

# Digital Watermarking

*By,*

**Ankush K R**

**ankush.k.r.007@gmail.com**

**+91-9739317537**

# INTRODUCTION

## Information Hiding Techniques



# WHAT IS A WATERMARK?

- A watermark is a form, image or text that is impressed onto paper, which provides evidence of its authenticity.
- A distinguishing mark impressed on paper during manufacture; visible when paper is held up to the light (e.g. \$ Bill)



Visible Watermarking



Invisible Watermarking

# WHAT IS DIGITAL WATERMARKING?

- Digital watermarking is an extension of watermarking concept in the digital world.
- A digital watermark is a pattern of bits inserted into a digital image, audio or video file that identifies the file's copyright information (author, rights, etc.).



**Image**



**Video**



**Audio**

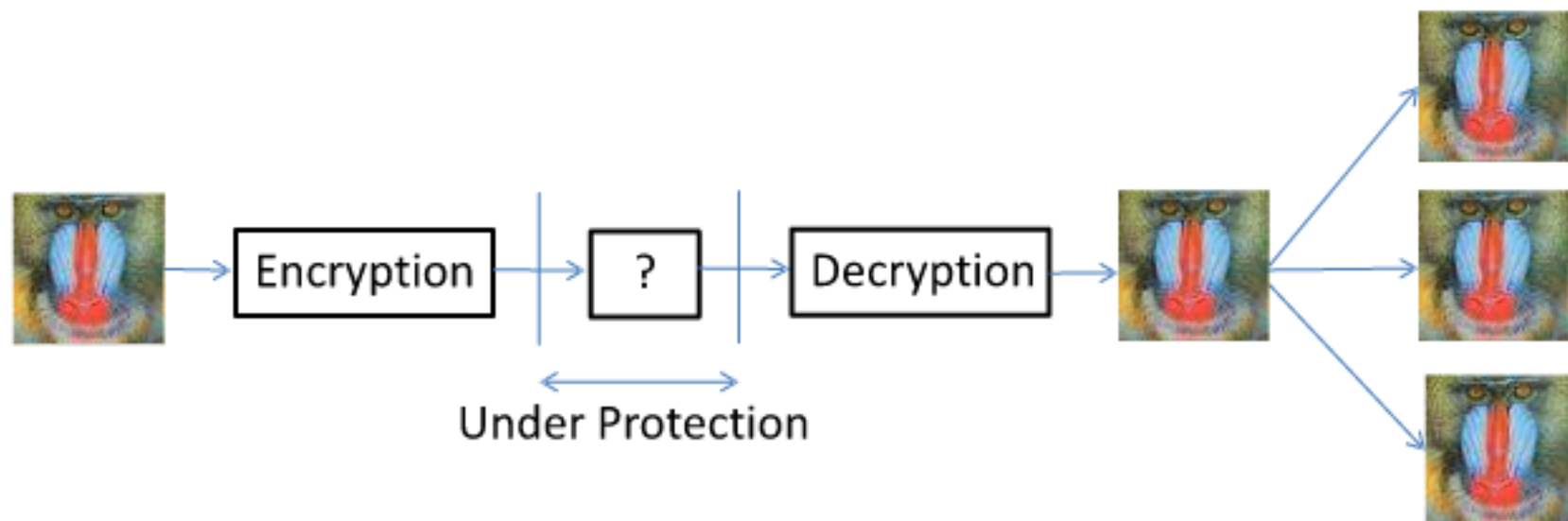
# How Watermarking is Different from Steganography and Cryptography.

## Steganography vs. Watermarking

- The main goal of **steganography** is **to hide** a message  $m$  in some audio or video (cover) data  $d$ , to obtain new data  $d'$ , practically indistinguishable from  $d$ , by people, in such a way that an eavesdropper cannot detect the presence of  $m$  in  $d'$ .
- The main goal of **watermarking** is **to hide** a message  $m$  in some audio or video (cover) data  $d$ , to obtain new data  $d'$ , practically indistinguishable from  $d$ , by people, in such a way that an eavesdropper cannot remove or replace  $m$  in  $d'$ .

