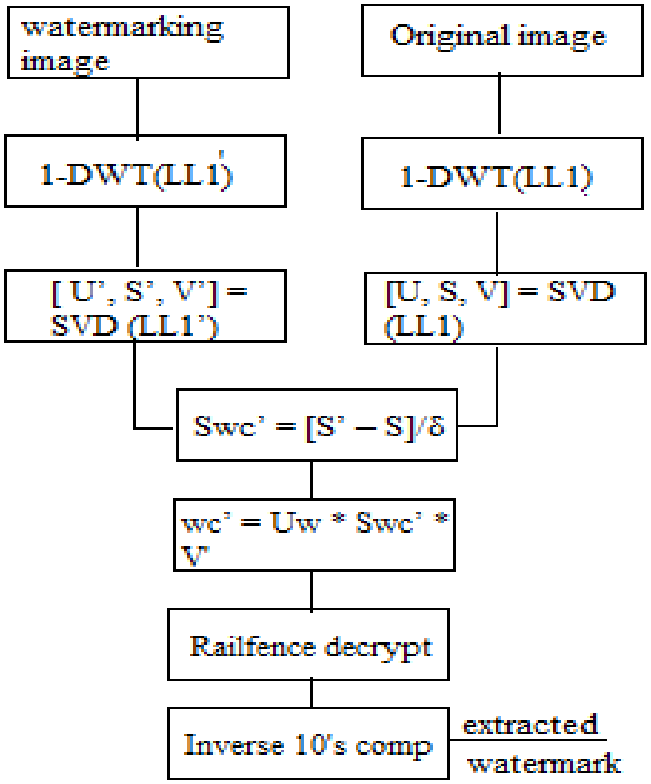


Figure 5: Proposed watermark extraction process

III. Process of original image extraction algorithm

The process of original image extraction is given below

Step1: Consider watermarking image (oi) and extracted watermark image (ew).

Step2: Apply 1-DWT on watermarking image and then apply SVD (LL1) sub band.

Step3: Apply 10's complement and rail-fence on extracted watermark image and got ew' then apply SVD (ew') of it.

Step4: Singular values of original image will be calculated by using the below formulae Snew=s(LL-1)-s(ew')* δ

Step5: Calculate, original-image=U*Snew*V'.

Step6: Apply IDWT (original-image) and it gives the Extracted original image.

CHAPTER 4

RESULT AND DISCUSSION

Result and Discussion

This proposed algorithm has implemented in the Matlab (8.1) version. The proposed method used the grey scale images (both for original and watermark image) and digital colour images (both for original and watermark image). In the both the cases it provided good results of PSNR (Peak signal noise ratio) and the NC (Normalized correlation). We have also observed that the proposed algorithm also provides the security as well as robustness. This proposed algorithm has applied on two types of the images such as grey scale images and digital colour images.

4.1 Grey scale images

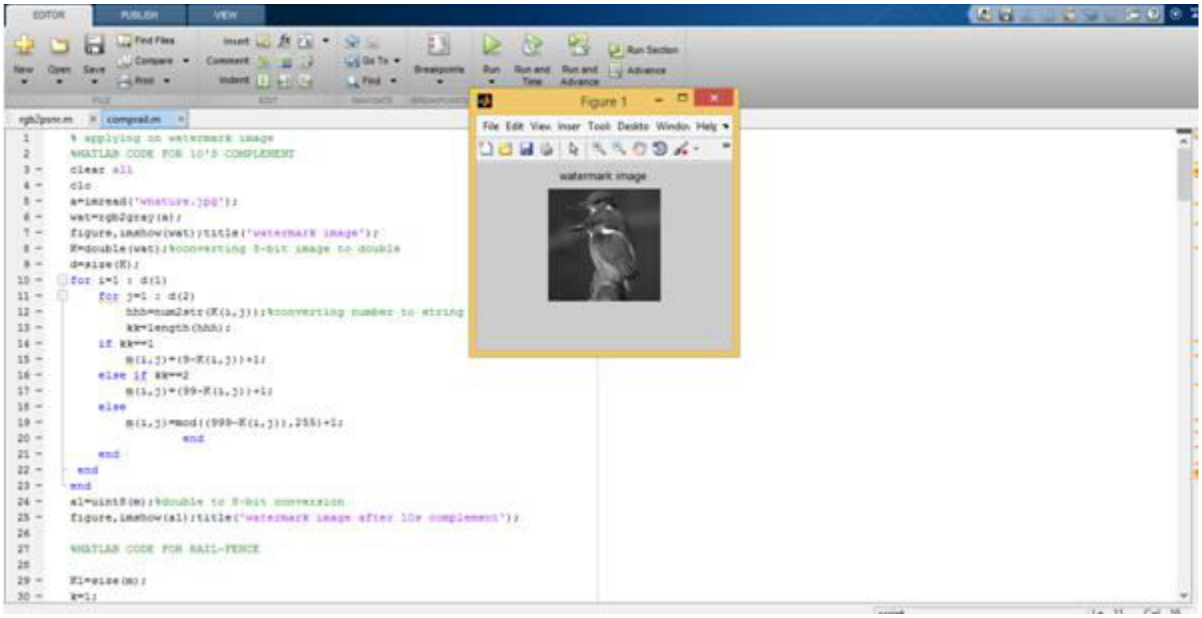
a. Watermark embedding algorithm on grey scale images

Consider 256×256 size original image and 128×128 size watermark image (both are grey scale images). First we performed 10's complement on the watermark images and it gave 10's complemented images. The range of grey scale image is 0-255. Whenever we will be performing 10's complement on the grey scale image some time it may exceed the range for example consider any pixel value as '100' by performing 10's complement on this it gives the result as 900. It has given the result which was not in the range so on such numbers we performed modulus operation with 255 so that the pixel value became within a range. Rail fence method applied on the 10's complement images and it gave encrypted image. After this we performed SVD of that image and we got the singular values of the encrypted watermark image. After completed this work we taken original image and we calculated LL-1 band of it by applied DWT. 'haar' filter has used for it. Calculated the SVD(LL-1) band and given the singular values. The encrypted watermark image singular values embedded in LL-1 singular and gave the new singular values (snew) by using the formulae snew=s+(δ *sw). After this we performed U*snew*V' will gives the inverse of SVD. Whenever we performed IDWT on this images will gives the watermarking image.

Let us consider original image as Nature and watermark image as Bird.

b. Watermark Extraction algorithm on grey scale images

We considered the original image and watermarking image for the extraction of the watermark image. First we calculated DWT of the both the images will gives the LL1 (original-image) and LL-1 (watermarking image). We calculated the singular values of the both the LL1 band images. S1=singular values of original image (LL1) and S2=singular values of watermarking image (LL1). Snew=(S2-S1)/ δ from this formula we grab the new singular values of watermark image (encypted). Then we applied inverse operation of rail-fence and inverse of 10's complement it given the extracted watermark image with good visibility.

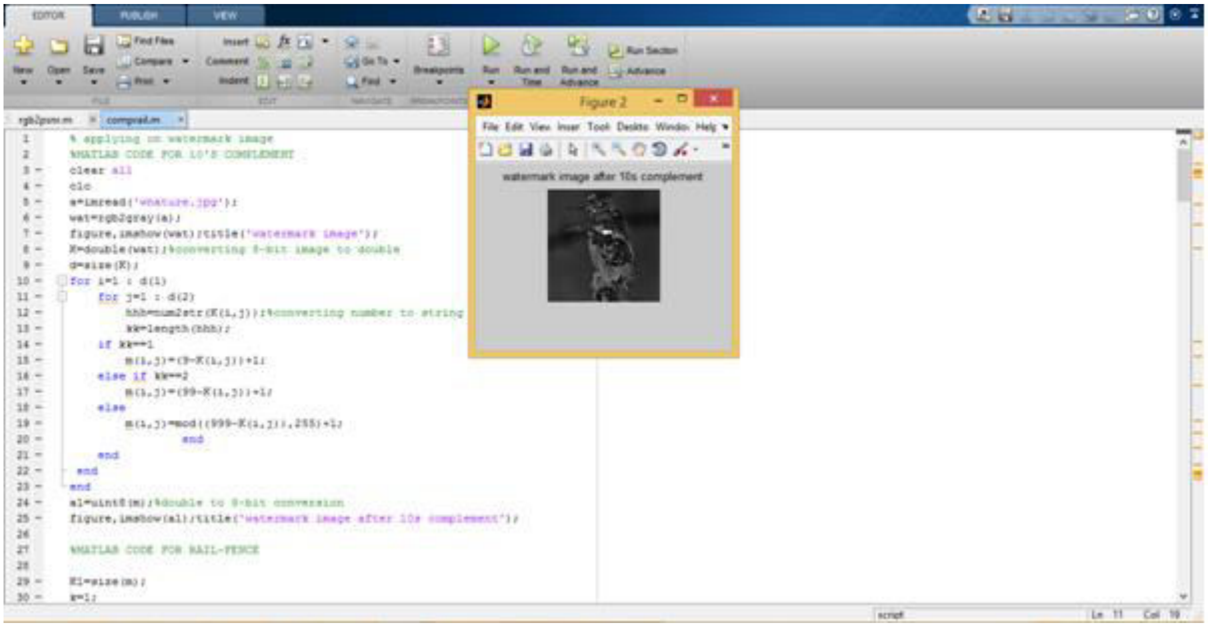


```
% applying on watermark image
%MATLAB CODE FOR 10'S COMPLEMENT
clear all
clc
a=imread('wnature.jpg');
wat=rgb2grey(a);
figure,imshow(wat);title('watermark image');
K=double(wat);%converting 8-bit image to double
d=size(K);
for i=1 : d(1)
    for j=1 : d(2)
        hhh=num2str(K(i,j));%converting number to string
        kk=length(hhh);
    if kk==1
        m(i,j)=(9-K(i,j))+1;
    else if kk==2
        m(i,j)=(99-K(i,j))+1;
    else
        m(i,j)=mod((999-K(i,j)),255)+1;
              end
    end
 end
end
a1=uint8(m);%double to 8-bit conversion
figure,imshow(a1);title('watermark image after 10s complement');

%MATLAB CODE FOR RAIL-FENCE

K1=size(m);
k=1;
```

