# FPGA based Multimedia Security in Real-time Applications

Endsem report

By
**Kunal Keshav Damame**
(121901050)

Under the guidance of

**Dr. Subramanyam Mula**
and
**Dr. Siva Ram Krishna Vadali**
Principal Scientist, CSIR-CMERI Durgapur

INDIAN INSTITUTE
OF TECHNOLOGY
PALAKKAD

Department of Electrical Engineering

## 1 . Introduction to project

The project's goal is to investigate specialized VLSI solutions for video watermarking and detection, as this is a computationally resource intensive activity and it demands quicker processing for on-the-fly embedding and detection of the watermark in live video streams .

Data sharing is increasing very rapidly due to the access of the internet for the masses especially in the last decade . Multimedia (text,video,image and audio) can easily be accessed by unauthorized users , for example it is very easy to make multiple copies of the content developed by someone without his/her consent , which just undermines the effort that was put into developing it . The secrecy, integrity, and authenticity of multimedia data are critical for the effective deployment of any multimedia media service. Traditional hardware (or software) based computer and network security algorithms do not sufficiently address the needs of content security. For a long time, encryption has been depended upon to safeguard digital material, but it now appears that encryption alone is insufficient to protect digital data throughout its existence . The protection of audio and video content owners' intellectual property rights has become a top priority. As a research area, designing security methods that can manage the processing of high bandwidth information while yet allowing some control over the intellectual property after it is conveyed has gathered attention.

Researchers are focused on digital watermarking to assure multimedia security. Digital watermarking is one type of authentication technology that has gathered the interest of academics . As a result, digital watermarking has been developed as an additional layer of security. The core concept is to incorporate information into digital content in an imperceptible manner. This watermarked signal should be able to withstand most typical signal processing and, if necessary even malicious signal processing. Security and digital rights protection, authentication, traitor tracking, forensics, adversarial signal processing, covert communication, and surveillance are among areas where digital watermarking has been recognized as a viable solution. It normally adds invisible copyright watermarks to the host data and encrypts it further. These invisible copyright watermarks are certification, symbols, digital signatures, and so on. A robust watermarking system must satisfy the basic design requirements like imperceptibility, robustness, detection with higher accuracy, and payload capacity.

Some desirable features of watermark are given below :

*Imperceptibility of the watermark*

If the human eye can't tell the difference between an original and a watermarked video, the watermarking algorithm is undetectable. The watermarked video should be nearly undetectable to the naked eye, and should appear identical to the original video.

*Higher detection Accuracy and False alarm Rate should be low:*

The embedding should be done in such a way that it can be detected with more precision while maintaining the aforementioned two features, and the suitable detector should be utilized to reduce the false alarm rate.

*Robustness of the watermark:*

The watermark should be able to endure compression standards in which it is subjected to unintended attack on the watermark, as well as purposeful attacks on the watermark that result in data loss. Only authorized individuals may read the watermark since they must know the secret key that creates the pseudo-random sequence and the manner the watermark is embedded onto the image.

*Proper Payload Carrying Capacity :*

The number of watermarking bits included in an image or video is referred to as the data payload. The payload of the watermark has an impact on its imperceptibility. The watermark becomes more perceptible as the payload increases, and vice versa.

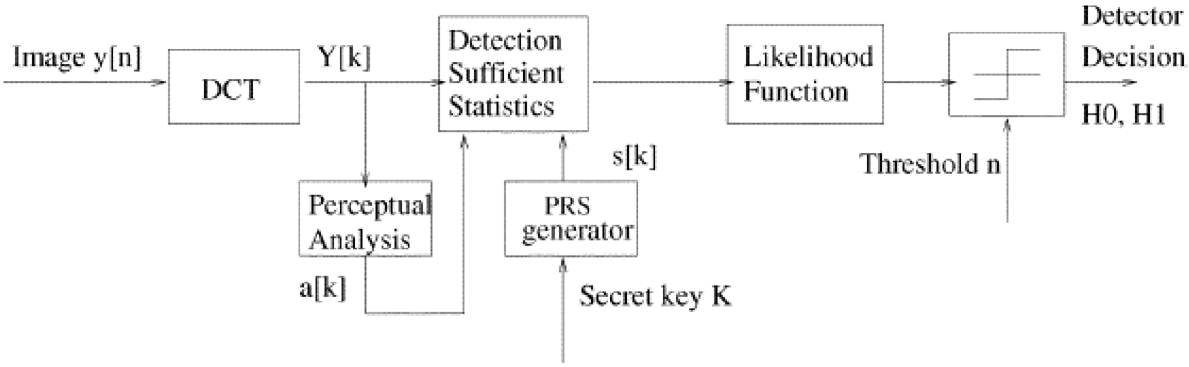
Due to conflicting characteristics b/w payload bits and perceptibility , these requirements are not been able to meet simultaneously , so it is very important to find the right balance between these two for various different types of watermarking techniques , thus the techniques used for the images and videos differ based on the requirements of the available data .