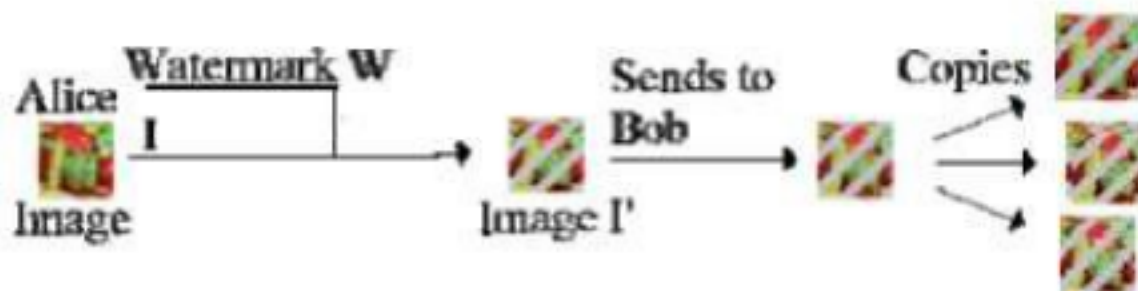
## **Cryptography vs. Watermarking**

- Cryptography is the most common method of protecting digital content and is one of the best developed science.
- However, encryption cannot help the seller monitor how a legitimate customer handles the content after decryption.
- Digital watermarking can protect content even after it is decrypted.





## Importance of Digital Watermarking



- As seen above in Fig, Alice creates an original image and watermarks it before passing it to Bob. If Bob claims the image and sells copies to other people Alice can extract her watermark from the image proving her copyright to it.
- The caveat here is that Alice will only be able to prove her copyright of the image if Bob hasn't managed to modify the image such that the watermark is damaged enough to be undetectable or added his own watermark such that it is impossible to discover which watermark was embedded first.

# WATERMARKING CLASSIFICATION

*Visible & Invisible Watermarking*

*Robust & Fragile Watermarking*

*Asymmetric & Symmetric Watermarking*

*Public & Private Watermarking*

*Steganographic & Non-steganographic Watermarking*



## Visible Watermarking

- Visible watermark is a translucent overlaid into an image and is visible to the viewer. Visible watermarking is used to indicate ownership and for copyright protection.



**Original Image**



**Watermarked Image**

## Invisible Watermarking

- Invisible watermark is embedded into the data in such a way that the changes made to the pixel values are perceptually not noticed. Invisible watermark is used as evidence of ownership and to detect misappropriated images.



