Digital Image Watermarking

MALIK ANEEB UL ISLAM (16D070035)

AJIT ZOTE (16D070002)

CONTENTS

Introduction

Overview

Working in the spatial domain

Working in frequency domain

Introduction

A few years back Unique Identification Authority of India (UIDAI) experienced a breach in user data as the information about millions of registered personnel was leaked to a third party for processing and unauthorised use. The main issue that was found at that time was the level of security that was used to safeguard the details of the registered users was not apt. This lack in the level of security was then rectified by UIDAI. Keeping the above issue in mind, what if there is some tampering with the user data, that UIDAI has, like fingerprints, retina scans or basic personal information? The current project deals with the safeguarding of these particular details with the help of the method of Digital Watermarking.

Overview

01 Digital watermarking is a method used to embed information in the form of bit-stream into a file.

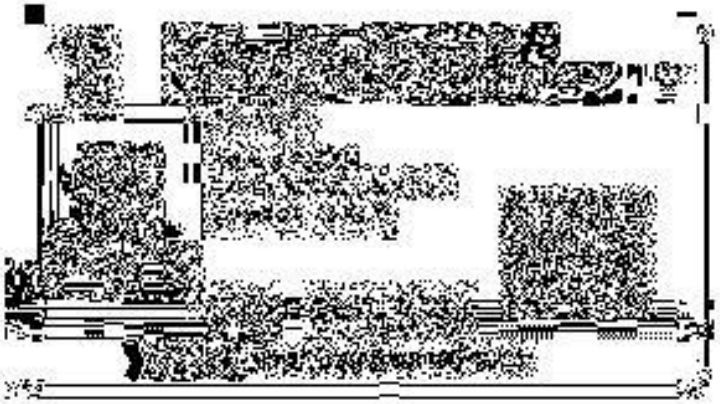
02 The information to be embedded is called the ‘message’ and the host file in which this bit-stream going to be embedded is called ‘asset’.

03 In our case the target files are images. Hence, all our work will be focused on the domain of image on image watermarking.

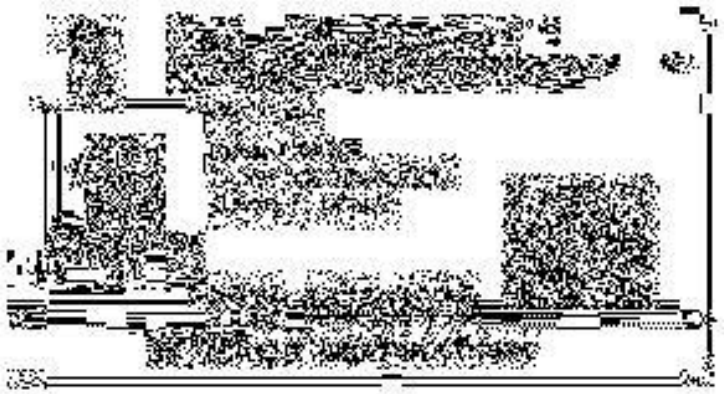
Bit-plane manipulation in Spatial Domain

Both the message and host files are bought to an 8-bit deep Grayscale level. The bit-planes of both of the images are extracted. The first few most significant bits contain the most information of the images and the trick is to utilize the first few most significant bit-planes of both the host and message images. In our case we've removed the bottom three bit-planes of the host and replaced the first three most significant bit-planes of the message in their place. Extracted bit-planes of both the host and the message are shown in the next few slides:

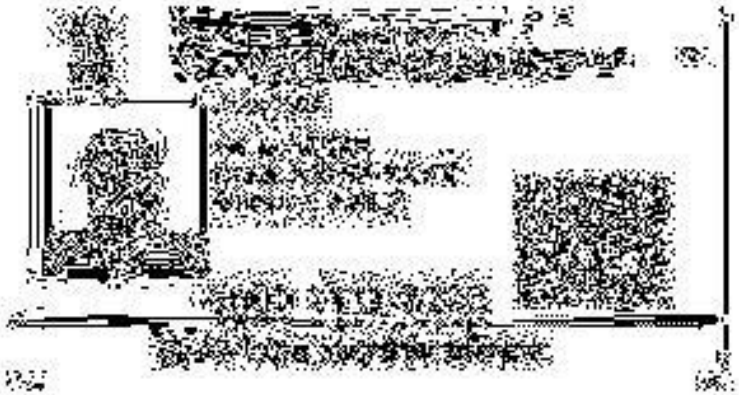
1st plane



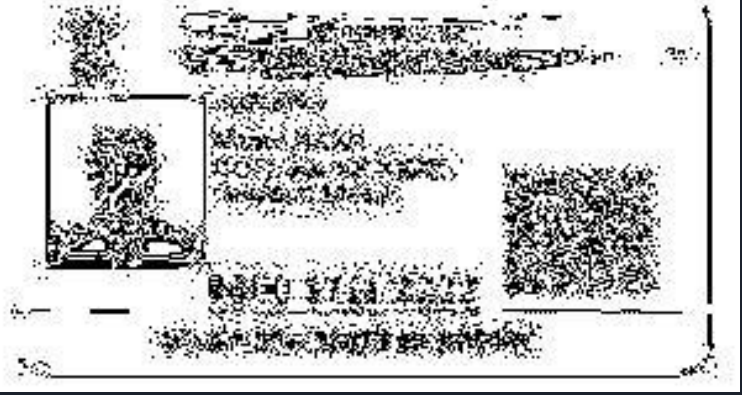
2nd plane



3rd plane

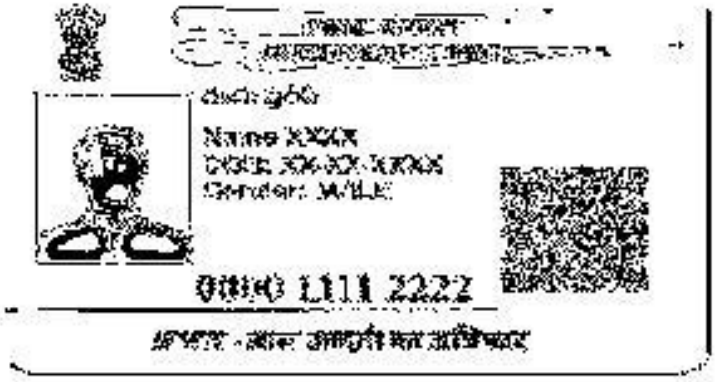


4th plane

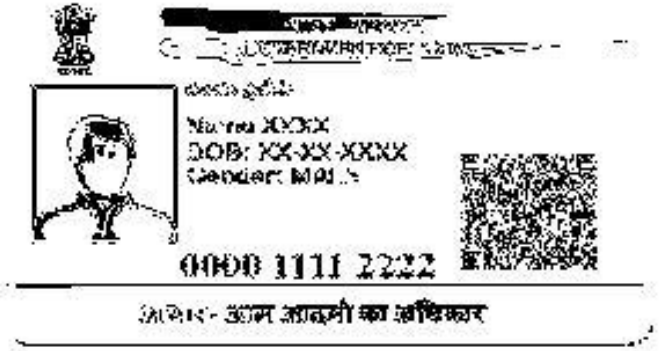


5th plane

6th plane



7th plane

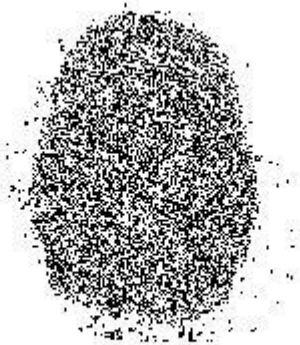


8th plane

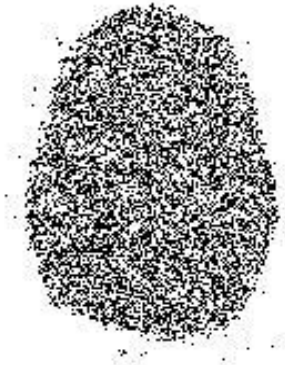
Recombined Result

Scaled Watermark

1st Watermark plane

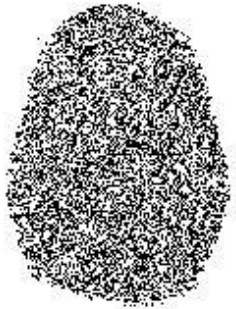


2nd Watermark plane

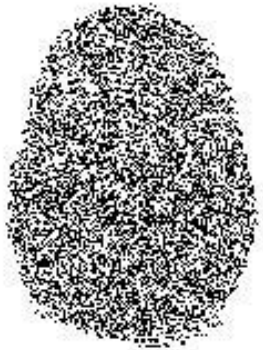


3rd Watermark plane

4th Watermark plane



5th Watermark plane