Video watermarking and detection is a computationally complex process in general. Furthermore, faster processing is required for on-the-fly watermark embedding and detection in live video streams. Though difficult, video piracy should be prevented by dynamically processing multimedia content as the video is being streamed, resulting in actual "on-the-fly" multimedia processing.

However, given the difficulties associated with the video piracy problem, there is a strong need to design-develop effective solutions that will greatly speed up the process by installing specific target hardware. This project will investigate specialized VLSI solutions and their FPGA/VLSI implementation for the specified challenge.

## 2 . Overall Process of Watermarking

The watermarking of video usually comprises of two parts embedding and retrieval of watermark :



### Embedding

Message encoding :

Any message is decoded into a sequence of zeros and ones, and then reorganized to higher dimensions either by filling zeros at the end or by repeating the same message to cover the entire image in the transform domain. The latter will increase the image's robustness, but at the expense of human perceptibility.

Pseudo-Random Sequence generator using a key (Encryption):

The Message is then fed into a pseudo random sequence generator using a key . This type of sequence appears random , but is not , in fact it is only possible to replicate this sequence if you have a message and key with you , even a slightest change in message will alter the sequence with zero correlation to the previous message sequence . The length of the sequence is determined by the various changes used to incorporate the picture. A separate sequence corresponding to a given bit (either 0 or 1), as well as two alternative sequences for 0 and 1, can be found depending on the transformations.

Masking to enhance perceptibility:

This mask ensures that the watermark is undetectable to the naked eye while also allowing for the most pixel value changes feasible in order to achieve enhanced robustness and detectability. It's done by multiplying the perceptual mask by the pseudorandom sequence. This mask is created by taking into account transform domain coefficients, human eye characteristics, and so on.

Transform domain watermarking:
The images and the obtained watermark to embed  are converted to the frequency domain by using the transformation. Then, the watermark image is embedded into the original host image by altering the transform domain coefficients of the host image through various transformations like DCT, DFT, DWT, and SVD.

## Retrieval :

Approximating the original data :

The watermarked picture is transformed back to transform domain, and the transform domain coefficients that were changed during the embedding stage are taken into account. The data is transferred and received . At the received end we can simply subtract the original image from the watermarked image and retrieve the watermark , but in practical case it is not feasible as it takes lot of storage space , so since both the coefficients of image and watermark found to be follow gaussian/Cauchy distribution , the resulting image coefficients follow the same , now the original image can be estimated using the gaussian/Cauchy distribution which can be approximated by taking large image database  , and thus we don't need the original image to detect the presence of watermark , as it can be approximated by using large sample of similar images .

Detector to detect the change in the original data:
By approximating with a specific distribution, the change that is noticed in the watermarked picture (transform domain) is identified using a detector by setting a threshold value.

## To explore dedicated VLSI solutions

It must be implemented in hardware using a field programmable gate array. To provide the hardware architecture for a digital video watermarking system that can authenticate video streams in real time. For the hardware architecture, FPGA-based prototyping must be built.

## 3 . Work Done

### DCT Domain

Implemented the watermarking on image using the DCT domain without any perceptual mask and the watermark was also very standard . The obtained image after watermarking was having some distortions at the edges due to lack of using the perceptual mask . The image used was one of the standard images from the matlab database. The DCT was implemented on the whole image and not on smaller blocks of the image , implementing it on smaller blocks gets us better results.