**Original Image**



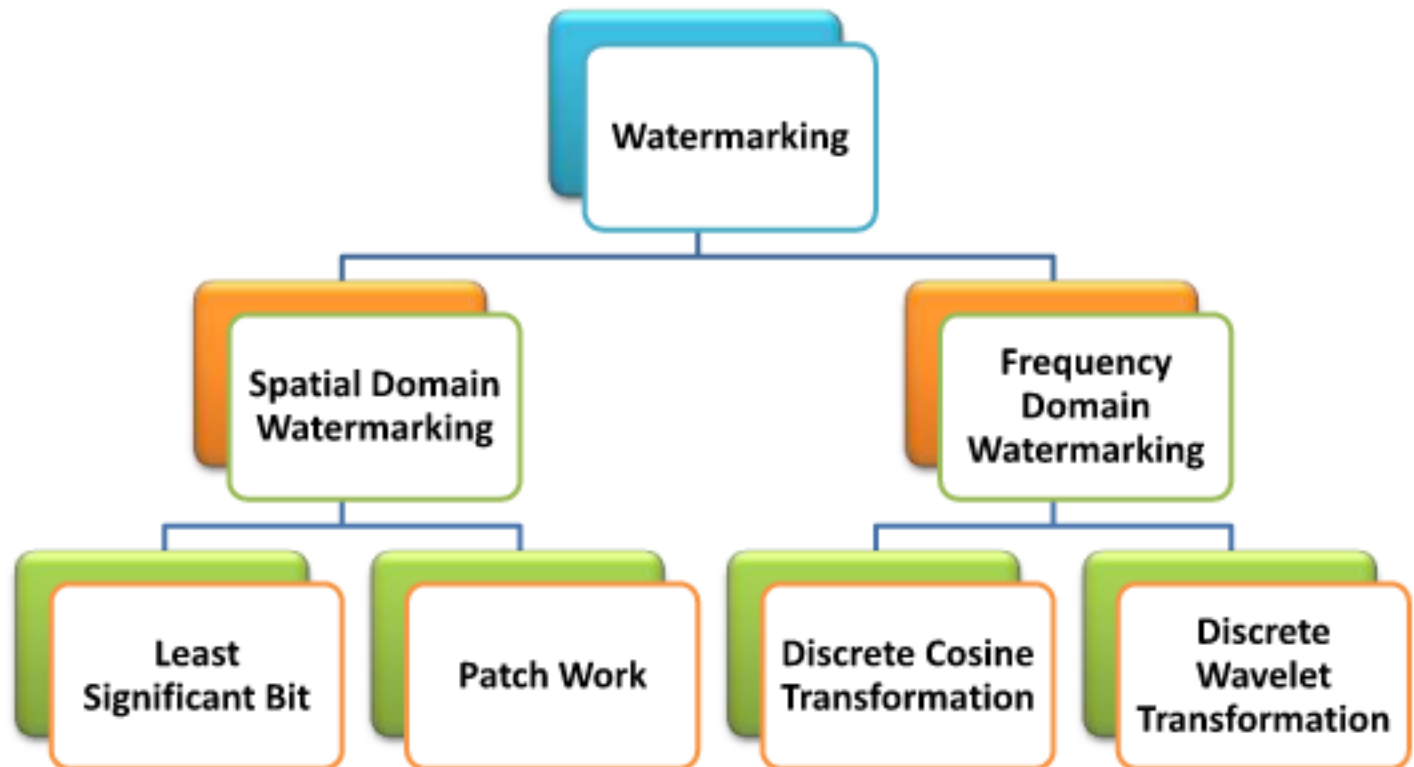
**Watermarked Image**

## Dual Watermarking

- Dual watermark is the combination of visible and invisible watermark. An invisible watermark is used as a backup for the visible watermark.

