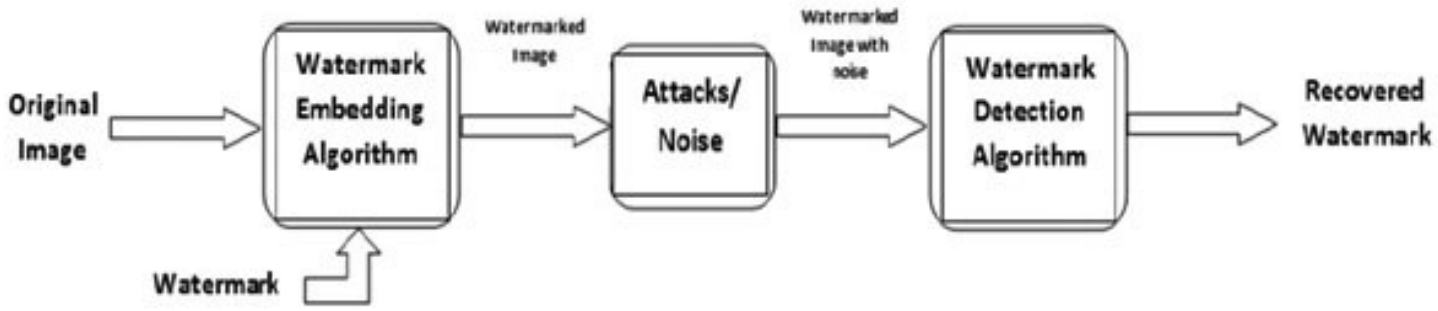
IMAGE PROCESSING

Project Report

Robustness of Spatial watermarking

[Bit manipulation method]



Made by: -
Arpnik Singh

Introduction

Image is defined as a two dimensional function, f(x,y), where x and y are spatial (plane) coordinates, and the amplitude of at any pair of coordinates (x,y) is called the intensity, or gray level of the image at that point. When (x,y) and f are all finite and discrete quantities, we call the image a digital image.

With advancement in technology there is an increase in number of digital images. Now-a-days, one may want to protect the ownership rights of digital image. This can be done by digital image watermarking. Its commercial applications range from copyright protection to digital rights management. In this technique our objective is to hide a noise tolerant marker in the image in order to preserve the ownership rights.

The technique works by embedding a subliminal signal, called a watermark, into the data without significantly affecting the visual appearance or visual quality of the data. The root of watermarking as an information hiding technique can be traced to ancient Greece as steganography, however the science of watermarking is a modern subject and it was only developed in recent years. Steganography is embedding a hidden message in the file such as video, audio, picture, etc in such a way that only the intended sender and receiver can view it and generally the hidden (invisible) message is not related to the file in which it is embedded. In watermarking the hidden message is actually related to the file and can be visible or invisible depending upon the technique used. Its main goal is that the message should be viewable by everyone but no one should be able to change it.

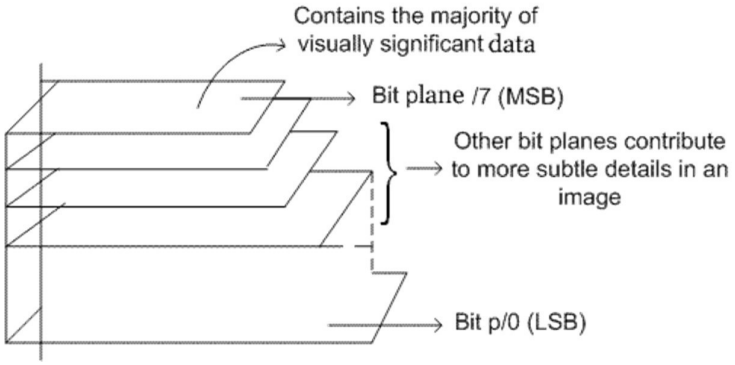
The success of a watermarking technology used in a copyright protection or digital rights management system relies heavily on its robustness to withstand attacks. Watermark attacks are aimed at removing or destroying any watermark signals in the host data. There are four categories based on the classification: removal attack, geometric attack, cryptographic attack and protocol attack.