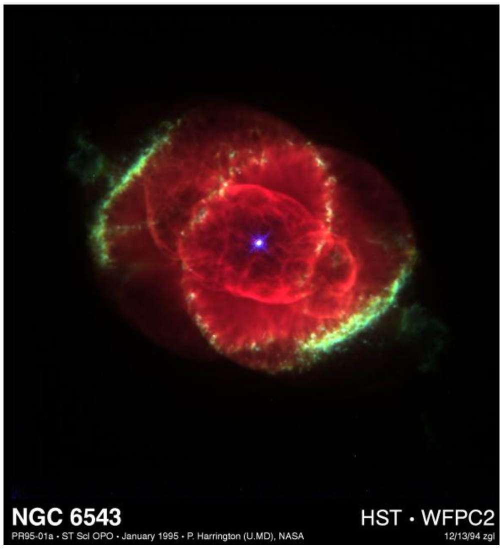
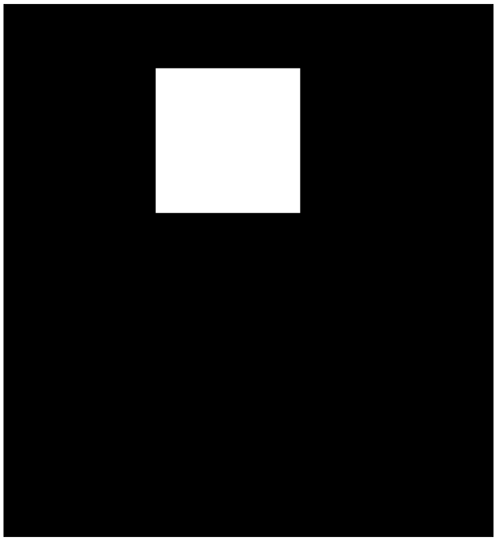

NGC 6543
HST • WFPC2
PR95-01a • ST ScI OPO • January 1995 • P. Harrington (U.MD), NASA
12/13/94 zgl

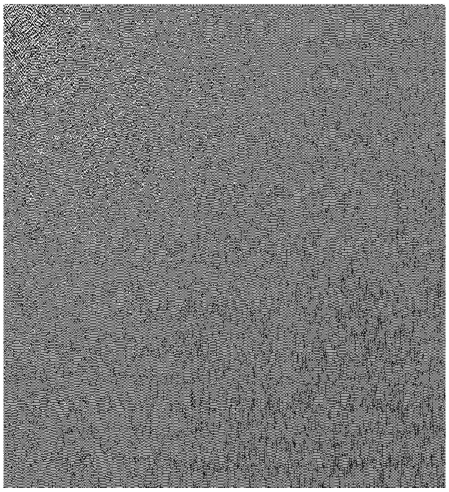
Image watermarked

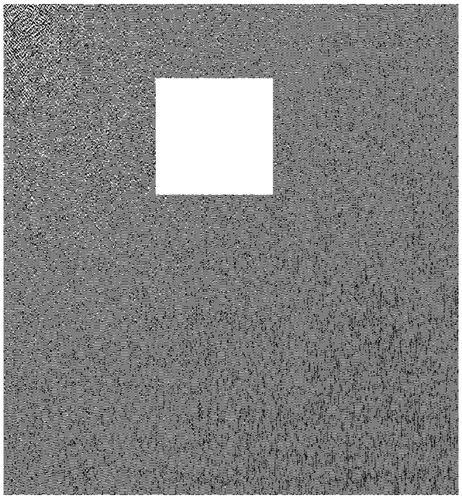


Watermark embedded

The DCT of the image is calculated in the RGB Domain . A water mark was added to the coefficients of DCT of each R,G,B domain separately with the same amount of weights . Research in this area has proved that doing manipulations on the luminance part in the yuv domain is more perceptual to the eye .