Figure 6: Grey scale watermark image

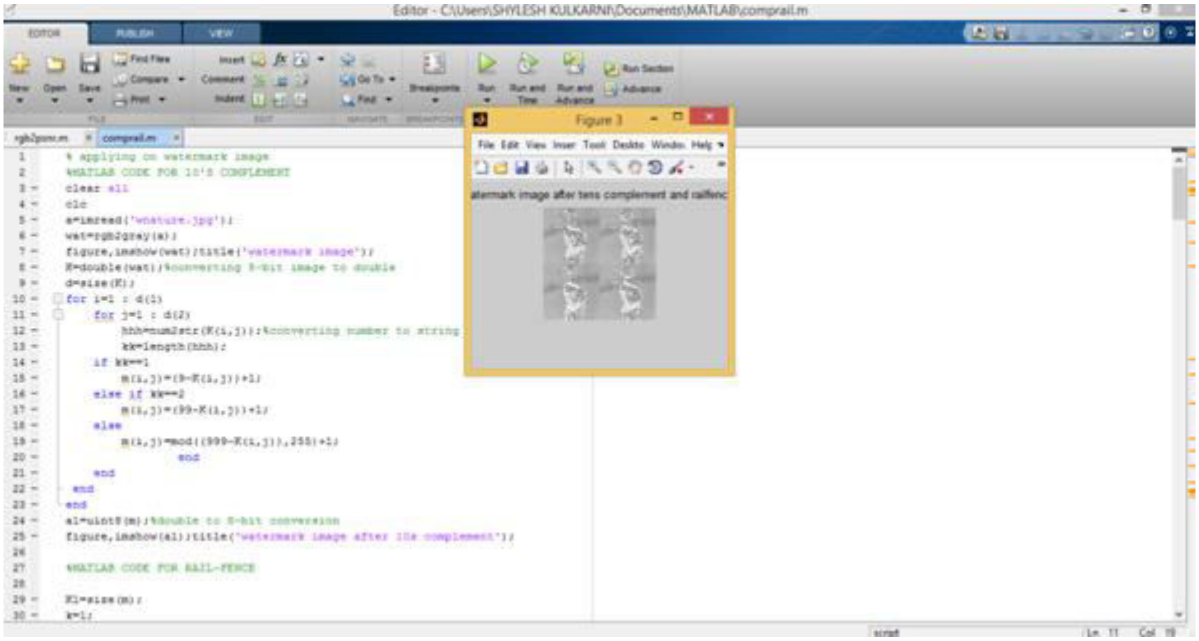


```
% applying on watermark image
%MATLAB CODE FOR 10'S COMPLEMENT
clear all
clc
a=imread('wnature.jpg');
wat=rgb2gray(a);
figure,imshow(wat);title('watermark image');
K=double(wat);%converting 8-bit image to double
d=size(K);
for i=1 : d(1)
    for j=1 : d(2)
        hhh=num2str(K(i,j));%converting number to string
        kk=length(hhh);
    if kk==1
        m(i,j)=(9-K(i,j))+1;
    else if kk==2
        m(i,j)=(99-K(i,j))+1;
    else
        m(i,j)=mod((999-K(i,j)),255)+1;
            end
    end
 end
end
a1=uint8(m);%double to 8-bit conversion
figure,imshow(a1);title('watermark image after 10s complement');

%MATLAB CODE FOR RAIL-FENCE

K1=size(m);
k=1;
```

Figure 7: 10's complemented watermark image

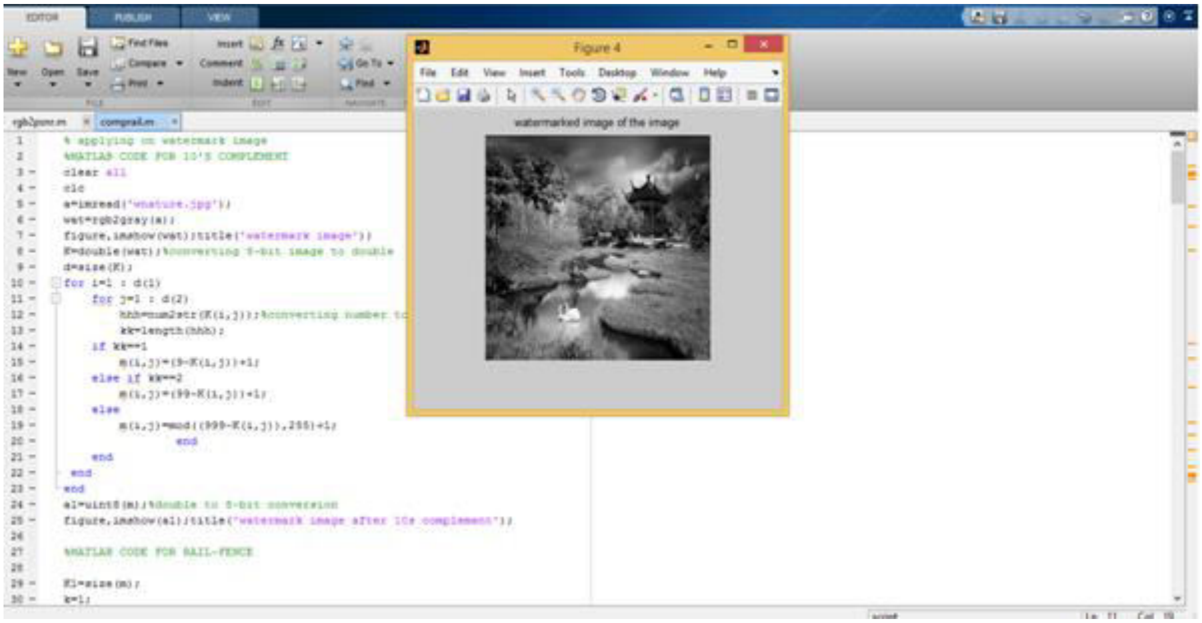


```
% applying on watermark image
%MATLAB CODE FOR 10'S COMPLEMENT
clear all
clc
a=imread('wnature.jpg');
wat=rgb2gray(a);
figure,imshow(wat);title('watermark image');
K=double(wat);%converting 8-bit image to double
d=size(K);
for i=1 : d(1)
    for j=1 : d(2)
        hhh=num2str(K(i,j));%converting number to string
        kk=length(hhh);
    if kk==1
        m(i,j)=(9-K(i,j))+1;
    else if kk==2
        m(i,j)=(99-K(i,j))+1;
    else
        m(i,j)=mod((999-K(i,j)),255)+1;
            end
    end
 end
end
a1=uint8(m);%double to 8-bit conversion
figure,imshow(a1);title('watermark image after 10s complement');

%MATLAB CODE FOR RAIL-FENCE

K1=size(m);
k=1;
```

Figure 8: Rail-fence encryption on 10's complemented watermark image

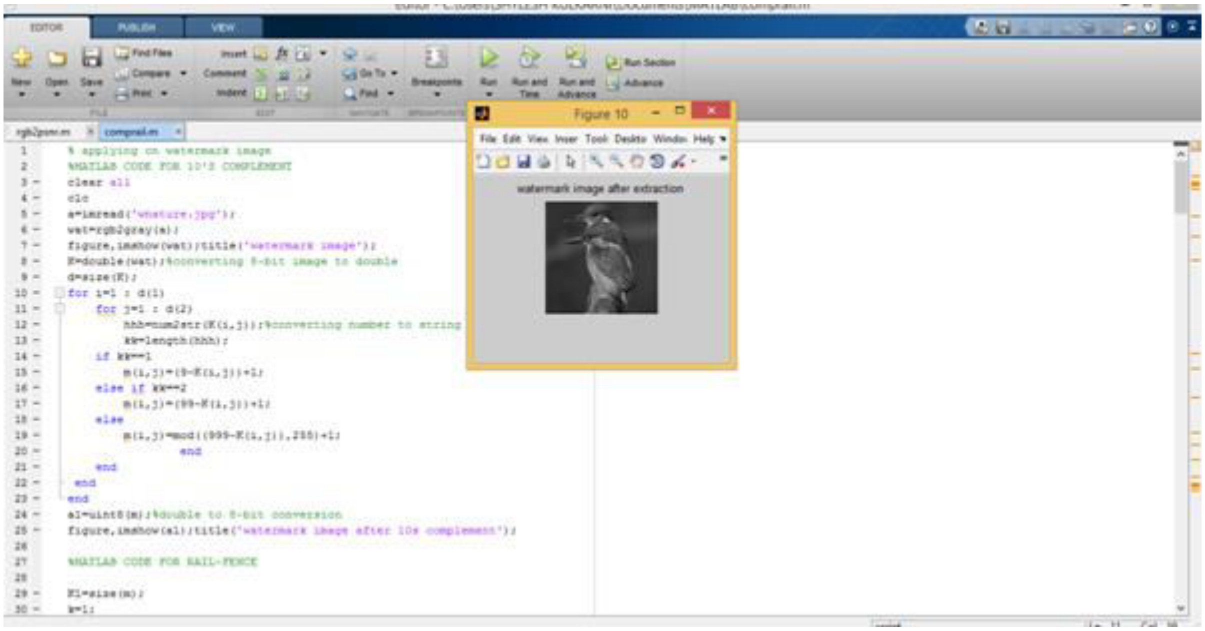


```
% applying on watermark image
%MATLAB CODE FOR 10'S COMPLEMENT
clear all
clc
a=imread('wnature.jpg');
wat=rgb2gray(a);
figure,imshow(wat);title('watermark image'));
K=double(wat);%converting 8-bit image to double
d=size(K);
for i=1 : d(1)
    for j=1 : d(2)
        hhh=num2str(K(i,j));%converting number to
        kk=length(hhh);
    if kk==1
        m(i,j)=(9-K(i,j))+1;
    else if kk==2
        m(i,j)=(99-K(i,j))+1;
    else
        m(i,j)=mod((999-K(i,j)),255)+1;
                end
    end
 end
end
a1=uint8(m);%double to 8-bit conversion
figure,imshow(a1);title('watermark image after 10s complement');

%MATLAB CODE FOR RAIL-FENCE

K1=size(m);
k=1;
```

