SYNOPSIS REPORT

on

DATA LEAKAGE PROTECTION USING WATERMARKING

Submitted by

ANEESHA SHARMA (R111216012)

SAMRIDHI PANDEY (R133216037)

MAYANK KHOSLA (R111216034)

AKSAH PRATAP SINGH (R111216005)

Under the guidance of

Mr Prashant Rawat
Assistant Professor , SOCSE

SCHOOL OF COMPUTER SCIENCE

UNIVERSITY OF PETROLEUM & ENERGY STUDIES
Bidholi Campus, Energy Acres, Dehradun – 248007.

August – 2018

School of Computer Science

University of Petroleum & Energy Studies, Dehradun

Project Proposal Approval Form (2018-19)

Minor I

PROJECT TITLE: DATA LEAKAGE PROTECTION USING WATERMARKING

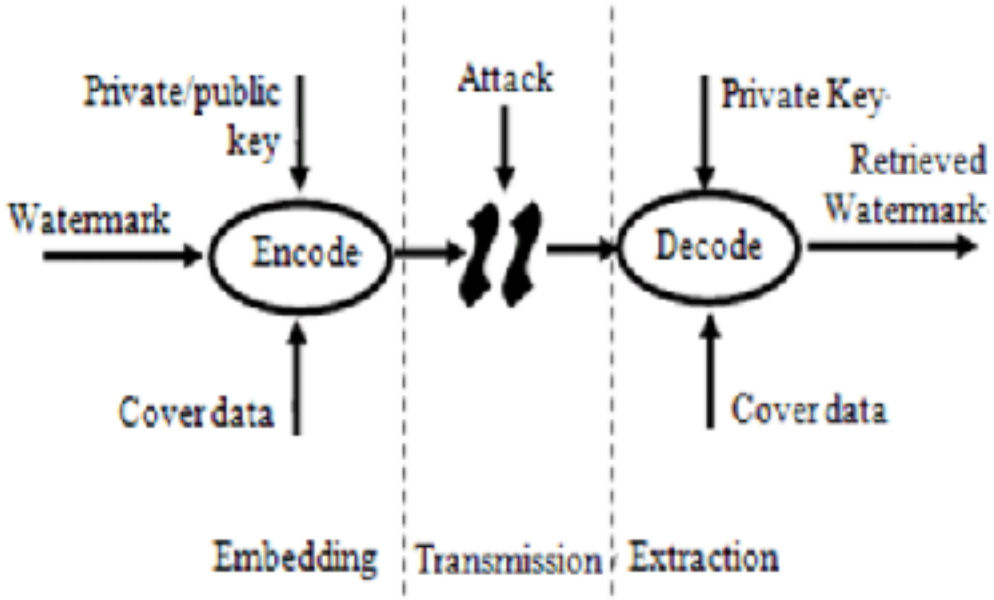
ABSTRACT

The increasing globalisation led to the transmission of vast number of digital documents like texts, images, videos or audios over the internet from one point to another. However, some of these documents might be highly confidential and its transmission over the internet must be protected from unauthorized access. In this project, we have proposed a novel method called watermarking that provides security to the digital documents. Watermarking is a technique in which pattern bits are inserted into digital image; video or audio files have copyright information such as rights authors etc. The aim of digital watermarks is to provide secured or copyright protection for intellectual property that's in digital format. Digital watermarks are completely invisible and inaudible in case of audio clips unlike printed watermarks. Apart from it, the actual bits representing the watermark must be scattered throughout the file in such a way that they cannot be identified and manipulated. The goal of watermarking is not to restrict access to the original image but to ensure the embedded data remain recoverable. The paper focuses on the C language simulation of watermark decoding scheme using Discrete Wavelet Transform (DWT). Digital image watermarking algorithms which are based on the discrete wavelet transform have been widely recognised to be more prevalent than others.

Keywords: Digital image watermarking, image copyright protection, Data leakage protection, Discrete Wavelet Transform (DWT).