*DCT coefficients before and after watermarking of Red signal (No mask)*

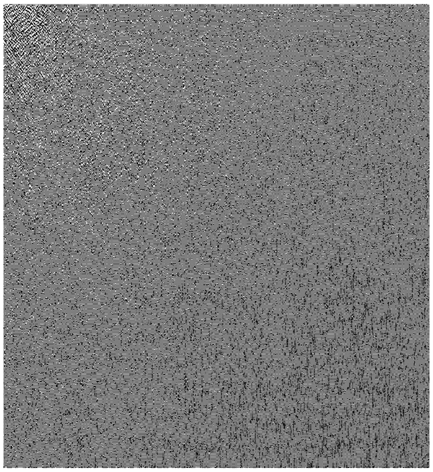


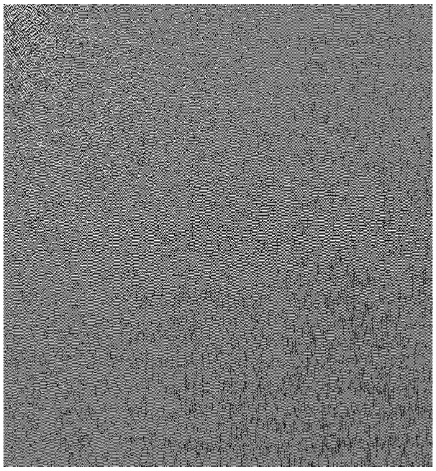


Before After

*DCT coefficients before and after watermarking of Red signal ( perceptual mask)*

The perceptual mask is now added in the addition of watermark in which we multiply the coefficients of watermark with the corresponding coefficients of image and weight , thus making the watermark more imperceptible.

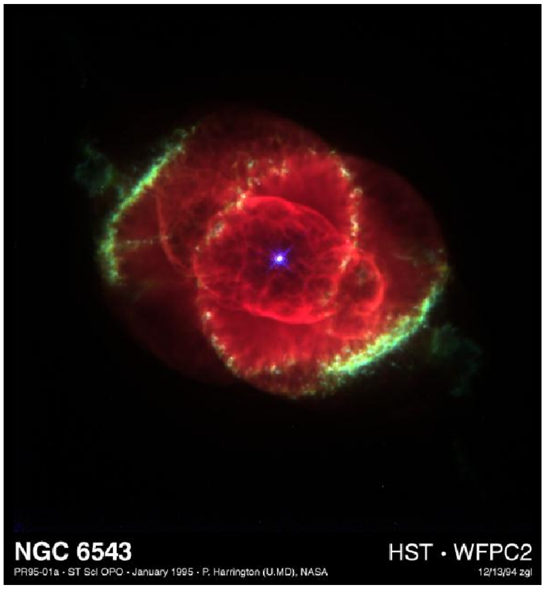




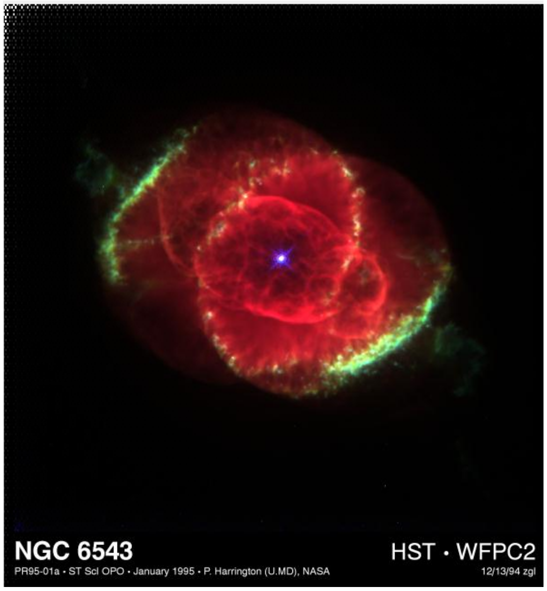
Before After

As we can see there is very less distortion in the frequency domain of the signal after we introduced the perceptual mask , thus making the image more imperceptible.

### *Resultant image after watermark (With and without perceptual mask)*


NGC 6543
PR95-01a • ST ScI OPO • January 1995 • P. Harrington (U.MD), NASA
HST • WFPC2
12/13/94 zgl

With Perceptual Mask

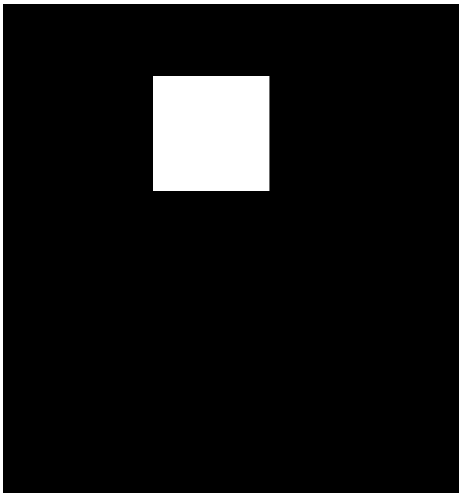

NGC 6543
PR95-01a • ST ScI OPO • January 1995 • P. Harrington (U.MD), NASA
HST • WFPC2
12/13/94 zgl