Figure 9: watermarking image

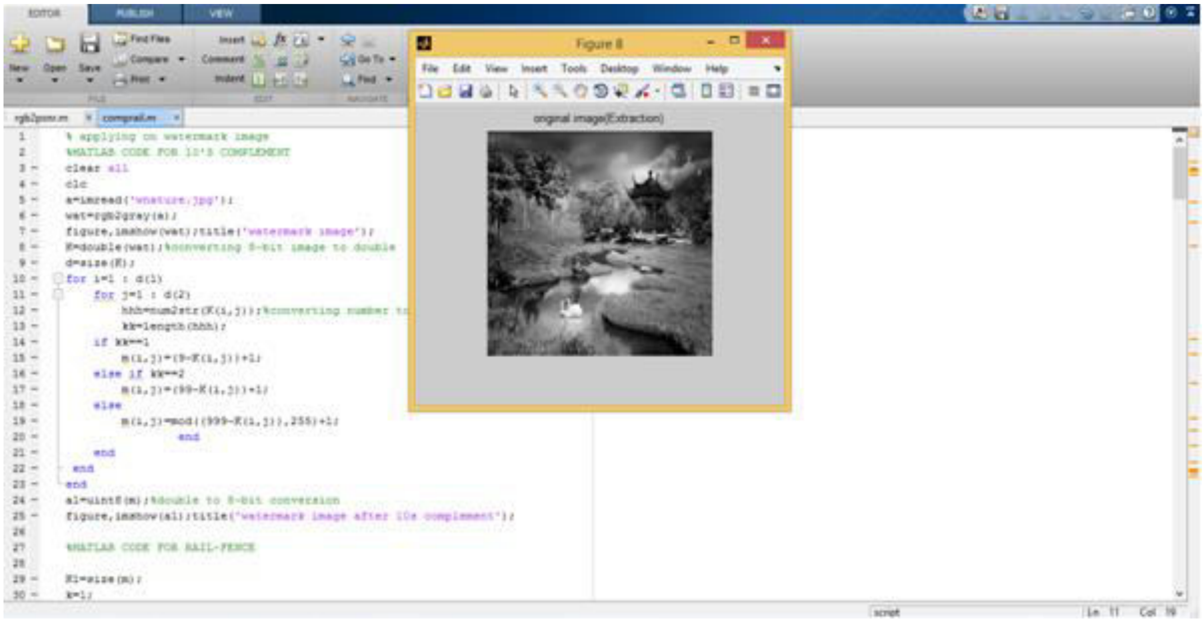


```
% applying on watermark image
%MATLAB CODE FOR 10'S COMPLEMENT
clear all
clc
a=imread('wnature.jpg');
wat=rgb2gray(a);
figure,imshow(wat);title('watermark image');
K=double(wat);%converting 8-bit image to double
d=size(K);
for i=1 : d(1)
    for j=1 : d(2)
        hhh=num2str(K(i,j));%converting number to string
        kk=length(hhh);
    if kk==1
        m(i,j)=(9-K(i,j))+1;
    else if kk==2
        m(i,j)=(99-K(i,j))+1;
    else
        m(i,j)=mod((999-K(i,j)),255)+1;
                end
    end
 end
end
a1=uint8(m);%double to 8-bit conversion
figure,imshow(a1);title('watermark image after 10s complement');

%MATLAB CODE FOR RAIL-FENCE

K1=size(m);
k=1;
```

Figure 10: Extracted watermark image



```
% applying on watermark image
%MATLAB CODE FOR 10'S COMPLEMENT
clear all
clc
a=imread('wnature.jpg');
wat=rgb2gray(a);
figure,imshow(wat);title('watermark image');
K=double(wat);%converting 8-bit image to double
d=size(K);
for i=1 : d(1)
    for j=1 : d(2)
        hhh=num2str(K(i,j));%converting number t
        kk=length(hhh);
    if kk==1
        m(i,j)=(9-K(i,j))+1;
    else if kk==2
        m(i,j)=(99-K(i,j))+1;
    else
        m(i,j)=mod((999-K(i,j)),255)+1;
              end
    end
 end
end
a1=uint8(m);%double to 8-bit conversion
figure,imshow(a1);title('watermark image after 10s complement');

%MATLAB CODE FOR RAIL-FENCE

K1=size(m);
k=1;
```

Figure 11: Extracted original image

The above results showed that, this proposed method provided robustness (watermark image and extracted watermark image are same) and as well as security (by using 10's complement and rail-fence method). This proposed method has also been applied on various images such as Baboon, Boat, Cameraman, Bird, Barbara and Peppers and got good results in case of PSNR and NC. Nature image is original image for every image**.**

c. PSNR and NC values

In case of PSNR and NC we can't compare the proposed method with existing method because of change in the data set. The existing method had used grey scale image for original image and black and white image for watermark image but the proposed method used the grey scale images (both for original and watermark image) and digital colour images(both for original and watermark image). But still the proposed method provided good PSNR and NC values.

Table1: PSNR and NC(w,w') values (For grey scale images).

image	δ=0.05	δ=0.005	δ=0.1

Nature with Baboon	PSNR=35.00
	NC=0.95
		PSNR=39.00
		NC=0.97
			PSNR=40.12
			NC=0.98

Nature with Boat	PSNR=39.12
	NC=0.98
		PSNR=36.35
		NC=0.96
			PSNR=39.00
			NC=0.978

Nature with Camera-man	PSNR=35.24
	NC=0.967
		PSNR=37.56
		NC=0.971
			PSNR=39.02
			NC=0.98

Nature with Bird	PSNR=37.00
	NC=0.97
		PSNR=36.01
		NC=0.96
			PSNR=39.12
			NC=0.99

Nature with Barbara	PSNR=38.00
	NC=0.98
		PSNR=39.23
		NC=0.988
			PSNR=40.23
			NC=0.999

Nature with Peppers	PSNR=35.24
	NC=0.967
		PSNR=34.78
		NC=0.957
			PSNR=36.22
			NC=0.96

From the above figure it has been concluded that when the δ values is 0.1 proposed method has given good PSNR and NC values. This proposed method also showed that it provided robustness from the above results. The loss of data is very less in the proposed method.

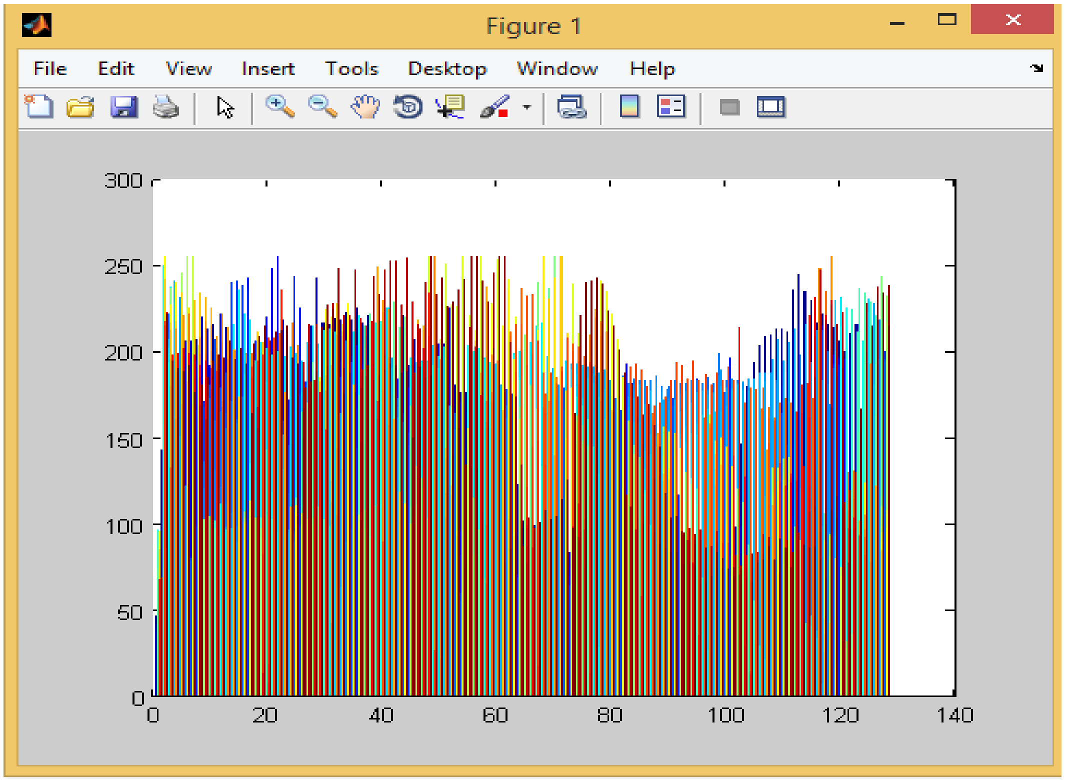


Figure 12: watermark (bird) image bar chart

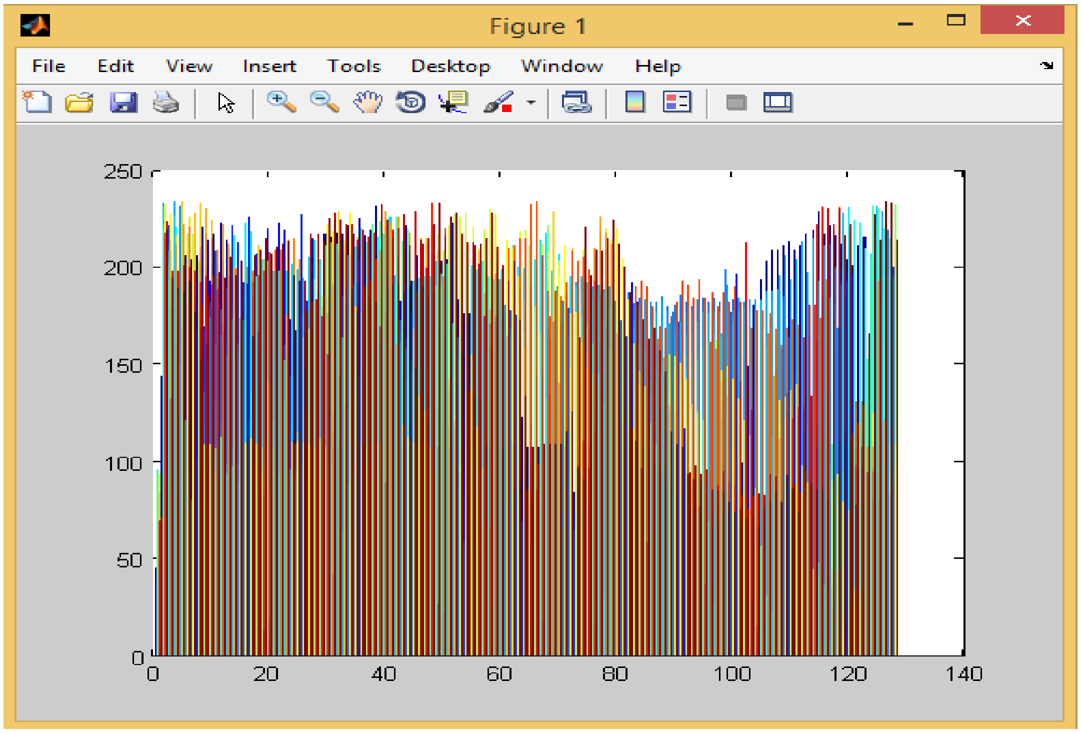
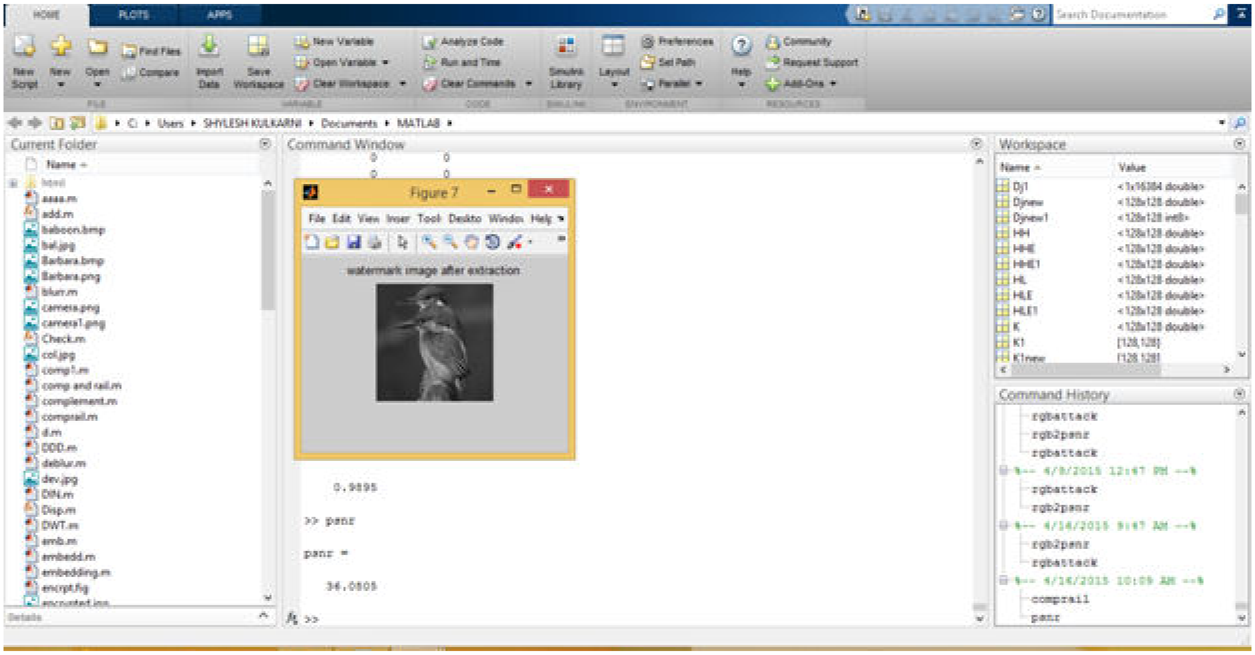