- Removal attack aims at the complete removal of the watermark information from the watermarked data without breaking the security of the water marking algorithm. Most of image processing methods, such as image smoothing and salt and pepper noise, belong to removal attack category.
- Geometric attack is different from removal attack. Instead of removing the watermark signals, geometric attack intends to distort the watermark detector synchronization with the embedding information.
- The aim of cryptographic attacks is to break the security of watermarking schemes and thus find a way to procedurally remove the embedded watermark information or to embed misleading watermarks.
- Protocol attack is a different type of watermark attack in a sense that it targets the entire concept of using watermarking techniques as a solution to copyright protection rather than the watermark itself. Whereas the other types of attacks aim at destroying, distorting or extracting the watermark signal, protocol attacks aim at producing ambiguities on the true ownership of the data in question.

Relevant terms

- Bit-Plane Slicing:

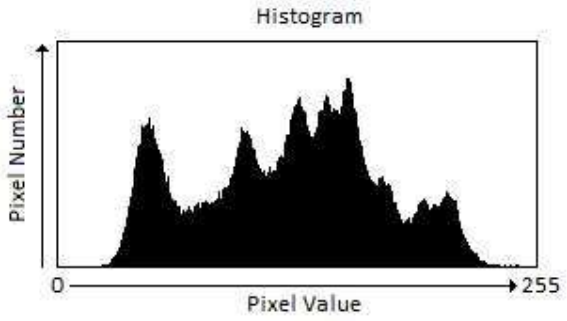
Suppose that each pixel in an image is represented by 8 bits. Imagine the image is composed of 8, 1-bit planes ranging from bit plane 1 (LSB) to bit plane 8 (MSB). In terms of 8-bits bytes, plane 1 contains all lowest order bits in the bytes comprising the pixels in the image and plane 8 contains all high order bits. The lower order bits of an image control the texture of the image whereas the higher order bit contribute to the finer details of the image.



- Histogram of an image:

  Image histogram is a type of histogram that acts as a graphical representation of the tonal distribution in a digital image. It plots the number of pixels for each tonal value. By looking at the histogram for a specific image a viewer will be able to judge the entire tonal distribution at a glance.

  In MATLAB histogram of an image can be viewed using: imhist('name_of_image').



- Median Filter:

The Median Filter is a non-linear digital filtering technique, often used to remove noise from an image or signal. Such noise reduction is a typical pre-processing step to improve the results of later processing (for example, edge detection on an image). Median filtering is very widely used in digital image processing because it preserves edges while removing noise.

In MATLAB median filter can be applied using medfilt2('name_of_image').

- Salt and Pepper Noise:

Salt-and-pepper noise is a form of noise sometimes seen on images. It is also known as impulse noise. This noise can be caused by sharp and sudden disturbances in the image signal. It presents itself as sparsely occurring white and black pixels.

In another words (in the sense of pixels), so for salt noise the values of this noise type are high (255 … 250), and for the pepper noise the values of this noise type are low (5 … 0)

An effective noise reduction method for this type of noise is a median filter or a morphological filter. For reducing either salt noise or pepper noise, but not both, a contra harmonic mean filter can be effective.

In order to apply salt and pepper noise on image in MATLAB we use the following code:

imnoise(I,'salt & pepper',d)
"J = imnoise(I,'salt & pepper',d) adds salt and pepper noise to the image I, where d is the noise density. This affects approximately d*numel(I) pixels. The default for d is 0.05." then (number of Black Pixels + number of White Pixels)/numel(grayImage) should approximately equal the value of d you used. It is safe to assume the proportion of black pepper noise and white salt noise should be about the same - 50% of each type.

CAUSES:

1. Salt-and-pepper noise is generated by errors during analog to digital conversion or data transfer.
2. Sensor heat while clicking an image

- PSNR and SNR:

PSNR stands for peak signal to noise ratio which is used to measure the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation.

$$\begin{aligned} PSNR &= 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right) \\ &= 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \\ &= 20 \cdot \log_{10}(MAX_I) - 10 \cdot \log_{10}(MSE) \end{aligned}$$

SNR is a measure independent of the type of noise that you are analysing, but the significance and usability of the parameter is very dependant of the type of noise. SNR is useful in random and uniformly distributed noise (like gaussian), but in images with other non-linear noises (like degradation between a threshold or degradation in a specific area and not the whole image) could give bad results. The below mentioned formula is from Digital Image Processing book where f^ is the noisy image and f is the original image.