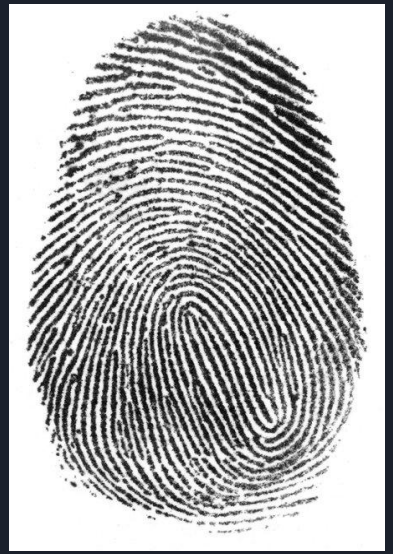


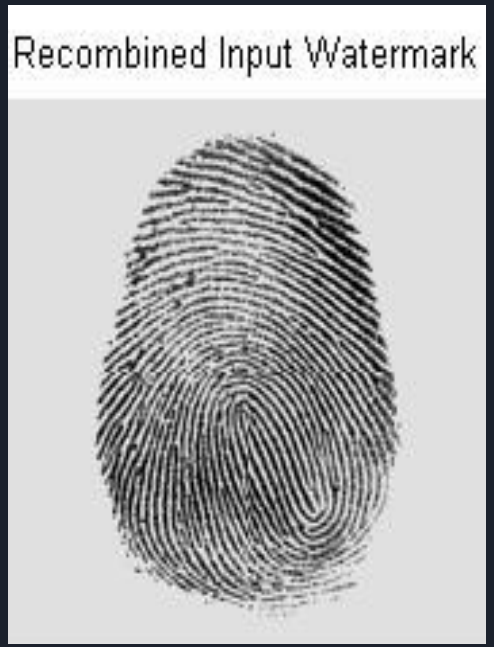
6th Watermark plane

7th Watermark plane

8th Watermark plane

ORIGINAL FINGERPRINT





Input Image

Watermarked Image

Watermark Extraction

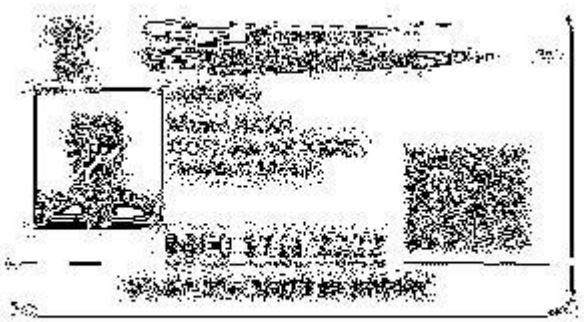
To separate the watermark from the image, we begin by generating the bit-planes of the given image. We then extract the least three significant bits of the image and using logical left shifts, we bring those three least significant bit-planes to the most significant positions. Then by superposition, we get the watermark separated from the host.