Without perceptual Mask

The image which is obtained after embedding the watermark (without mask) is having some distortions at the edge on the top left corner , thus it does not satisfy the criterion of imperceptibility . But the image on the left does not have that distortion thus it satisfies the imperceptibility criterion. This is one of the reasons why a perceptual mask is a must whenever applying the watermark in any domain , there are various different masks other than the one I used here .

The above methods of embedding the watermark are not very robust to attacks as the watermark is embedded in specific coefficients , to overcome this problem of attacks , usually the watermark is embedded using more advanced techniques and upon retrieval , only the probability that water mark was present or not is captured , which can sometimes go upto accuracy of 99.999 % in some cases.

*Recovered Watermark*



The watermark is simply recovered using the known original image , which is certainly not the way to go as it wastes a lot of storage space.

Effect of Various attacks on watermarks (JPEG compression attack)

Jpeg compression is a very common form of image compression technique that helps in significantly reducing the data size of the image . The below demonstrates the effect of the data compression on the recovered watermark.

without compression(watermark recovered)

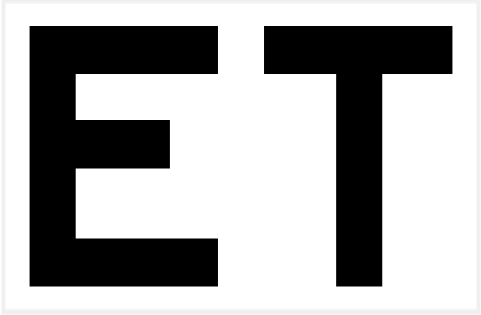
watermark recovered after compression

As we can clearly see that some data points are lost in the compression attack so a complete watermark is not recovered but some distorted version of it is recovered.

## Embedding the watermark and detection using statistics

Embedded the watermark in DWT and DCT domain and managed to recover the watermark in DWT domain .