$$\text{SNR} = \frac{\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\hat{f}(x,y)^2}{\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}[f(x,y)-\hat{f}(x,y)]^2}$$

Theory

There are two main methods for embedding watermark image i.e. in spatial domain or frequency domain. In spatial domain there are three different methods to hide the image:

- Bit modification: This is the simplest spatial domain algorithm. The least significant bit of each 8-bit pixel is written over by a bit from the watermark. It may be carried out in two ways: either the watermark information can be inserted over each and every pixel of cover image, or the busier areas of the image can be calculated and the watermark is embedded there to enhance imperceptibility. The least significant bits are highly sensitive to noise, so that the watermark can easily be removed by image manipulations such as rotation and cropping. Thus, the LSB method provides high imperceptibility and less robustness.
  If we embed the watermark image in higher bit plane then they are easily visible but are resistant to various attacks. Other method can be to use a number of consecutive bit planes to hide the watermark.
- Log-average Luminance Method for Colour Images: A coloured-image is divided into blocks after converting the RGB coloured image to YCbCr colour space. To embed the watermark, 16 blocks of size 8x8 are selected and used to embed the watermark image into the original image. The selected blocks are chosen spirally (beginning form the centre of the image) among the blocks that have log-average luminance higher than or equal the log-average luminance of the entire image. Each byte of the monochrome watermark is added by updating a luminance value of a pixel of the image. The watermark is taken to be a monochrome image. If the byte of the watermark image represented white colour (255) a value α is added to the image pixel luminance value, if it is black (0) the α is subtracted from the luminance value. To extract the watermark, the selected blocks are chosen as the above, if the difference between the luminance value of the watermarked image pixel and the original image pixel is greater than 0, the watermark pixel is supposed to be white, otherwise it supposed to be black.
- Block Probability in Spatial Domain Method: A binary watermark image is permutated using sequence numbers generated by a secret key and Grey code, and then embedded four times in different positions by a secret key. Each bit of the binary encoded watermark is embedded by modifying the intensities of a non-overlapping block of 8x8 of the blue component of the host image. The extraction of the watermark is by comparing the intensities of a block of 8x8 of the watermarked and the original images and calculating the probability of detecting '0' or '1'.

Spatial domain techniques are easier to implement and have lower computational complexity. But as images are embedded using a simple method, it is relatively easier for a third person to separate out the watermark, thus defeating the whole purpose. It also very susceptible to a wide range of attacks, hence not robust.

Frequency domain techniques, on the other hand, has better imperceptibility and robustness. But the computational cost is higher. For e.g. watermarking in the DCT domain needs pre-processing operations such as inverse entropy coding and inverse quantization. Also, we can combine more than one frequency domain methods to get better results.

In this project we will embed the watermark image using bit modification technique and we will try to test the robustness of hidden image by using many different bit planes.

Experimentation

To describe the procedure briefly:

->First select both the main content and watermarking image

->Then convert the watermark image to binary image since we hide it in 1-bit plane.

->Select the bit plane.

->Embedded the hidden image

->To check robustness, attack the image with noise and apply various functions like reflection, etc.

-> Recover the embedded image

->Show the results for visual comparison

->Compare the PSNR and SNR of the original hidden image and recovered the hidden image.