Figure 13: watermark image (bird) after extraction bar chart

From the above two figure we observed that after completion of the watermark extraction the loss of data is very less which is negligible.

Suppose an intruder wants to extract the watermark image, he will try to apply most used methods such as DWT, SVD on the watermarking image then he gets an image (w/o inverse operation of rail-fence and 10's complement algorithm). After this process he will try to apply the rail-fence inverse algorithm he will other image (w1) (w/o inverse of 10's complement). When he see the pixel values of the image he may conclude that this algorithm would be 10's complement if suppose if he applies directly inverse 10's complement algorithm on based on the available image data(w1) then this hacker can't get the original data of the image. After this type of attack we will get our output as follows:



Current Folder

```
Name
html
aaaa.m
add.m
baboon.bmp
bal.jpg
Barbara.bmp
Barbara.png
blur.m
camera.png
camera1.png
Check.m
col.jpg
comp1.m
comp and rail.m
complement.m
comprail.m
d.m
DDD.m
deblur.m
dev.jpg
DIN.m
Disp.m
DWT.m
emb.m
embedd.m
embedding.m
encrpt.fig
encrypted.jpg
```

Command Window

```
      0         0
      0         0

   0.9895

>> psnr

psnr =

   36.0805

>>
```

Workspace

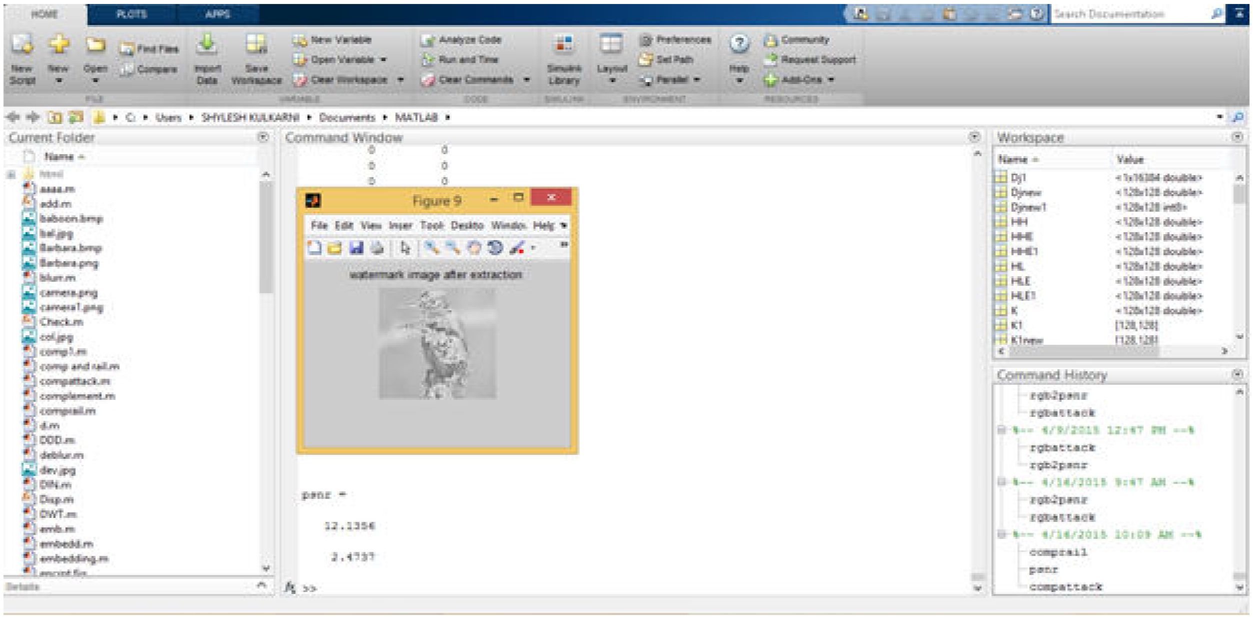
Name	Value
Dj1	<1x16384 double>
Djnew	<128x128 double>
Djnew1	<128x128 int8>
HH	<128x128 double>
HHE	<128x128 double>
HHE1	<128x128 double>
HL	<128x128 double>
HLE	<128x128 double>
HLE1	<128x128 double>
K	<128x128 double>
K1	[128,128]
K1new	[128,128]

Command History

```
  rgbattack
  rgb2psnr
  rgbattack
%-- 4/8/2015 12:47 PM --%
  rgbattack
  rgb2psnr
%-- 4/14/2015 9:47 AM --%
  rgb2psnr
  rgbattack
%-- 4/16/2015 10:09 AM --%
  comprail
  psnr
```

Figure 14: watermark image after extraction (on grey scale)

In the above we are considering grey scale peppers watermark image. After extracting the image we will get the watermark image without loss. It is having good PSNR value which is equal to 45.37 and good NC value which is 1.0004. So from the above figure we can conclude that data loss is very less.



```
        0         0
        0         0
        0         0

psnr =

   12.1356

    2.4737

>>
```

Name	Value
Dj1	<1x16384 double>
Djnew	<128x128 double>
Djnew1	<128x128 int8>
HH	<128x128 double>
HHE	<128x128 double>
HHE1	<128x128 double>
HL	<128x128 double>
HLE	<128x128 double>
HLE1	<128x128 double>
K	<128x128 double>
K1	[128,128]
K1new	[128,128]

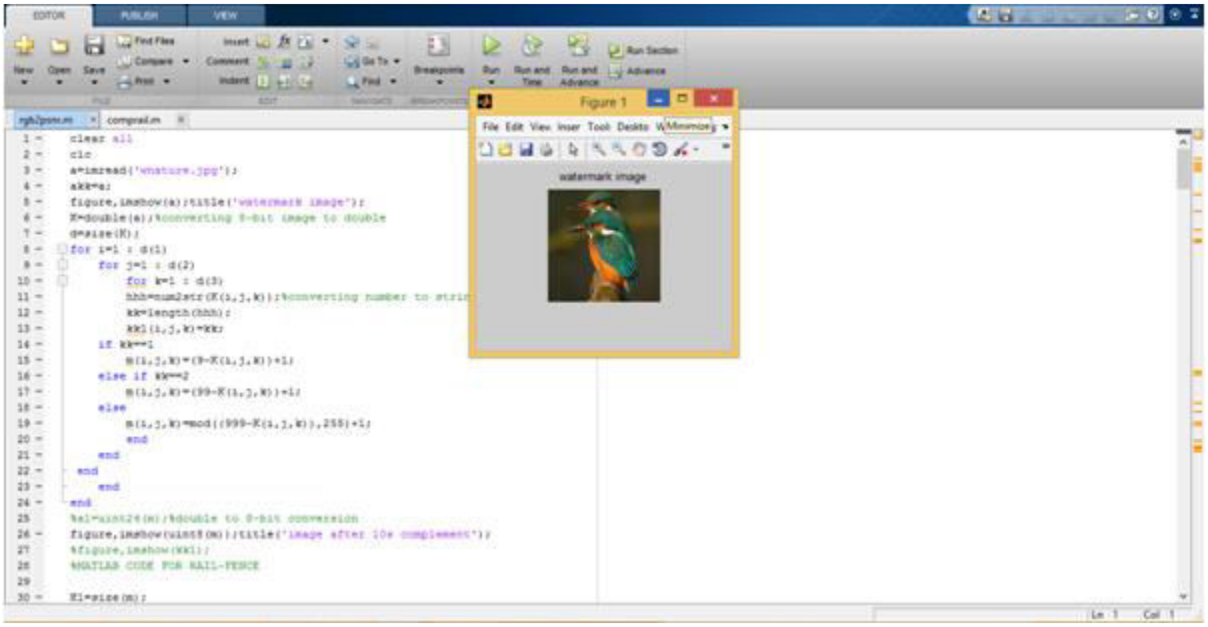
```
   rgb2psnr
   rgbattack
%-- 4/9/2015 12:47 PM --%
   rgbattack
   rgb2psnr
%-- 4/14/2015 9:47 AM --%
   rgb2psnr
   rgbattack
%-- 4/14/2015 10:09 AM --%
   comprail
   psnr
   compattack
```

Figure 15: watermark extraction by attacker (grey scale image)

If hacker wants to extract the watermark but he won't get the exact image because of lack in the idea of inverse 10's complement algorithm. If suppose an attacker extracted the watermark image (by his own inverse 10's complement algorithm) then it produces the image with huge loss of pixel value and it is giving just 12.50 of PSNR value. So it is one of the advantage of the proposed method hacker can't easy to get the original watermark image. This attack is the example of brute force attack.