# **WATERMARKING TECHNIQUES**

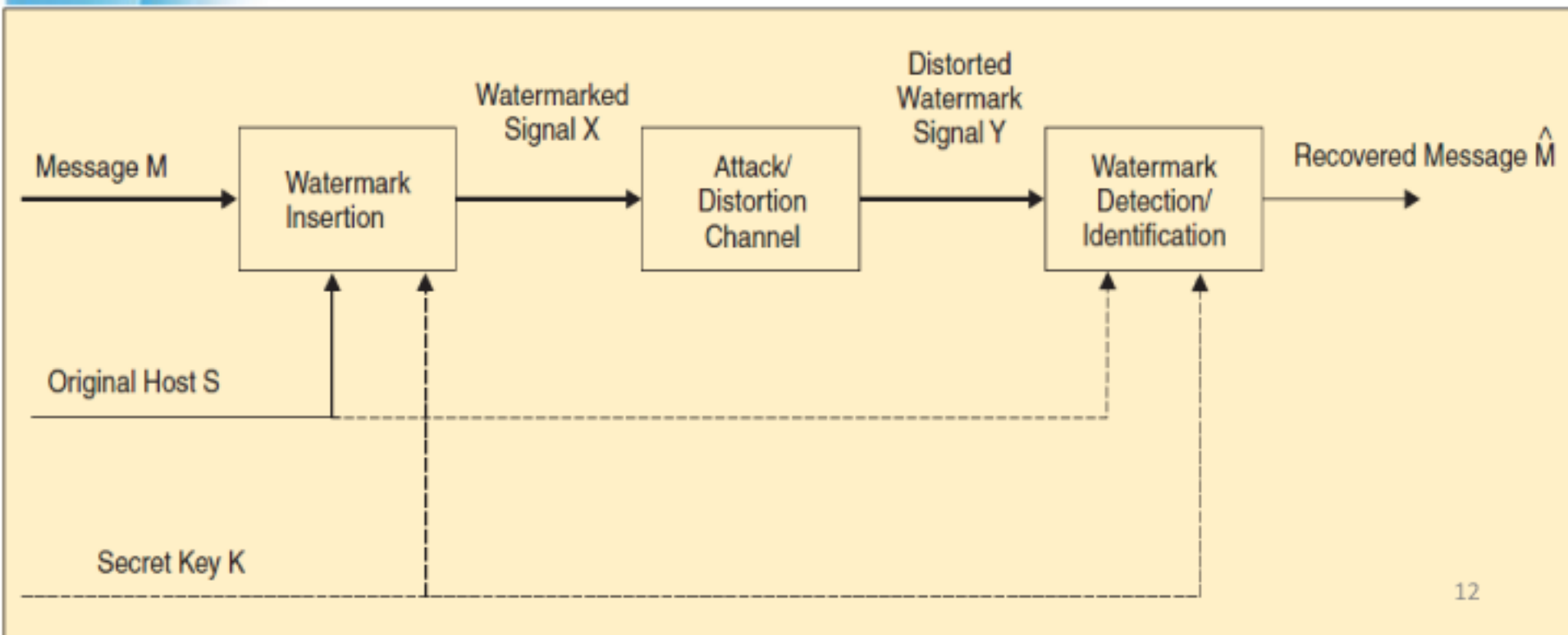
**(According to Working Domain )**



# Digital Watermarking Life Cycle Phases

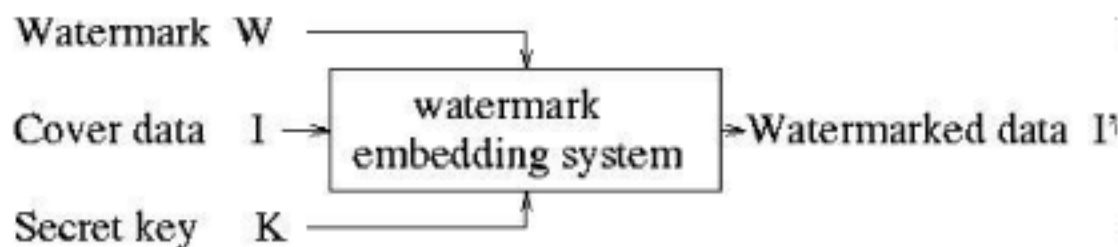
A watermarking system is usually divided into three distinct steps.

- Embedding
- Attack
- Detection



# Embedding

In embedding, an algorithm accepts the host and the data to be embedded, and produces a watermarked signal.



Inputs to the scheme are the **watermark**, the **cover data** and an optional **public or secret key**. The output are **watermarked data**. The key is used to enforce security.

# Attacks

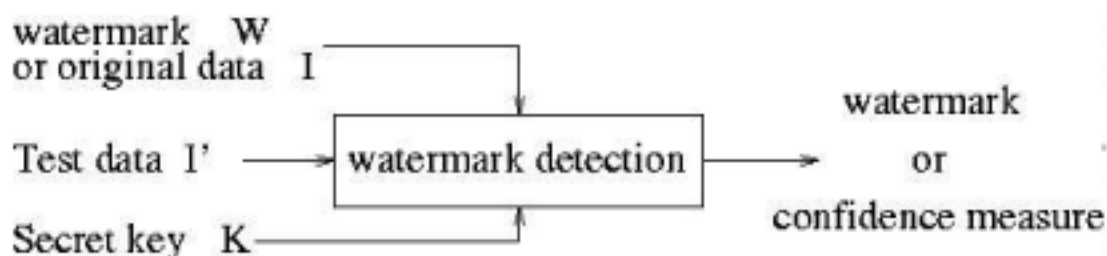
The watermarked digital signal is transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an *attack*.