INTRODUCTION

Digital watermarking technology is an emerging field in computer science, cryptography, signal processing and communications. Digital watermarking is intended by its developers as the solution to the need to provide value added protection on top of data encryption and scrambling for content protection. In general, a digital watermark is a technique which allows an individual to add hidden copyright information or other verification message to digital media. Watermarking is the process that embeds data called a watermark or digital signature or tag or label into a multimedia object such that watermark can be detected or extracted later to make an assertion about the object. Digital watermark is a sequence of information containing the owners copyright for the multimedia data. It is inserted visibly or invisibly into another image so that it can be extracted later as an evidence of authentic owner. Usage of digital image watermarking technique has grown significantly to protect the copyright ownership of digital multimedia data as it is very much prone to unlawful and unauthorized replication, reproduction and manipulation. The watermark may be a logo, label or a random sequence. A typical good watermarking scheme should aim at keeping the embedded watermark very robust under malicious attack in real and spectral domain. Watermarking requires two operations, embedding the watermarks with the information and extraction. According to the type of document, watermarking techniques can be divided into four categories; they are (i) text watermarking (ii) image watermarking(ii) audio watermarking and (iv) video marketing. Image watermarking can be classified both in spatial domain and frequency domain. We will be implementing frequency domain as it is more robust, imperceptible and fragile as compared to spatial domain [1].



(General process involved in a watermarking system)

PROBLEM STATEMENT

To develop watermarking schemes for images (which are stored in spatial domain as well as transformed domain) which can sustain the known attacks and various image manipulation operations. Out of image, audio and video, the image watermarking was chosen as a goal because any successful image watermarking algorithm may be extended to video watermarking also. Therefore, to keep the future extension in mind, the cover medium chosen is an image [2].

- Explore the ways such that attack impacts may be minimised before the watermark embedding process.
- Explore the relationship between the performance of watermarking scheme and the cover image characteristics itself.
- combined the two techniques of DCT and DWT to improve the digital watermarked image in terms of fidelity, robustness and resistance

LITERATURE REVIEW

The appropriate background of literature and the concepts of digital image watermarking are reviewed in this chapter. The copyright protection of multimedia content has become a critical issue now days due to easy copying, the latest developments in digital transmission and widespread of broadband networks and the internet. The transmission of information takes place in different forms and is used in many applications, where the communication must be done in secret form. Such secret communication techniques include the transfer of medical data, bank transfers, corporate communications, purchasing using bank cards, a large amount of information through emails and etc. Steganography, cryptography and watermarking are the different techniques used to perform secret communication [3].

Properties of Digital Image Watermarking

The efficiency of a digital image watermarking process can be evaluated based on the properties of imperceptibility, robustness, capacity, data payload, fidelity, security, the cost of computation, recovery of watermark with or without the need of the cover image and the speed of embedding process etc. To understand watermarking methods and determine their applications, the following properties of digital image watermarking must be known:

Robustness-
of a watermark is its ability to withstand different image distortions such as cropping, rotation, filtering, resizing and compression, etc. Data Payload is the data size of the watermark in cover image and it depends on the size. Capacity is defined as the amount of information that can be carried by watermark. If more than one watermark embedded into cover image, the capacity of the watermarked image equal to the sum of the information carried by individual watermarks. If the robustness of the watermarked image increases, the capacity also increases and the imperceptibility decreases, hence there is a trade-off between imperceptibility and robustness

Imperceptibility –
defined as the quality of the watermarked image that cannot be destroyed by the watermark

Fidelity-
defined as the visual similarity between the cover image and the watermarked image

Security-
of the watermark defined as its ability to resist different attacks, which try to destroy the watermark and try to remove the watermark from the cover image.

Computational cost-
of the watermarking technique defends upon the resources required to perform watermark embedding and extraction.

OBJECTIVES

The main objective of this project is to:

- The image is divided into two different watermarks are inserted into the horizontal and vertical sub bands of wavelet coefficients. It is recognised that Human Visual System (HVS) is less sensitive to the removal of smaller.

- The DWT is applied to the host image. Then, the SVD transform is applied to each sub-band of the transformed image and the singular values of each sub-band and the singular values of the watermark image are converted to semi-binary arrays.

- Finally, the bits of the singular values of the watermark image are inserted into the selected bits of the singular values of decomposed host image’s sub-bands.

METHODOLOGY

Since DWT has the excellent spatio-frequency localization property, it has been extensively utilized to identify the image areas where a disturbance can be more easily hidden. A new method for digital image watermarking which does not require the original image for watermark detection.

Watermark Embedding:

The algorithm to embed a watermark in the original image is summarized as follows:
1-Decompose the original image into four levels (thirteen sub bands).