4.2 Digital colour images

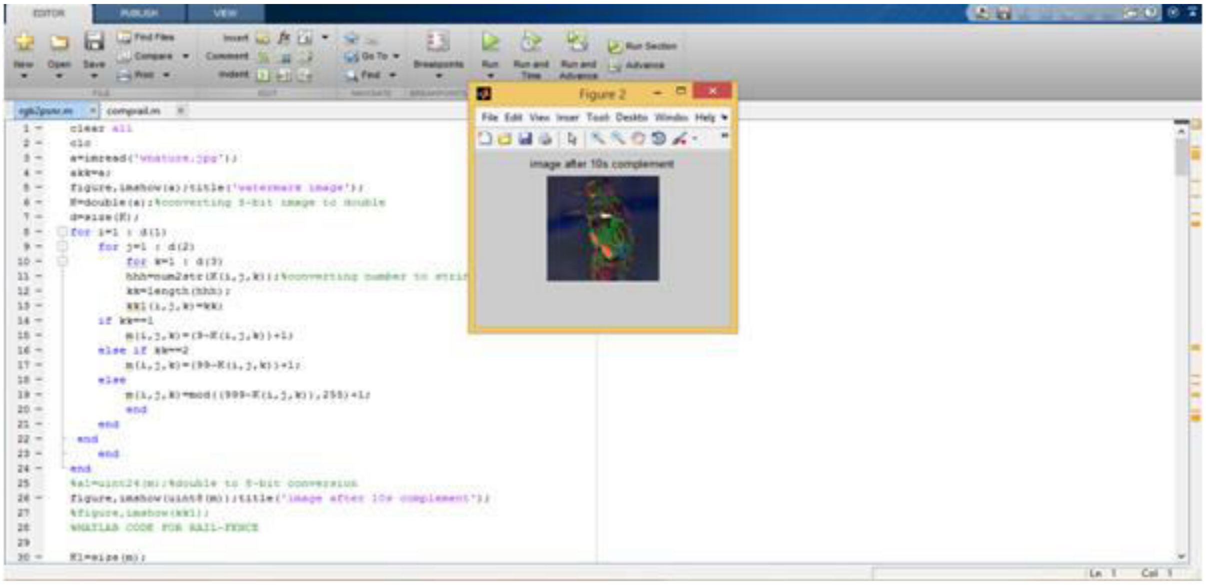
The process of embedding and extraction in grey scale images and digital colour images are same only but grey scale images in two dimensional where as digital colour images has three dimensional data. The time complexity and space complexity of the digital colour images are more when it has compared with grey scale images. When we have performed 10's complement then we applied modular operation (with 255) on the pixel value which has more than 255. By this the complexity of the process will reduces. Remaining all process of this embedding and extraction of digital colour images same as grey scale images (same as the above).



```
clear all
clc
a=imread('whature.jpg');
akk=a;
figure,imshow(a);title('watermark image');
K=double(a);%converting 8-bit image to double
d=size(K);
for i=1 : d(1)
    for j=1 : d(2)
        for k=1 : d(3)
        hhh=num2str(K(i,j,k));%converting number to strin
        kk=length(hhh);
        kk1(i,j,k)=kk;
    if kk==1
        m(i,j,k)=(9-K(i,j,k))+1;
    else if kk==2
        m(i,j,k)=(99-K(i,j,k))+1;
    else
        m(i,j,k)=mod((999-K(i,j,k)),255)+1;
        end
    end
 end
    end
end
%a1=uint24(m);%double to 8-bit conversion
figure,imshow(uint8(m));title('image after 10s complement');
%figure,imshow(kk1);
%MATLAB CODE FOR RAIL-FENCE

K1=size(m);
```

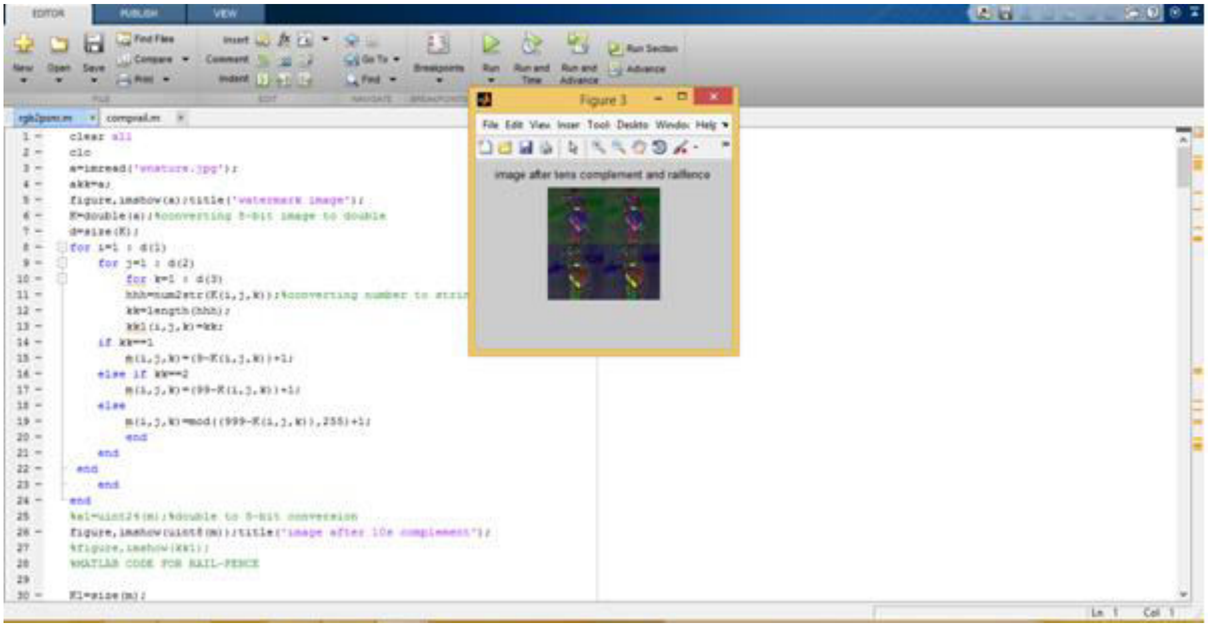
Figure 16: digital colour watermark image



```
clear all
clc
a=imread('whature.jpg');
akk=a;
figure,imshow(a);title('watermark image');
K=double(a);%converting 8-bit image to double
d=size(K);
for i=1 : d(1)
    for j=1 : d(2)
        for k=1 : d(3)
        hhh=num2str(K(i,j,k));%converting number to strin
        kk=length(hhh);
        kk1(i,j,k)=kk;
    if kk==1
        m(i,j,k)=(9-K(i,j,k))+1;
    else if kk==2
        m(i,j,k)=(99-K(i,j,k))+1;
    else
        m(i,j,k)=mod((999-K(i,j,k)),255)+1;
        end
    end
 end
    end
end
%a1=uint24(m);%double to 8-bit conversion
figure,imshow(uint8(m));title('image after 10s complement');
%figure,imshow(kk1);
%MATLAB CODE FOR RAIL-FENCE

K1=size(m);
```

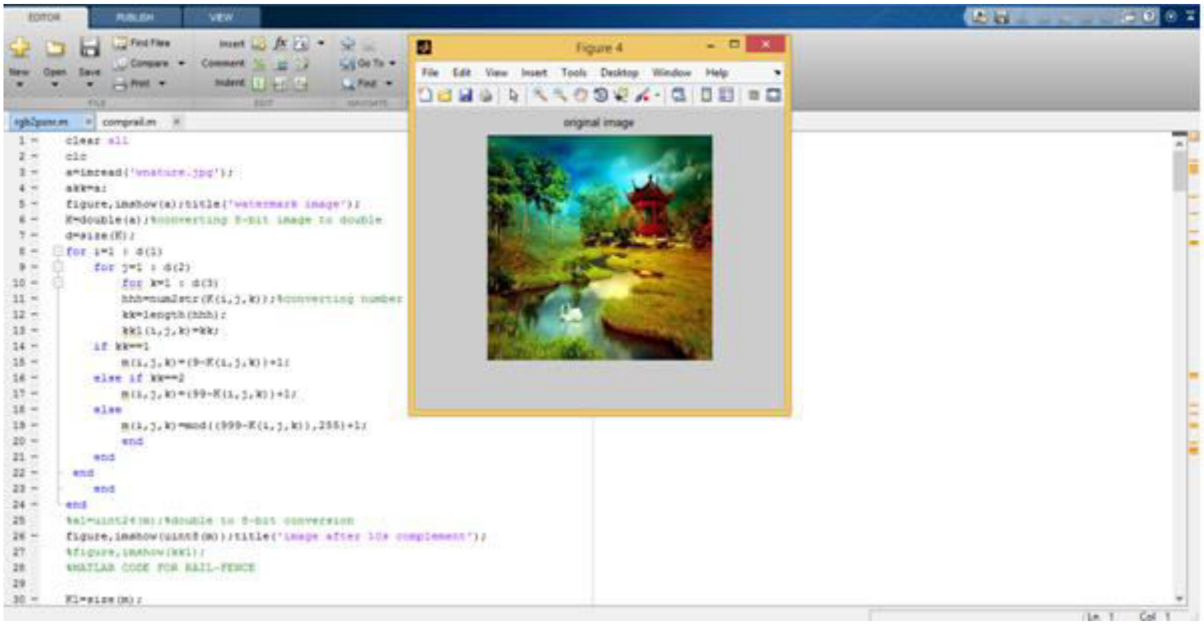
Figure 17: 10's complemented watermark image



```
clear all
clc
a=imread('wnature.jpg');
akk=a;
figure,imshow(a);title('watermark image');
K=double(a);%converting 8-bit image to double
d=size(K);
for i=1 : d(1)
    for j=1 : d(2)
        for k=1 : d(3)
        hhh=num2str(K(i,j,k));%converting number to strin
        kk=length(hhh);
        kk1(i,j,k)=kk;
    if kk==1
        m(i,j,k)=(9-K(i,j,k))+1;
    else if kk==2
        m(i,j,k)=(99-K(i,j,k))+1;
    else
        m(i,j,k)=mod((999-K(i,j,k)),255)+1;
        end
    end
 end
    end
end
%a1=uint24(m);%double to 8-bit conversion
figure,imshow(uint8(m));title('image after 10s complement');
%figure,imshow(kk1);
%MATLAB CODE FOR RAIL-FENCE

K1=size(m);
```