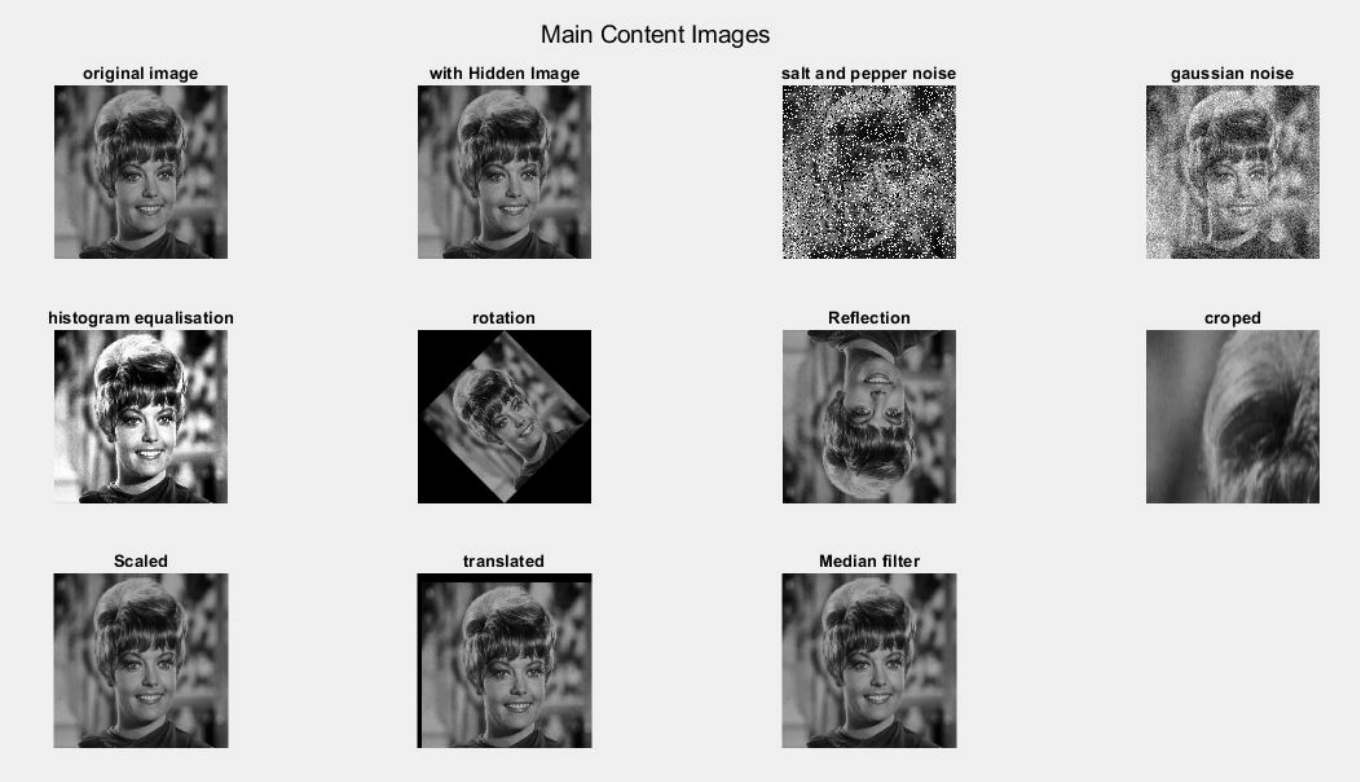
Results

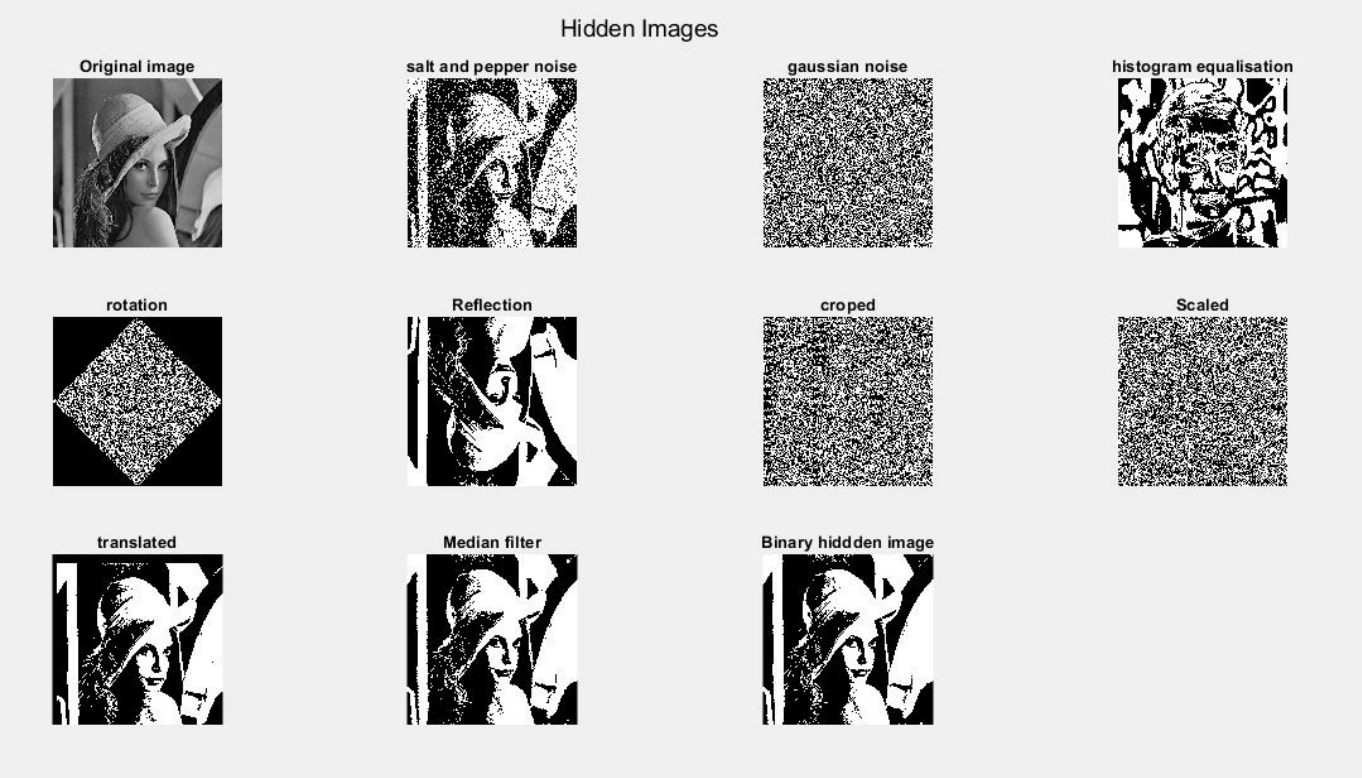
Taking Threshold value as 0.4,
salt and pepper noise = 0.25
gaussian noise = 0.15
watermarking image as lenna and main content image as Zelda