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

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

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

5-The pseudo-random binary sequence generated from the binary image is rearranged in three different ways to be embedded in the LH3, HL3, HH3, LH2, HL2, and HH2 using the pixel-wise computation.

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

Watermark Extraction:

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

$$Z >= T$$

Then watermarking revealed it means watermarked image

$$Z < T$$

Then watermarking not revealed it means non-watermarked image [3].

SYSTEM REQUIREMENTS

HARDWARE REQUIREMENTS: -

The selection of hardware is very important in the existence and proper working of any software. In the selection of hardware, the size and the capacity requirements are also important.

The Digital Watermarking Algorithm (FHT) can efficiently run on System With minimum requirements, of at least 128 MB RAM and Hard disk drive having 20 GB that can be driven by a processor of 600 MHz. suits the information system operation

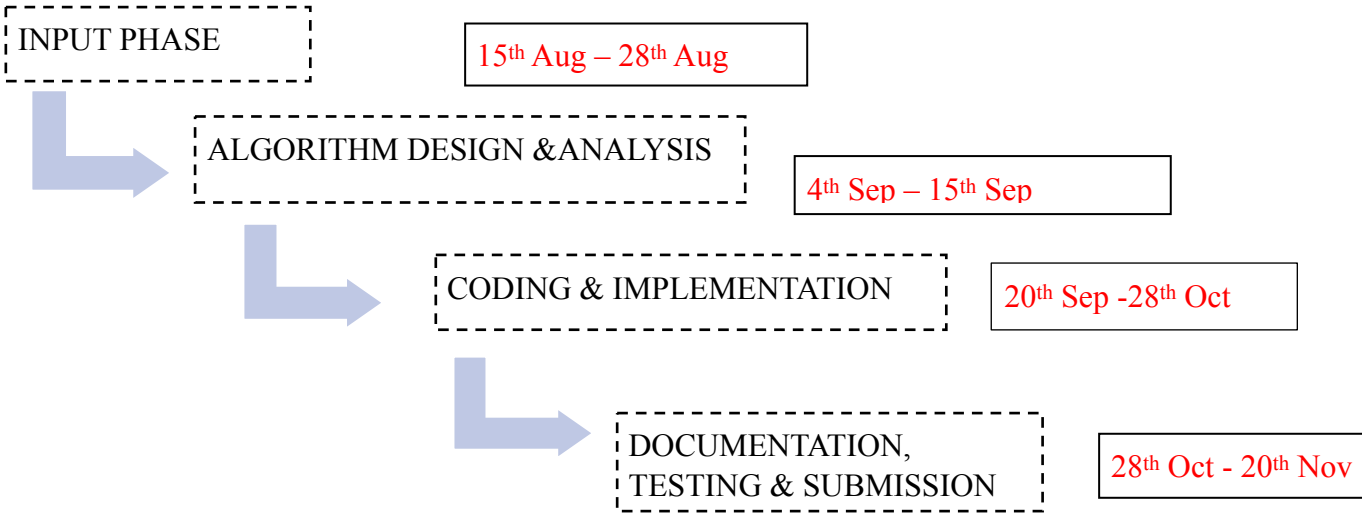
- Processor -------- PIII, 600MHz
- RAM Capacity -------- 128MB or above
- Hard Disk -------- 20GB or above

SOFTWARE REQUIREMENTS

One of the most difficult tasks is that, the selection of the software, once system requirement is known is determining whether a particular software package fits the requirements. This section first summarizes the application requirement question and then suggests more detailed comparisons.

- Operating System -------- Windows 2000 or later
- Software -------- C

SCHEDULE (Pert chart)



REFERENCES

[1] Ibrahim, R. and Kuan, T. S., Steganography Imaging (SIS): Hiding Secret Message inside an Image. Proceedings of the World Congress on Engineering and Computer Science, 2010, San Francisco, USA.

[2] International Journal of Computer Applications (0975 – 8887) Volume 118 – No. 1, May 2015

[3] International Journal of Advancements in Research & Technology, Volume 2, Issue4, April-2013 19ISSN 2278-7763

[4] International Research Journal of Engineering andTechnology(IRJET) Volume: 02Issue: 02| May-2015

Synopsis Draft verified by

Project Guide
(Mr Prashant Rawat)

HOD
(Dr. Neelu Jyoti Ahuja)