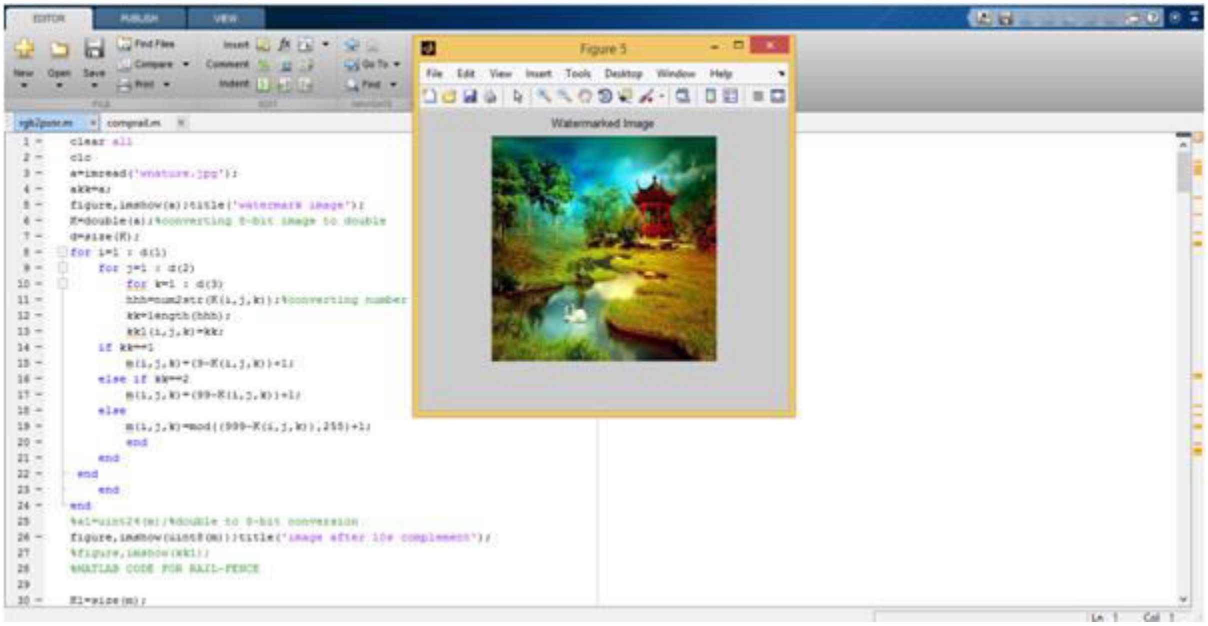
Figure 18: Rail-fence encryption on 10's complemented watermark image



```
clear all
clc
a=imread('wnature.jpg');
akk=a;
figure,imshow(a);title('watermark image');
K=double(a);%converting 8-bit image to double
d=size(K);
for i=1 : d(1)
    for j=1 : d(2)
        for k=1 : d(3)
        hhh=num2str(K(i,j,k));%converting number
        kk=length(hhh);
        kk1(i,j,k)=kk;
    if kk==1
        m(i,j,k)=(9-K(i,j,k))+1;
    else if kk==2
        m(i,j,k)=(99-K(i,j,k))+1;
    else
        m(i,j,k)=mod((999-K(i,j,k)),255)+1;
        end
    end
 end
    end
end
%a1=uint24(m);%double to 8-bit conversion
figure,imshow(uint8(m));title('image after 10s complement');
%figure,imshow(kk1);
%MATLAB CODE FOR RAIL-FENCE

K1=size(m);
```

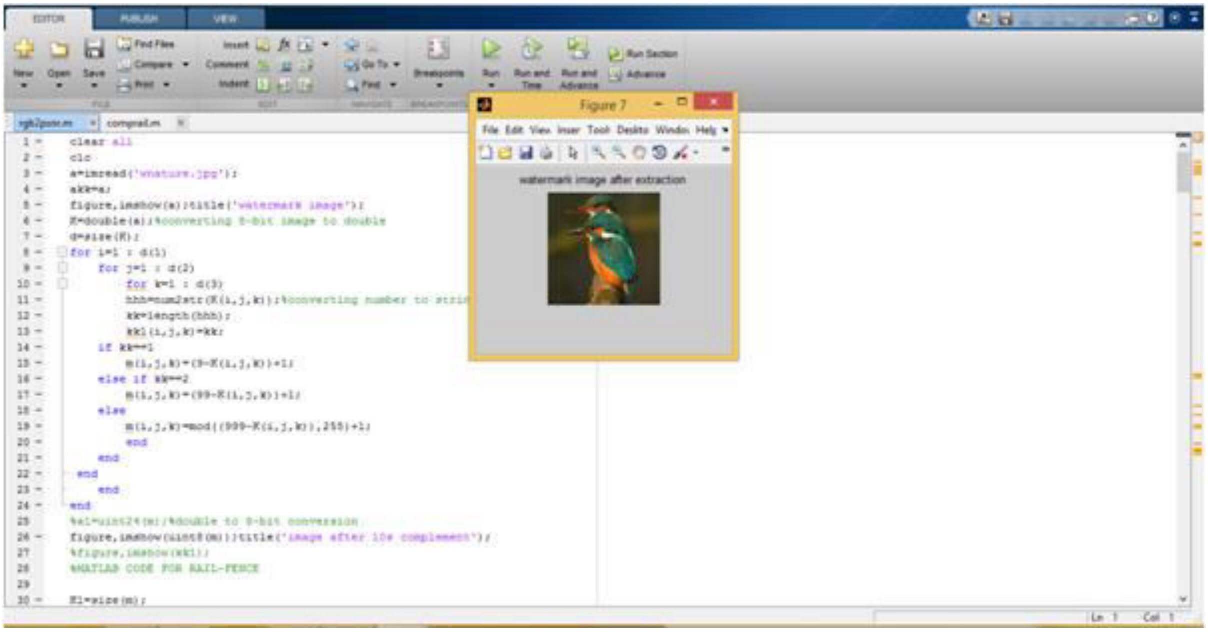
Figure 19: Original image



```
clear all
clc
a=imread('wnature.jpg');
akk=a;
figure,imshow(a);title('watermark image');
K=double(a);%converting 8-bit image to double
d=size(K);
for i=1 : d(1)
    for j=1 : d(2)
        for k=1 : d(3)
        hhh=num2str(K(i,j,k));%converting number
        kk=length(hhh);
        kk1(i,j,k)=kk;
    if kk==1
        m(i,j,k)=(9-K(i,j,k))+1;
    else if kk==2
        m(i,j,k)=(99-K(i,j,k))+1;
    else
        m(i,j,k)=mod((999-K(i,j,k)),255)+1;
        end
    end
 end
    end
end
%a1=uint8(m);%double to 8-bit conversion
figure,imshow(uint8(m));title('image after 10s complement');
%figure,imshow(kk1);
%MATLAB CODE FOR RAIL-FENCE

K1=size(m);
```

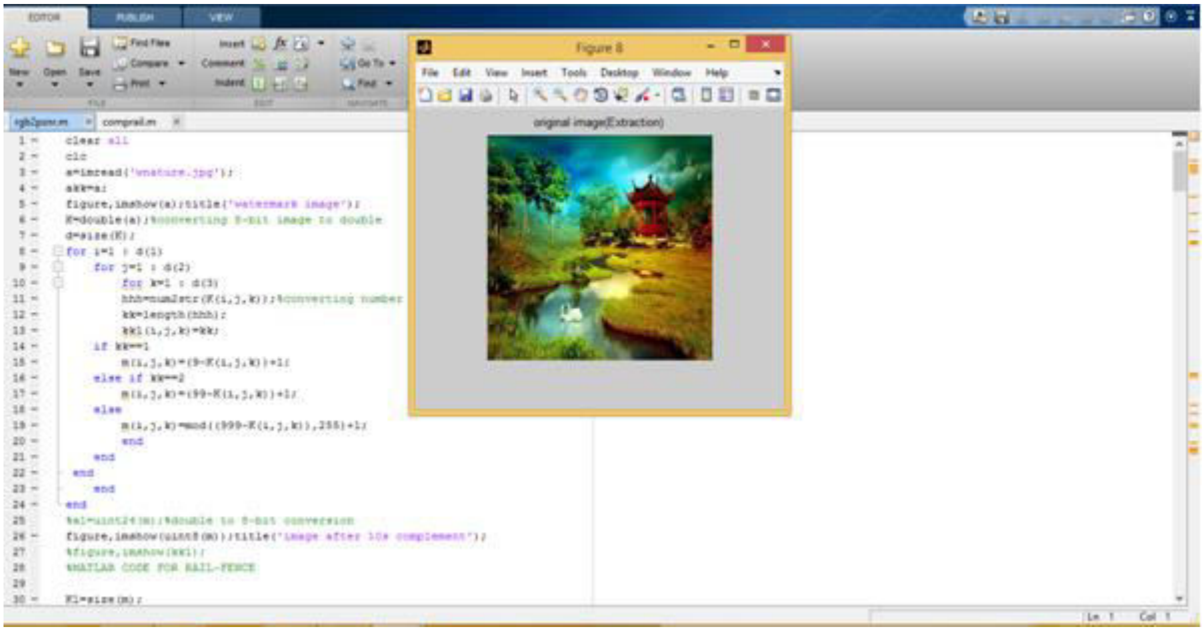
Figure 20: Watermarking image



```
clear all
clc
a=imread('wnature.jpg');
akk=a;
figure,imshow(a);title('watermark image');
K=double(a);%converting 8-bit image to double
d=size(K);
for i=1 : d(1)
    for j=1 : d(2)
        for k=1 : d(3)
        hhh=num2str(K(i,j,k));%converting number to stri
        kk=length(hhh);
        kk1(i,j,k)=kk;
    if kk==1
        m(i,j,k)=(9-K(i,j,k))+1;
    else if kk==2
        m(i,j,k)=(99-K(i,j,k))+1;
    else
        m(i,j,k)=mod((999-K(i,j,k)),255)+1;
        end
    end
 end
    end
end
%a1=uint8(m);%double to 8-bit conversion
figure,imshow(uint8(m));title('image after 10s complement');
%figure,imshow(kk1);
%MATLAB CODE FOR RAIL-FENCE

K1=size(m);
```

Figure 21: Watermark image after extraction process



```
clear all
clc
a=imread('wnature.jpg');
akk=a;
figure,imshow(a);title('watermark image');
K=double(a);%converting 8-bit image to double
d=size(K);
for i=1 : d(1)
    for j=1 : d(2)
        for k=1 : d(3)
        hhh=num2str(K(i,j,k));%converting number
        kk=length(hhh);
        kk1(i,j,k)=kk;
    if kk==1
        m(i,j,k)=(9-K(i,j,k))+1;
    else if kk==2
        m(i,j,k)=(99-K(i,j,k))+1;
    else
        m(i,j,k)=mod((999-K(i,j,k)),255)+1;
        end
    end
  end
    end
end
%a1=uint24(m);%double to 8-bit conversion
figure,imshow(uint8(m));title('image after 10s complement');
%figure,imshow(kk1);
%MATLAB CODE FOR RAIL-FENCE

K1=size(m);
```

Figure 22: Original image after extraction

The above figure has shown that the watermark has extracted without less amount of loss. So this algorithm has also been worked efficient for digital colour images. It's also provided good PSNR and NC results.

This is the formula to calculate the PSNR value:

PSNR=10 $\log_{10}(\frac{\text{Imax}^2}{\text{MSE}})$ where Imax is the maximum possible pixel value of the Image 'I' and MSE is the Mean Square Error. If the value of the PSNR is more, then the quality of the image is more and the less in the Error rate of the image.