LENNA WATERMARKING IMAGE

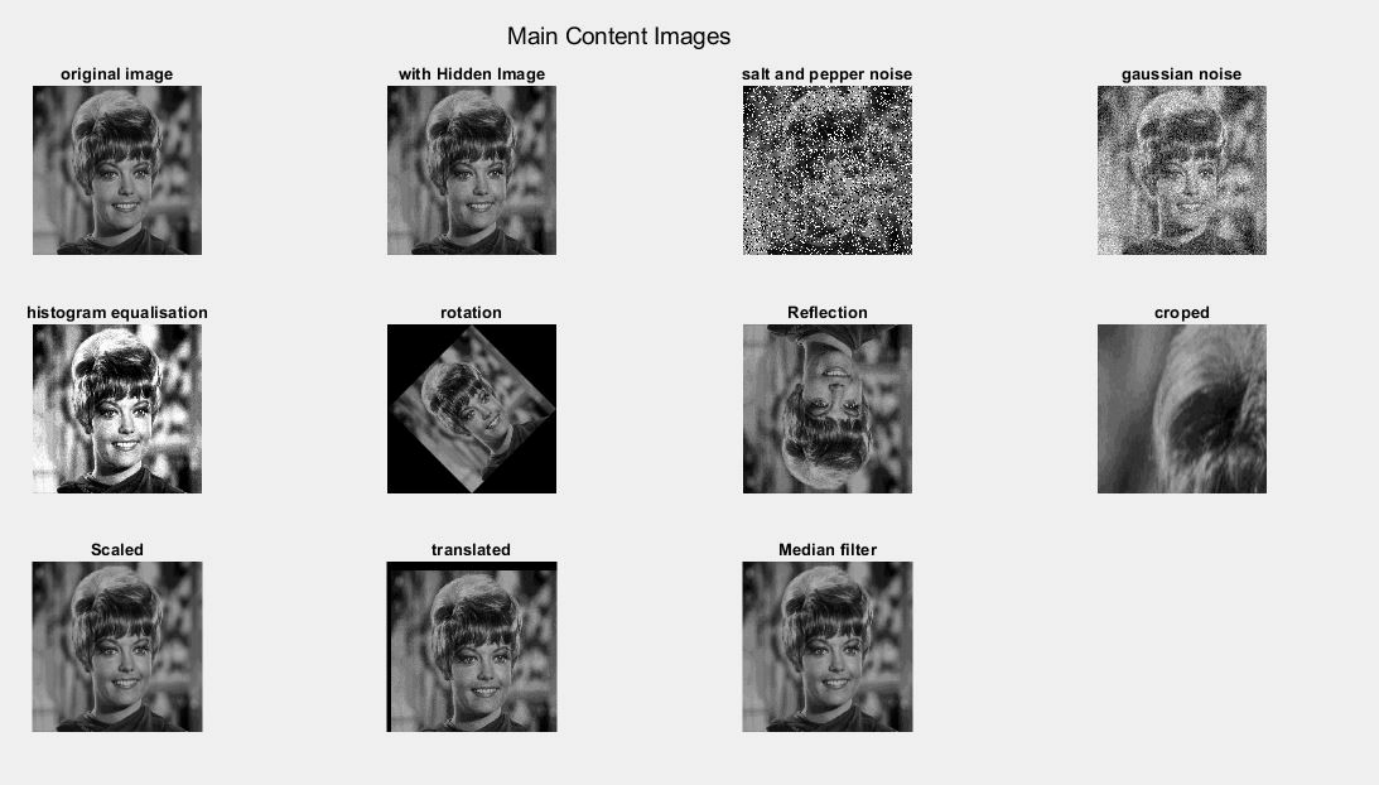
ZELDA MAIN IMAGE

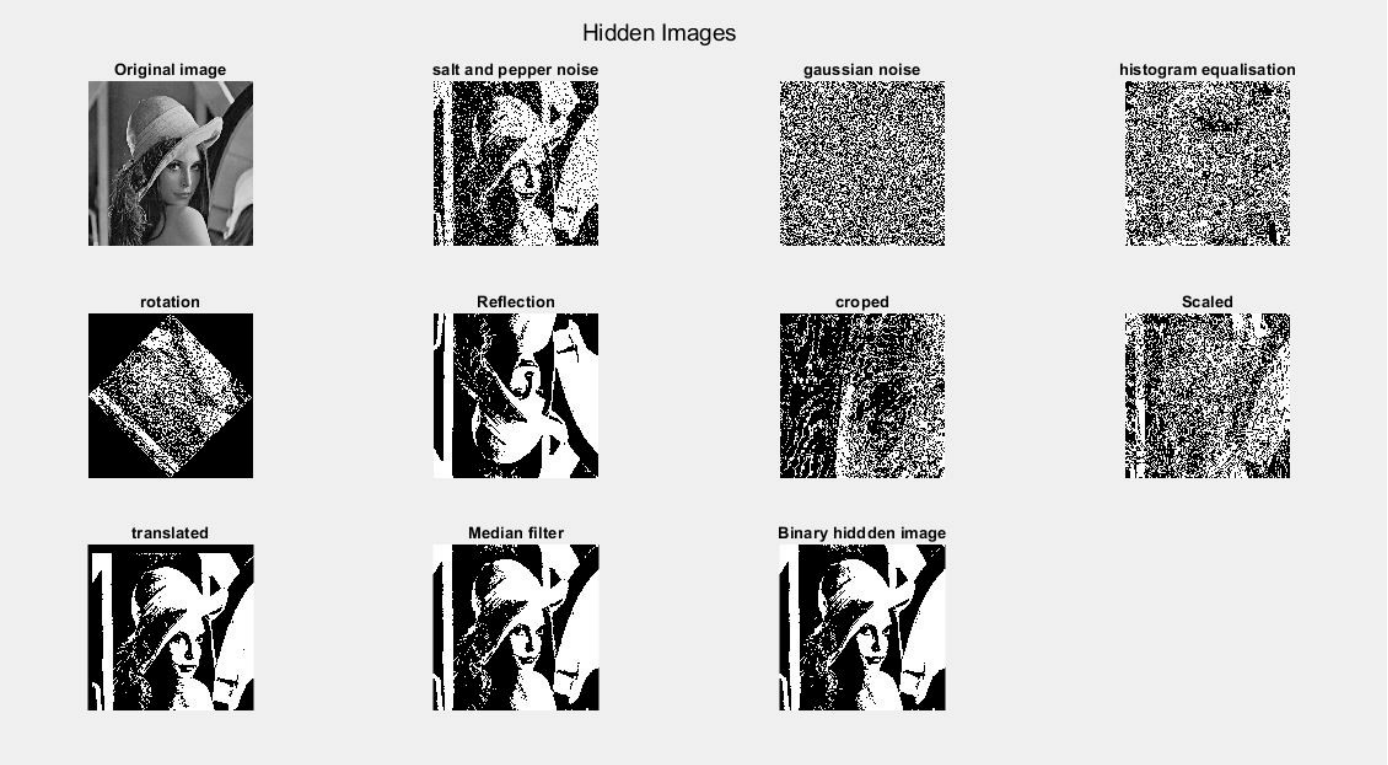
Using bit plane 1





Using bit plane 4





Using bit plane 7

From the above figures we can see that as we hide the image in higher bit plane, we get a clearer extracted image but the original image carrying the hidden image gets distorted. Since the higher bit planes carry more information about the edges and structure of the image so, if we replace those bits by that of watermarking image, we lose a lot of important structural information and thus get a distorted image. But if we use lower bit planes, all the noise attacks generally effect the lower bit planes.

PSNR

bit plane	salt and pepper noise	gaussian noise	histogram equalisation	rotation	Reflection	Croped	Scaled	translated	Median filter
1	9.041515727	3.008842304	2.918339501	3.25072708	4.42869202	3.06770131	3.00443919	5.085401977	14.40450749
4	9.019384504	3.015239737	2.727004778	3.35636124	4.42869202	3.25219818	4.725743	5.085401977	15.58441592
7	9.01793071	2.908424246	2.740715768	3.45632278	4.42869202	3.28935036	9.30186657	5.085401977	17.50247212

SNR

bit plane	salt and pepper noise	gaussian noise	histogram equalisation	rotation	Reflection	croped	Scaled	translated	Median filter
1	5.713017245	-0.319656178	-0.41015898	-0.0777714	1.10019354	-0.2607972	-0.32405929	1.756903496	11.07600901
4	5.690886023	-0.313258745	-0.601493704	0.02786276	1.10019354	-0.0763003	1.39724452	1.756903496	12.25591744
7	5.689432229	-0.420074236	-0.587782713	0.1278243	1.10019354	-0.0391481	5.97336809	1.756903496	14.17397363

In the formula of SNR, the denominator is the square of difference between the original watermarking image and extracted image so as we can see that the value of SNR is increasing with the bit plane used, thus the difference must be decreasing.

If we hide the image in higher bit plane, the watermark is more robust but the cost paid is visual distortion of the original image. But if we use lower bit planes than the watermarking image is more likely to get distorted while transmission or other methods.

