ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

# Image Leakage Detection and Prevention

**Pardeep Kumar**
Computer Science Engineering, Lovely Professional University, Phagwara(Punjab), India
sharma.pardeep04@gmail.com

## Abstract

As we know now a days we have to share our image with many other companies to get the service from them and share it on the internet ,so it is very dangerous for the data to get into the wrong hands .But, some of the data that we are sharing might be very sensitive to organization. So, we have to protect (copyright) it from leaking so, they don't reach to wrong people .We have to find the person responsible for the leakage of data . if the data distributed to the third party found in the public domain ,it might be very serious threat to the owner of the company.

**Keywords**: DCT , PSNR , MSE , DWT.

## Introduction

This Research is all about the Image Leakgae Detection and Prevention, As we know now a days we have to share our data(image) with many other companies to get the service from them and share it on the internet ,so it is very dangerous for the data to get into the wrong hands .But, some of the data that we are sharing might be very sensitive to organization. So, we have to protect (copyright) it from leaking so, they don't reach to wrong people .We have to find the person responsible for the leakage of data . If the data distributed to the third party found in the public domain ,it might be very serious threat to the owner of the oragnization.[1,3]
For eg. Company might be giving the data to the 2nd party ,who are doing research on the finding the new treatments to cure some particular disease . It is need of the time that we have to share our data with other organization .

Another eg. Some XYZ company wants to do survey of their product then XYZ should give their data to company who will be doing survey for it. But, on the same time we should protect our data also .Now, a days when in business we need the service from various vendors then we should share a our with them also but in very safe manner , it might get harm to our organization.

Our need is to Increase the probability of finding the person responsible for the leaking the sensitive data to the third party .we can use perturbation technique , in this we add noises to our sensitive data .but in some cases we cannot add any noises because originality of data is very essential to the 2nd party . Today, we have globalization in our businesses we have to interact or deal with the various other companies also .

Every company wants that their data should be very secure ,even after distributing to the various other companies .we should take care of data that nobody will leak our data .Traditionally leakage is handled by watermarking technique .

Even the Companies provide the text-files with containing the watermark on it .by this they prove their ownership ,origin of the data etc.but , now a days they had developed the technique by which we can remove watermark from the soft copy of the data.

We should make the technique which is more efficient to make these sharing secured .So, that they do not harm to the any of the company neither distributor nor 2nd party (agent).

We should increase the probability of finding the agent who is guilt .we should work on the allocation strategy to allocate the data . so that It will be safe in the hands of the agent .But , main question is how we can do this , that I will elaborate in the further discussions .[3]

I want to make this process more easy and efficient as compared with other techniques developed by other people who had done research on this . Further this can be used to find the guilt agent who is leaking the data and take strict actions against them .it will make data transaction more easy and secured .

By this we can manage to share our data in very oragnised way .In the end I just want to say that it is the need of the hour to work on these topics because now a days we need the trusted channel to share our data so that it is convenient for the distributor to share the data with the only trusted Agents only.

In this paper I will improve the PSNR(Peak signal to Noise Ratio ) And other aspects will be computed to give the more quality in the watermark. In this I will use DCT technique to image and obtain DCT Coeffiecient of images by.

C=dct(V).

And, Use PSNR function to check the image quality.

PSNR=10.log10(max^2/MSE)
MSE= Mean Square error.

## Related work

Protection of multimedia information has attracted a lot of attention during the last few years. The motive of such technique is to protect the copyright of broadcast or publicly exposed digital data. Attackers have the freedom to obtain copies of copyrighted digital through the Internet and use them acc. To their own will. The most famous method to protect the information is watermarking.[1]

The main requirements for an acceptable technique of watermarking are as follows.