To calculate the Normalized cross correlation (NC) the formula is:

$$\text{NC (w, w')} = \frac{\sum_{i=0}^{m} \quad \sum_{j=0}^{n}[w(i,j), w'(i,j)]}{\sum_{i=0}^{m} \quad \sum_{j=0}^{n}[wc(i,j) * wc(i,j)]}$$

Where w(i,j) is original watermark image and w'(i,j) is the extracted image.

a. PSNR and NC values

Table2: PSNR and NC (w,w') values (For digital colour images) where Nature is the original image.

Image	δ=0.05	δ=0.005	δ=0.1

Nature with Baboon	PSNR=42.22
	NC=0.98
		PSNR=42.15
		NC=0.97
			PSNR=44.14
			NC=0.99

Nature with Boat	PSNR=39.12
	NC=0.96
		PSNR=44.14
		NC=0.99
			PSNR=43.33
			NC=0.98

Nature with Camera-man	PSNR=41.22
	NC=0.98
		PSNR=43.15
		NC=0.98
			PSNR=40.25
			NC=0.97

Nature with bird	PSNR=44.10
	NC=0.99
		PSNR=43.90
		NC=0.989
			PSNR=42.14
			NC=0.998

Nature with Barbara	PSNR=43.65
	NC=0.99
		PSNR=39.54
		NC=0.96
			PSNR=41.32
			NC=0.98

Nature with Peppers	PSNR=44.12
	NC=0.998
		PSNR=43.65
		NC=0.99
			PSNR=39.69
			NC=0.96

From the above figure it has been concluded that when the δ values is 0.1 proposed method has given good PSNR and NC values. This proposed method also showed that it provided robustness from the above results. The loss of data is very less in the proposed method.

4.3 Extraction of the original image (Digital colour image)

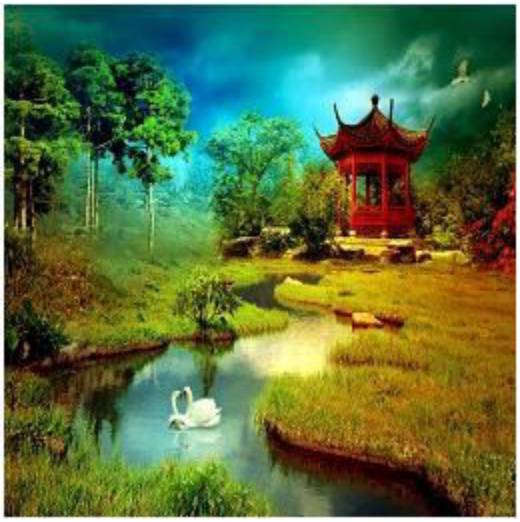


Figure 23: Nature original image

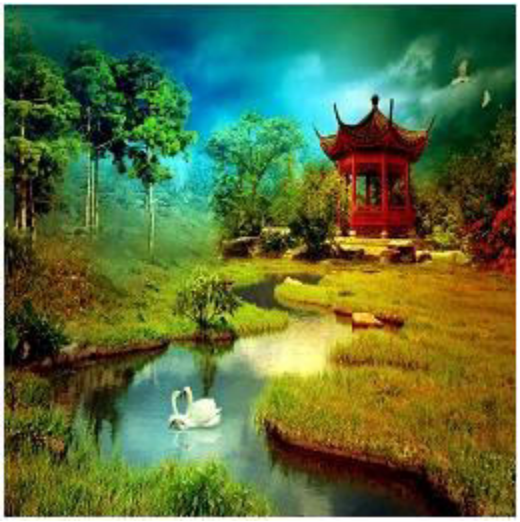


Figure 24: Extracted original image

From the above figures we have concluded that both images have look like same so there is less loss of data. From this we have said that this proposed method efficiently work for both grey scale images and as well as digital colour images.

The brute force attack performed on the digital colour images and it results are showing in the below

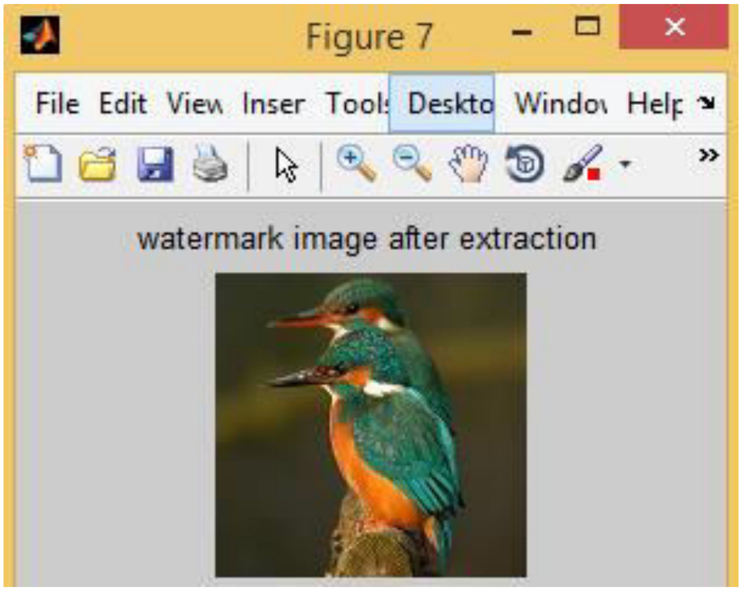


Figure 7
File Edit View Inser Tools Deskto Windov Help
watermark image after extraction

Figure 25: watermark image after extraction (on digital colour image)

In the above we are considering grey scale peppers watermark image. After extracting the image we will get the watermark image without loss. It is having good PSNR value which is equal to 45.37 and good NC value which is 1.0004. So from the above figure we can conclude that data loss is very less.

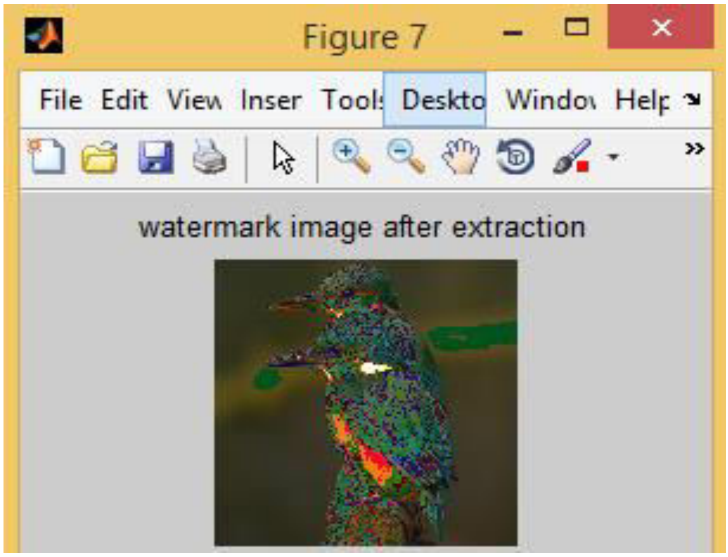


Figure 7
File Edit View Inser Tools Deskto Windov Help
watermark image after extraction

Figure 26: watermark extraction by attacker (digital colour image)

When we extract watermark image (w/o brute force attack) then we will get the PSNR and NC value of the above bird image (Fig 23) as 42.144 and 0.9996. but when attacker wants to perform brute attack on the image (after derail-fence process) then he will get this bird image(fig 24). The PSNR and NC values of the attacked image are 15.22 and 0.66 so from the above two figures we can conclude that the extraction process is very difficult for the attacker. If he wants to extract the watermark image with brute force attack he loose the main information in the watermark image. Hence we can say that our algorithm gives the security in an efficient manner.

The bar-charts of the watermark image and extract watermark image after applying brute force attack are given below:

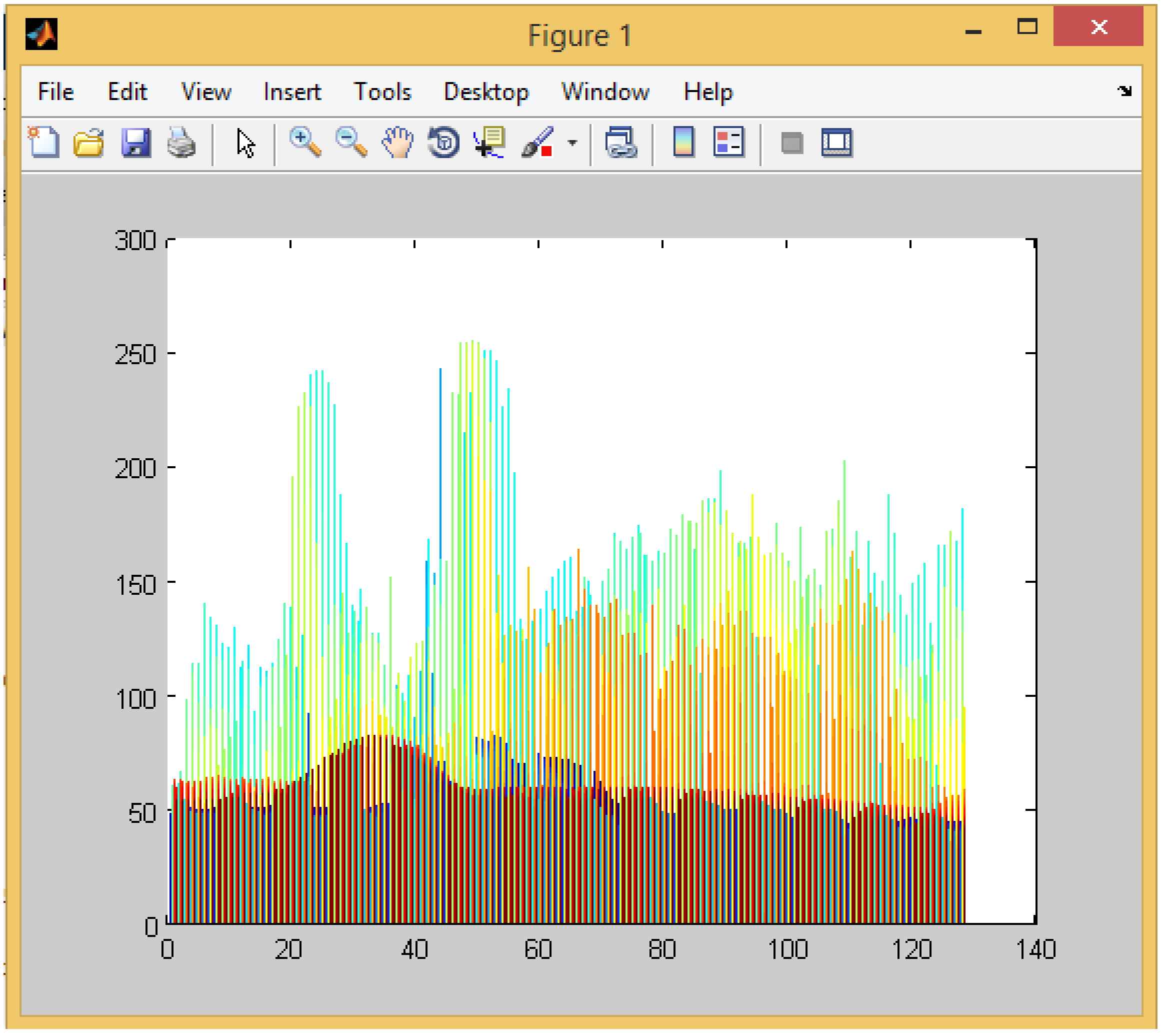


Figure 27: Watermark image bar chart

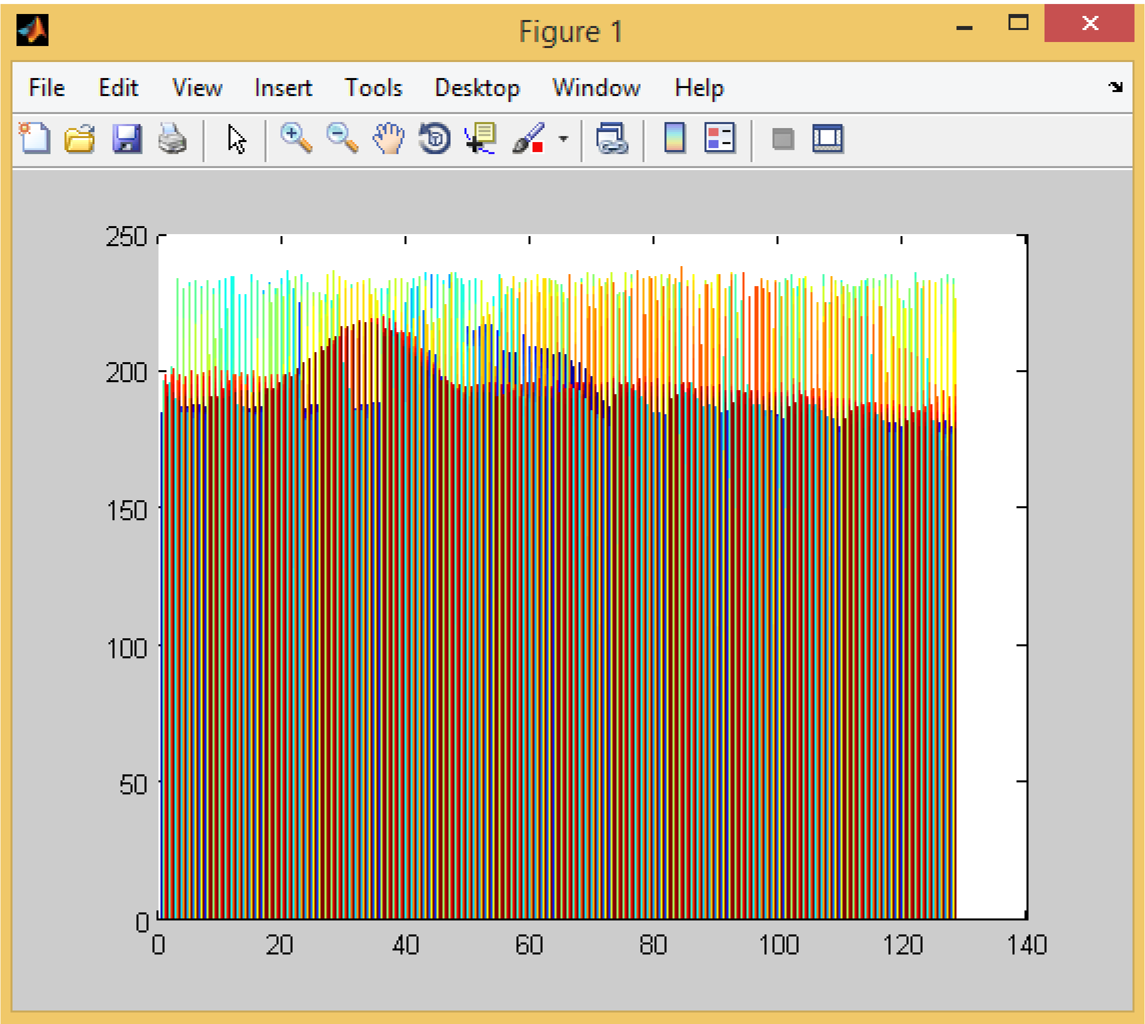


Figure 28: Watermark image bar chart after brute- force attack

From the above two figures we can conclude that the extraction process is very difficult for the attacker. If he wants to extract the watermark image with brute force attack he loose the main information in the watermark image. Hence we can say that our algorithm gives the security in an efficient manner.

CHAPTER 5

CONCLUSION AND FUTURE SCOPE

Conclusion and Future scope

The Advantages of proposed method are, it has provided robustness and as well as security to the watermark image. When we have used grey scale images then its time and space complexity became less. When we have used RGB images visible quality of the image (better visible for eyes) was increased. It provides security against active and passive attacks in the network. The below discussion will tell us about the security of the proposed method: Let us consider two pixel values 99 and 9, the 10's complement of these pixel values will be 1 and 1. When hacker gets these values then he thinks that they are similar pixels but actually they are different so it is difficult to trace (because the similar pixels are more in an image) the exact pixel values for the attacker. So in such case it has mandatory to have the inverse 10's complement algorithm then only it gives good results.

Table 3: 10's complement results

Pixel values	10's complement
9	1
99	1

Advantages of using 10's complement and rail-fence method with an example: This proposed method has used the 10's complement which provides security to the watermark image. It is very difficult to analyze the exact pixel value of the watermark image after applying 10's complement on it. The below example will show another advantage of the 10's complement. Let us consider one pixel value of the grey scale watermark image as '10'. After applied 10's complement on the pixel value it gave the result as 90. In the above example 10 became 90 so there is much difference in between 10 and 90. By using this method it is very difficult for the attacker to get the exact image due to the variation in the pixel values before and after extraction. The proposed method has the mixture of 10's complement and rail-fence method these two methods provides the security to the watermark image. The rail-fence method provides security against active and passive attacks. But the experiments have shown that this had destroyed by the attackers in the earlier days. If it has combined with the 10's complement then definitely it will become one of the best encryption methods for securing the image. Whenever we applied 1's complement and 2's complement on the image pixel values the pixel values became almost similar when we compared with the original pixel , but using 10's complement it has became much difference In the original pixel value and the after 10's complemented pixel. So it has provided more security when it compared with the 1's complement and 2's complement.

Table 4: 10's complement comparison results

Complement method	Original pixel value	Pixel value after applied complement method
1's complement	10	5
2's complement	10	6
10's complement	10	90

From the above figure it has concluded that whenever 10's complement has used the pixel value will become drastic change. This change will be helpful for providing the security to the watermark image. From this we have concluded that this proposed method has provided robustness and security in an efficient way. This proposed algorithm has used on both grey scale image and digital colour image where as existing system only worked on grey scale. It has given and NC values even after applied some types of image processing attacks, active and passive attacks. The proposed method is robust as well as secure approach.

Future scope

Sometimes the attacker may be get original pixel values easily if he will perform brute force attack but it will definitely take some time to get the original pixel values. If we use the best security algorithm like symmetric algorithms such as DES and AES then our watermark security will increases. The PSNR and NC values of the proposed method gave the good results but if we will use PCA (principle component analysis) in place of svd (singular value decomposition) then it will give better values because the loss of data in PCA is less when we will compare it with SVD.

CHAPTER 6

REFERENCES

References

Reports and Official Documents

[1] Bhattacharya Saurav, Chattopadhyay, T and Pal Arpan (2006),"*A Survey on Different Video Watermarking Techniques and Comparative Analysis with H.264/AVC".*

[2] Ghobadi Monia (2001), "*A Survey on Wavelet-based Coding and its Application in JPEG2000".*

[3] Gu Jinwei (2008) "*An Introduction of Support Vector Machine*".

[4] Gunjal L Baisa and Mali N Dr. Suresh (2012), "*A Survey on Applications of Digital Image Watermarking in Industries*".

[5] Hui-fang Li, Ning Chen, Xiao-ming Chen (2010), *"A study on Image Digital Watermarking Based on Wavelet Trnasform".*

[6] Mishra Anurag, Agarwal Charu, Sharma Arpita, Bedi Punam (2014), *"Optimized Gray-Scale Image Watermarking using DWT–SVD and Firefly Algorithm".*

[7] Singh Neha and Nandi Arnab (2003), "*Digital watermarking Mark This Technology*".

[8] Singh prabhishek, Chadha S R (2003), "*A survey on Digital Watermarking Techniques, Applications and Attacks".*

[9] Shukla D Panchamkumar(2003), "*Complex Wavelet Transform and their applications*".

[10] Xu J Z, Wang Z Z, Lu Q (2011), "*Research on Image Watermarking Algorithm based on DCT"*

Websites:

https://www.youtube.com/watch?v=uvXTZxSzdMk

http://in.mathworks.com/matlabcentral/

CHAPTER 7

APPENDIX

7.1 Questionnaire

i. Why do we need digital watermarking?

The major reason for using these watermarking techniques is to secure or protect the digital content (image, text, audio or video). Digital watermarking has used in many areas. Digital watermarking has been popular topic for both researches and applications in the last 10 years. Now a day's multimedia technology has been grown very fast and for secure digital data transmission, need some special mechanisms like digital watermarking. Normally user uses the audio and video file's that are exist in the websites at free of cost but the problem comes in case of the protection of that digital content (audio or video file). If any un-authorized user will access that digital content and altering that data is called as attacking against authentication. Use such a watermarking technique that will protect our digital content in such a way that it will give protection during its (watermark) entire lifespan. These watermarking techniques also provide the ownership identity, proof of ownership and they are two important applications of multimedia technology.

ii. What is the problem in the existing method?

But the problem with the existing system is, if the attacker known the two algorithms (DWT and SVD) then the watermark image will be easily identified sometimes. In this case there is no secure algorithm is providing to the watermark before calculate the singular values of it. So possibilities of active and passive attacks are more in th case of existing method.

iii. How proposed method works?

The proposed method is having the secure approach which will be compare with the existing method and which provides the more security. This presents the two methods such as 10's complement and rail fence methods which are easy to implement and provide the more security.

7.2 List of abbreviations

DCT- “Discrete Cosine Transformation”

DWT-“Discrete Wavelet Transformation”

IDCT-“Inverse Discrete Cosine Transformation”

IDWT-“Inverse Discrete Wavelet Transformation”

NC- “Normalized Cross Correlation”

PSNR- “Peak Signal to Noise Ratio”

SVD- “Singular Value Decomposition”

WT- “Wavelet Transformation”

Publications

Paper accepted

I. Shylesh Kulakarni and Chirag Sharma (2015)" Efficient Watermarking Technique using DWT, SVD, Rail fence and 10's complement applied on Digital Images", International Journal of Applied Engineering and Research (IJAER).