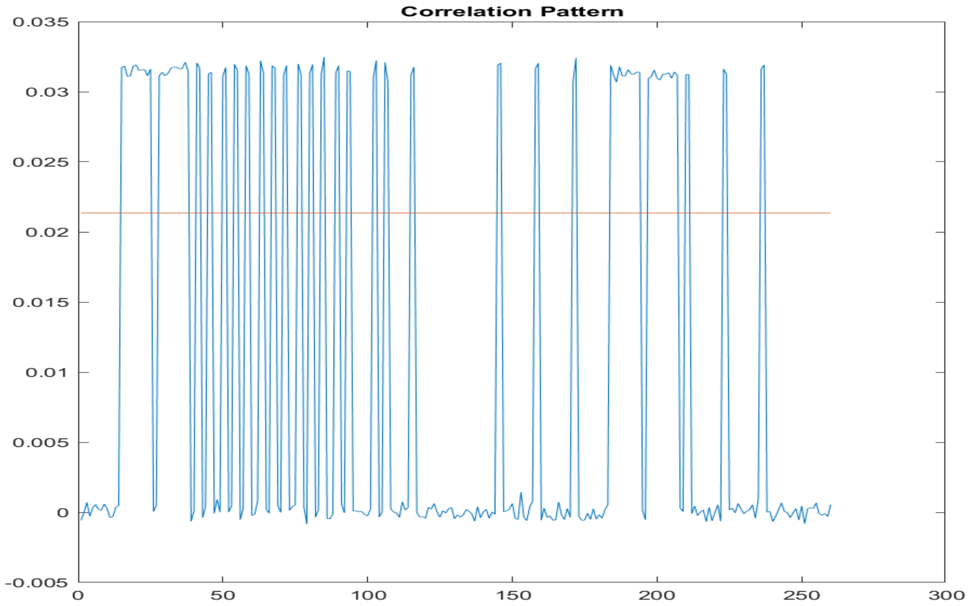
original image



Watermark embedded

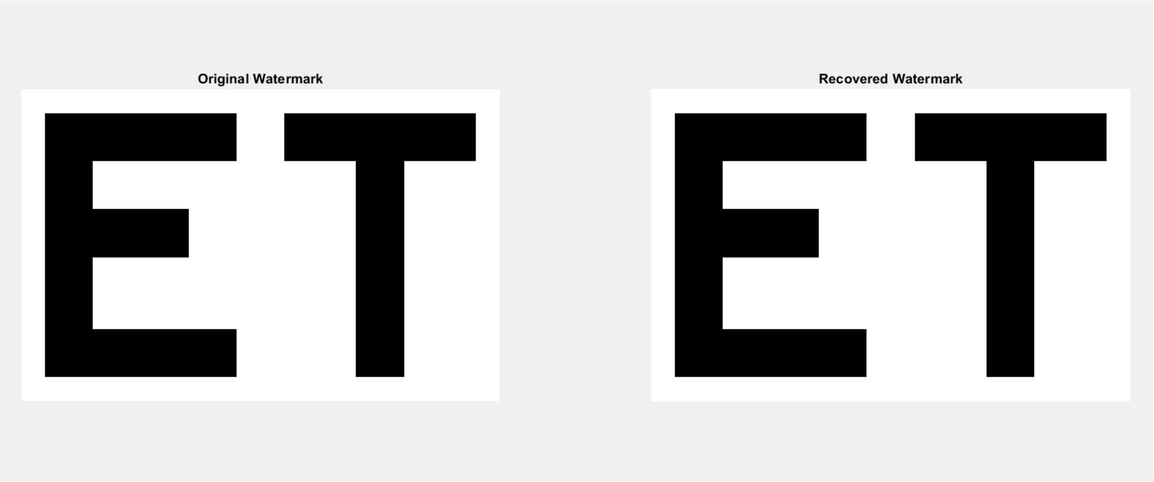
## Detection

The watermark was embedded in approximation coefficients as they carry the least amount of data and can hold the information without much affecting the quality of the image . Later correlation of the recovered coefficients is found with the original sequence generated with use of the key and a proper threshold is set , and bits are compared to find the recovered watermark.



The correlation pattern corresponds to each bit embedded , if the correlation is greater than the threshold , then the original bit was zero and if less than threshold, then the original bit was one .

Original vs recovered watermark



The original watermark and the recovered watermark are very much similar to each other .

Future Work

Make an optimal detector who can only detect if the watermark is present or not from any of the images without knowing beforehand what the watermark is . Then extend this technique to video where we take any random frames and try to find if the watermark is present . Then develop a VLSI architecture to implement the same in verilog . Finally the verilog design will be mapped on to FPGA.

## 4 . References

[1] Aaqib Rashid , Digital Watermarking Applications and Techniques: A Brief Review , International Journal of Computer Applications Technology and Research Volume 5–Issue 3 .

[2] Gwenaël Doërr and Jean-Luc Dugelay , VIDEO WATERMARKING :OVERVIEW AND CHALLENGES , Multimedia Communications, Image Group Eurécom Institute Sophia-Antipolis, France

[3]M. D. Swanson, B. Zhu, and A. H. Tewfik, “Transparent robust image watermarking,” in Proc. IEEE Int. Conf. on Image Processing, Lausanne, Switzerland, Sept. 1996, pp. 211–214.

[4] V. Capellini, M. Barni, F. Bartolini, and A. Piva, “A DCT-domain system for robust watermarking,” Signal Processing, vol. 66, pp. 357–372, 1998.

[5] G. Voyatzis and I. Pitas, “The use of watermarks in the protection of digital multimedia products,” Proc. IEEE, vol. 87, pp. 1197–1207, Jul. 1999.

[6] Md. Asikuzzaman and Mark R. Pickering “An Overview of Digital Video Watermarking”, IEEE Transactions on Circuits and Systems for Video Technology ( Volume: 28, Issue: 9, Sept. 2018)

[7]Asymptotically optimal detection for additive watermarking in the DCT and DWT domains , Athanasios Nikolaidis 1, Ioannis Pitas .
https://pubmed.ncbi.nlm.nih.gov/18237932/