1). *Imperceptibility*: the watermark should not be easily noticed by simple visual inspection.
2). *Key uniqueness*: Unique keys should produce unique, independent statistically watermarks.
3). *Non-invertibility*: it should not be computationally feasible to find the watermark by possessing a watermarked image.
4). *Image dependency*: a single key produces the single watermark, this watermark should adapt to the image content.
5). *Reliable detection*: Watermark should be efficiently detected for any value of false alarm probability up to a certain threshold.

*Robustness*: watermark should be efficiently detected after the most common Signal Processing Operations. A tradeoff is necessary between watermark imperceptibility and robustness. However, most of them do not consider simultaneous robustness to several types of attacks. Most of them focus on robustness against JPEG or any other compression techniques.

They will never do this kind of act in the future if distributor do share/transaction with him. otherwise ,action will be taken against him and expelled from the sharing process. It will increase the probability to find the leakage of data .by this we can implement water marking before handing over any images to the 2nd party .watermark should be according to the 2nd party. So that we can easily detect that party who is responsible for it .

## Current scheme

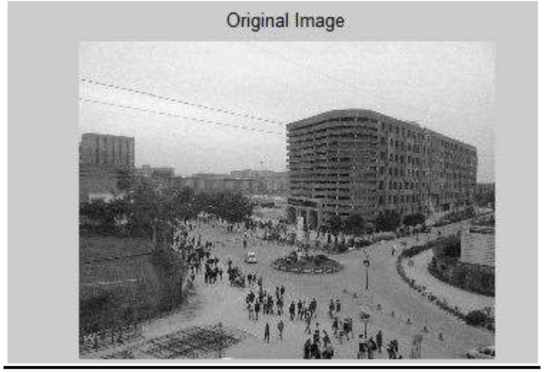
1. Bring the image to frequency domain by applying the DCT.
2. Generate a watermark signal.
3. Use the thousand largest coefficients of the original image to embed a watermark sequence of length 1000.
4. Coefficients are modified according to the stream bits of the message using the equation below,
   |CAW = CA (1 + α Wi)| .
5. Extraction process – simply subtracting the original DCT coefficients from the watermarked image coefficients

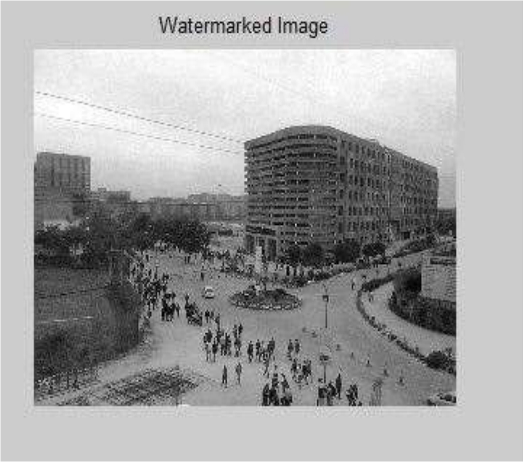
## Result and discussion

Result shows that the Value of the following tests are :

MSR = 31.0631

PSNR = 76.9314





## Conclusions

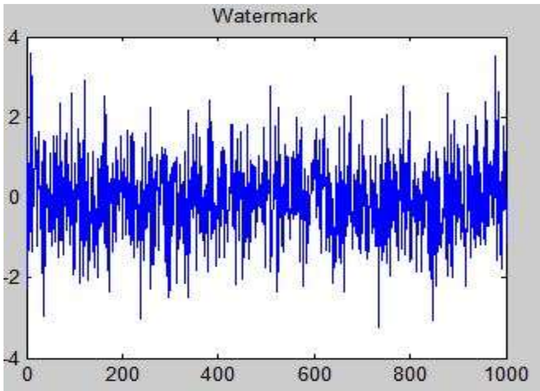
Increase the probability of finding the guilt agent. To make this more easy and effective .So, that if some one will leak the data(image) we should came to know the agent who is responsible for this. We can stop doing any transaction with him in the future.