1st extracted plane

2nd extracted plane

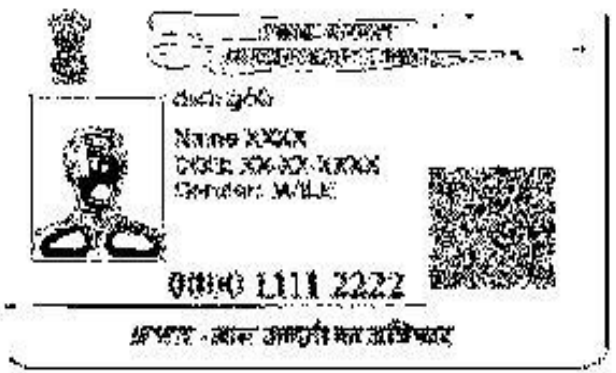
3rd extracted plane

4th extracted plane

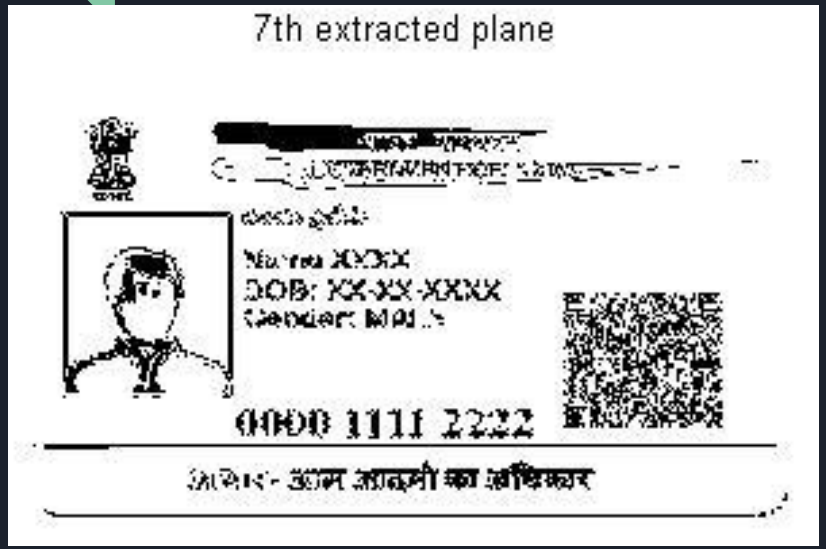


5th extracted plane

6th extracted plane



7th extracted plane

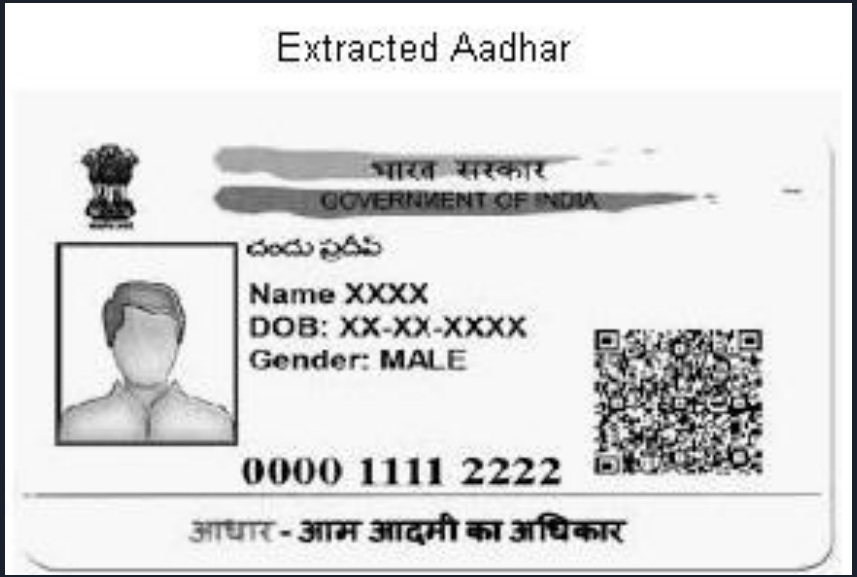


8th extracted plane

ORIGINAL FINGERPRINT

Input Image

Extracted Aadhar



Working in frequency domain

There are several transforms that bring an image into frequency domain. Among most common of those, we can mention are: Discrete Cosines Transform (DCT) and Fast Fourier Transform (FFT).

Here we use DCT

In frequency domain, coefficients are slightly modified. This will make some unnoticeable changes in the whole image and makes it more robust to attack compared to what we have in spatial methods

In this method, Discrete Cosines Transform (DCT) is applied on the asset image as shown in Fig. 7. Fortunately, there is a direct command for obtaining DCT coefficients of images: B = dct2(A);

We use r1xc1 largest coefficients to embed a watermark sequence of length r1*c1. The only exception is the DC term, located in (0,0) of the DCT matrix, that should not be changed due to its perceptible change in the whole brightness of the picture

In On the other hand, high frequencies are easily changed under common attacks such as compression.

Bits of the message using to the equation

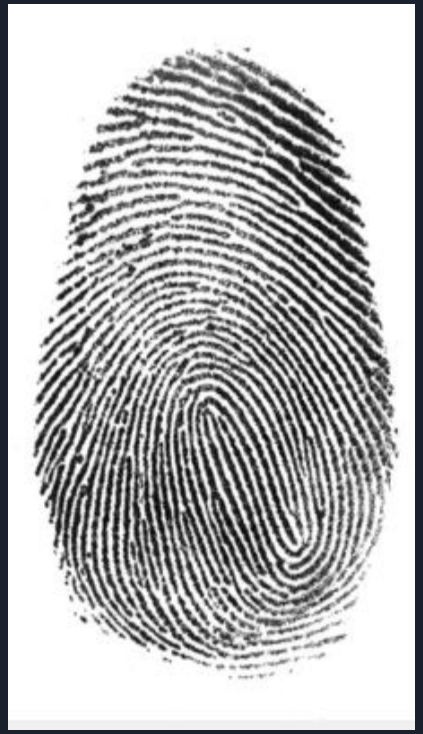
$$C_{AW}=C_A(1+Wx\alpha)$$

In which C_{AW} is the watermarked coefficient, C_A is the original one, α represents watermarking strength we take this to be 0.1.


भारत सरकार
GOVERNMENT OF INDIA
చందు ప్రదీప్
Name XXXX
DOB: XX-XX-XXXX
Gender: MALE
0000 1111 2222
आधार - आम आदमी का अधिकार

Image after adding the watermark

Original image



Retrieved watermark image

Original image which was used as a watermark

Original image

Image retrieved after removing watermark

Thank you!