Conclusion

Digital Image Watermarking is currently a very important topic for media, for university administrators and for the publishing industries. In digital watermarking robustness describes whether the watermark can be reliably detected after any changes in the original image like rotation, scaling, cropping or addition of noise. It exists for entertainment companies and libraries because it offers the promise of better protecting their multimedia content from piracy. It is transparent in use, does not increase files sizes, and yet is highly robust and secure. The understanding of the theory behind digital watermarking will lead to the design of more reliable systems for more applications.

References

[1] S. Lyu and H. Farid, “Steganalysis using color wavelet statistics and oneclassvector support machines,” in Proc. SPIE Security, Steganography,Watermarking Multimedia Contents, vol. 5306, E. J. Delp III and P. W.Wong, Eds., 2004, pp. 35–45.

[2] J. Fridrich, “Feature-based steganalysis for JPEG images and its implicationsfor future design of steganographic schemes,” in Proc. Inf. HidingWorkshop, Springer LNCS, vol. 3200, 2004, pp. 67–81.

[3] Gonzalez, Rafael C., and Paul A. Wintz. "Image Compression Standards."Digital Image Processing. 2nd ed. Upper Saddle River, NJ: Prentice-Hall, 2002.492-510. Print.

[4] Lyu, S., & Farid, H.(2006).Steganalysis using higher-order image statistics.Forensics and Security, IEEE Transactions on, 1(1), 111-119.

[5]Kundur, Deepa. Watermarking with diversity: Insightsand implications. IEEE Multimedia, 2001, 8(4), 46-52.

[6] Page, Thomas. Rights management: Digitalwatermarking as a form of copyright protection. Computer Law & Sec. Rep., 1998, 14(6), 390-92.

[7] Rao,N.V.& Pandit, S.N.N. Multimedia digital rightsprotection using watermarking techniques. Inform.Sys. Sec., 2007, September, 93-99.

[8] Rosenblatt, Bill. DRM, law and technology: AnAmerican perspective. Online Inform. Rev., 2007