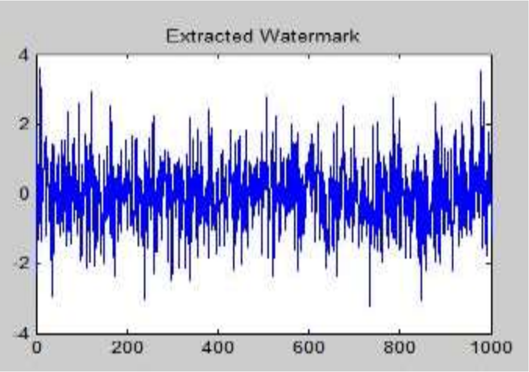
In this we study the problem Proving ownership rights on images it is very important in today internet-based application environments and in many content distribution applications .In this research, we present a technique for proof of ownership based on the secured embedding of a robust imperceptible watermark in images .

There are 3 phases of this research :-

- Generation
- Embedding
- Extraction

In the end i got this result that watermark and extracted watermark should be same like this :





During the past 10 yrs, with the development of information digitalization, digital media,internet, increasingly predominate over an traditional analog media.As one of the concomitant side-effects,in this world everyone can use others images and also transmit to the other party. The digital watermark is introduced to solve this problem.

The main highlights of this paper are :

1. A unified framework for identifying the preservation, privacy and performance offered by a system.
2. An algorithm for finding systems that achieve a desired balance between the 3 P's(preservation,privacy ,performance)

Watermarking is embedding information, which is able to show the ownership into the digital video, image and also for the audio. Its purpose is to determine that the watermark should be indivisible and robust to common processing and attack. Currently the digital watermarking technologies can be divided into two categories by the embedding position—— transform domain watermark and spatial domain.

The Spatial domain techniques developed earlier and is easier to implement, but is not effective in robustness, while transform domain techniques, which can be embed watermark in the host's transform domain, also it is more sophisticated and robust.

***Invisible:*** A watermarking system is of no use if it destroys the cover image to the point of being useless,. Ideally the watermarked imaged should look indistinguishable from the original even i use higher quality tools.

***Robust*:** The watermark should be resistant to distortion introduced by during either normal use or a

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

intentional attempt to disable or remove the watermark present.

***Unambiguous:*** Retrieval of the watermark should unambiguously identify the owner. Acc. to domain for watermark

***Embedding***: Spatial domain watermarking technologies change the intensity of original image or gray levels of thier pixels. This type of the watermarking is simple and with low computing the complexity, because no frequency transform is required. Frequency-domain watermarking embeds the watermark into the transformed image. It is difficult but has the advantages which the former approach lack.Acc. to ability of watermark to resist attack :

Fragile watermarks are ready to be destroyed by random image processing methods. The change in watermark is easy to be find, so it can provide info. for image completeness. Robust watermarks are always robust under most image processing methods and can be extracted from attacked watermarked image. Thus it is preferred in the copyright

## *References*

1. *Novel DCT based watermarking scheme for digital Images Neminath Hubballi, Kanyakumari D P,Dept of Computer Science,Indian Institute of Technology Guwahati International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009.*
2. *REVIEW ON DATA LEAKAGE DETECTION Naresh Bollam,Mr.V.Malsoru/ International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 1, Issue 3, pp.1088-1091 1088*
3. *A MODEL FOR IMPROVING GUILT PROBABILITIES TO DATA LEAKAGES A.Mounika, M. Satwik, G. Rajesh Chandra,Advances in Computer Science and its Applications (ISSN 2166-2924) 131Vol. 1, No. 2, June 2012) Copyright ©World Science Publisher, United States*
4. *Data Leakage: What You Need to Know by Faith M. Heikkila, Pivot Group Information Security Consultant*
5. *A Novel Technique for Image Steganography Based On Block-DCT and Huffman Encoding Arunima Kurup P& Poornima D Sreenagesh S8, Department of Information Technology, Mohandas College Of Engineering,andtechnology,Anad,thiruvananthapurm.*