## Few Possible Attacks

- **Robustness attacks** :Which are intended to remove the watermark such as... JPEG compression, cropping, etc.
- **Presentation Attacks** :Under watermark detection failure they come into play. Geometric transformation, rotation, scaling, translation, change aspect ratio, affine transformation etc.
- **Counterfeiting attacks** :Rendering the original image, generate fake original.

## Extraction/Detection

*Detection* (often called extraction) is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was unmodified during transmission, then the watermark still is present and it may be extracted.



**Inputs** to the scheme are the **watermarked data**, the **secret or public key** and, depending on the method, the **original data and/or the original watermark**. The **output** is the **recovered watermarked  $W$**  or some kind of **confidence measure indicating how likely it is for the given watermark at the input to be present in the data under inspection**.



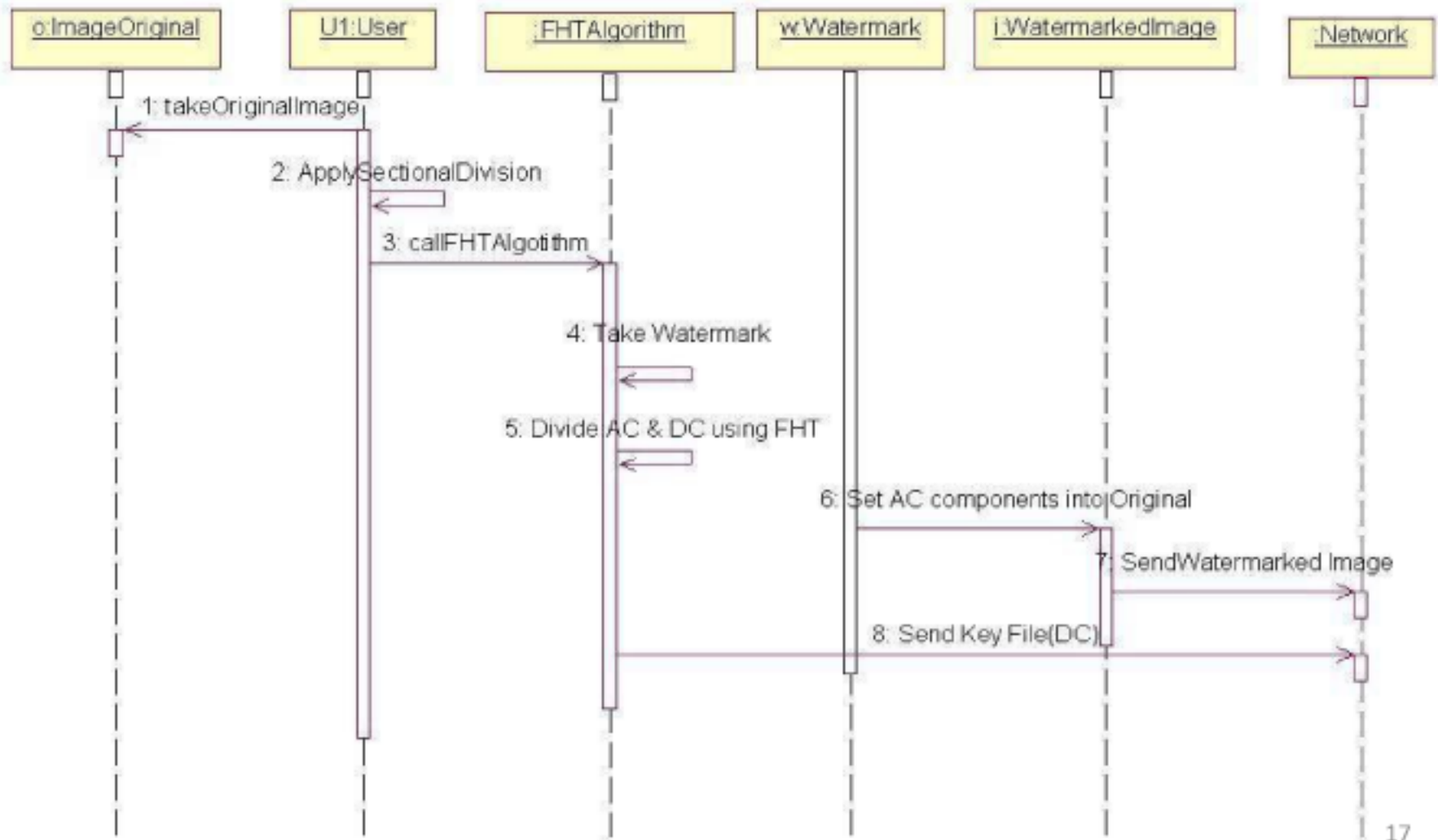
# ALGORITHM

## FAST HADAMARD TRANSFORM(FHT)

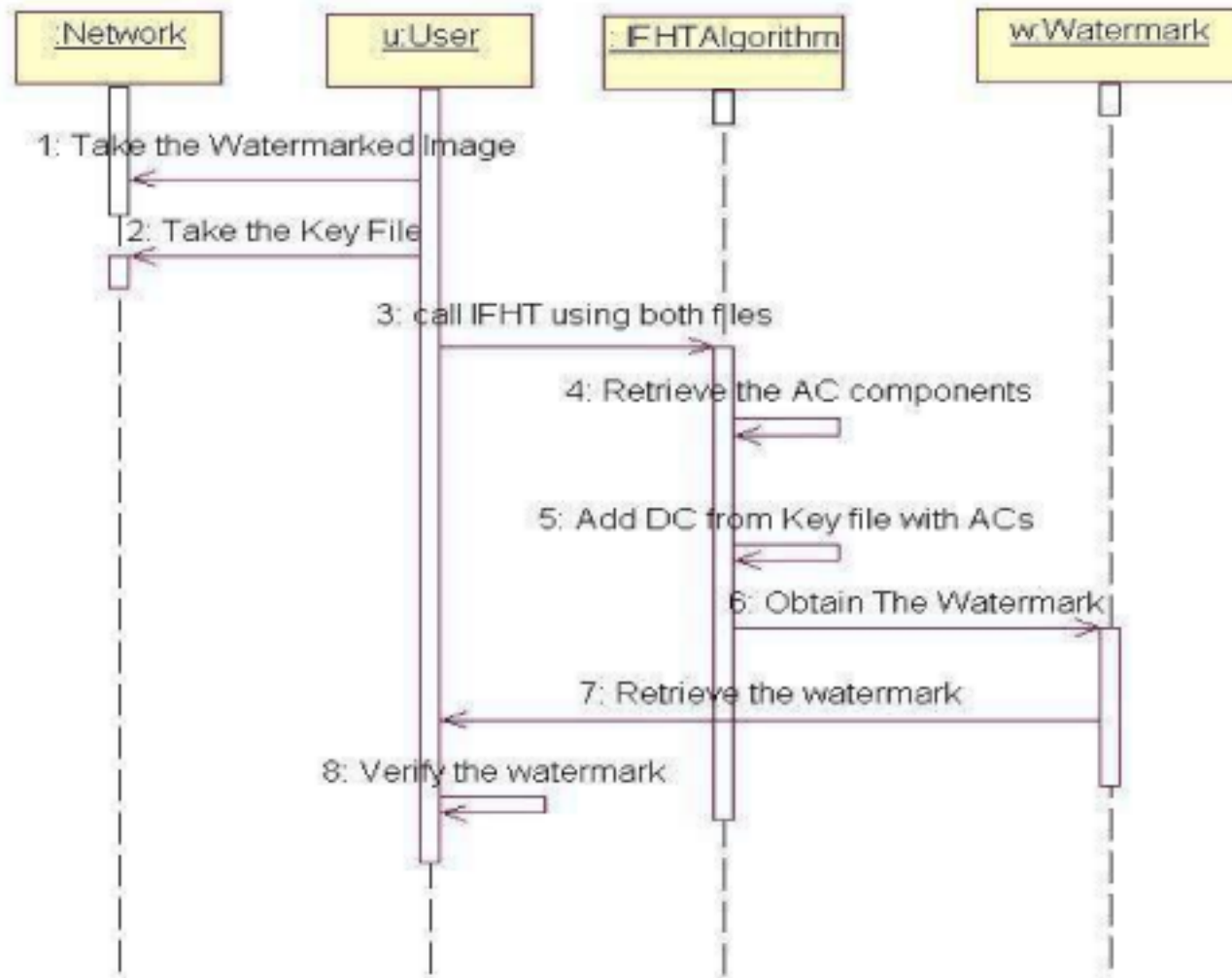
### Advantages of FHT

- Shorter processing time
- Invisibility of the watermark guaranteed
- Increased watermark energy leads to higher robustness

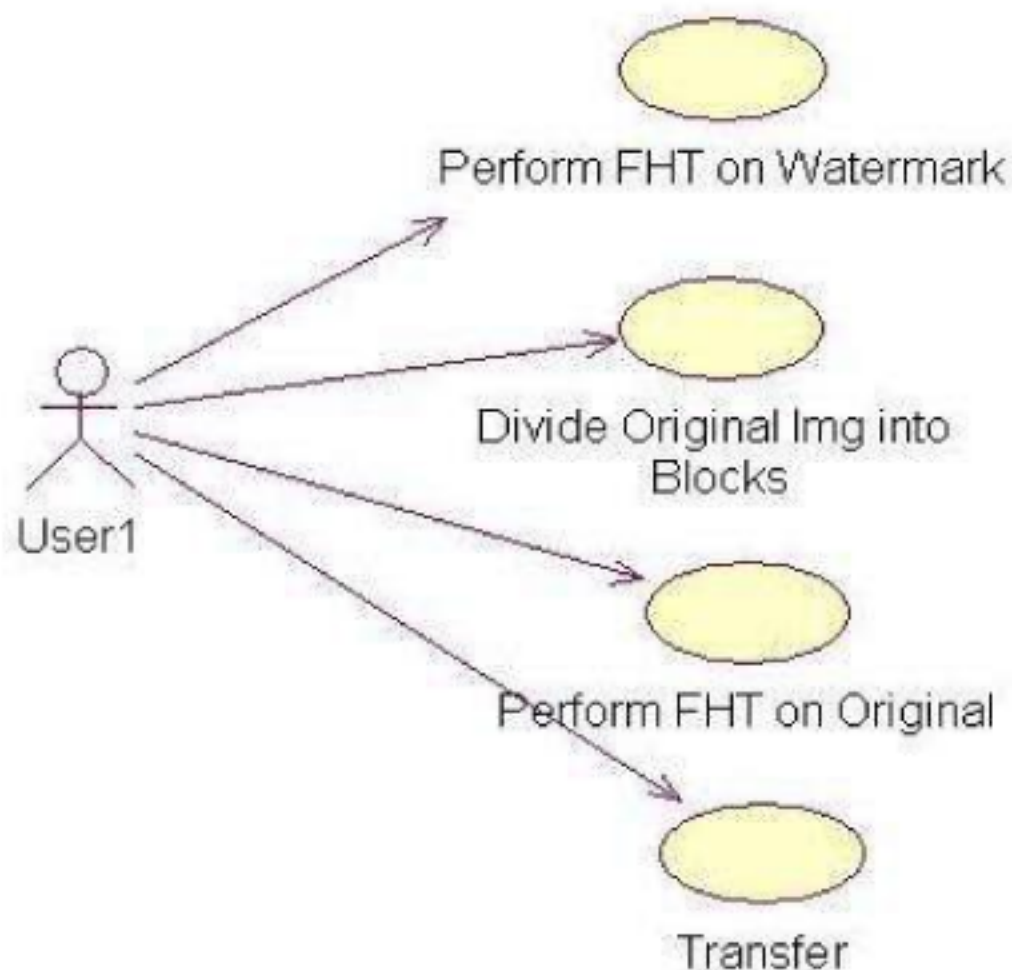
## Sequence diagram1 (Insertion):



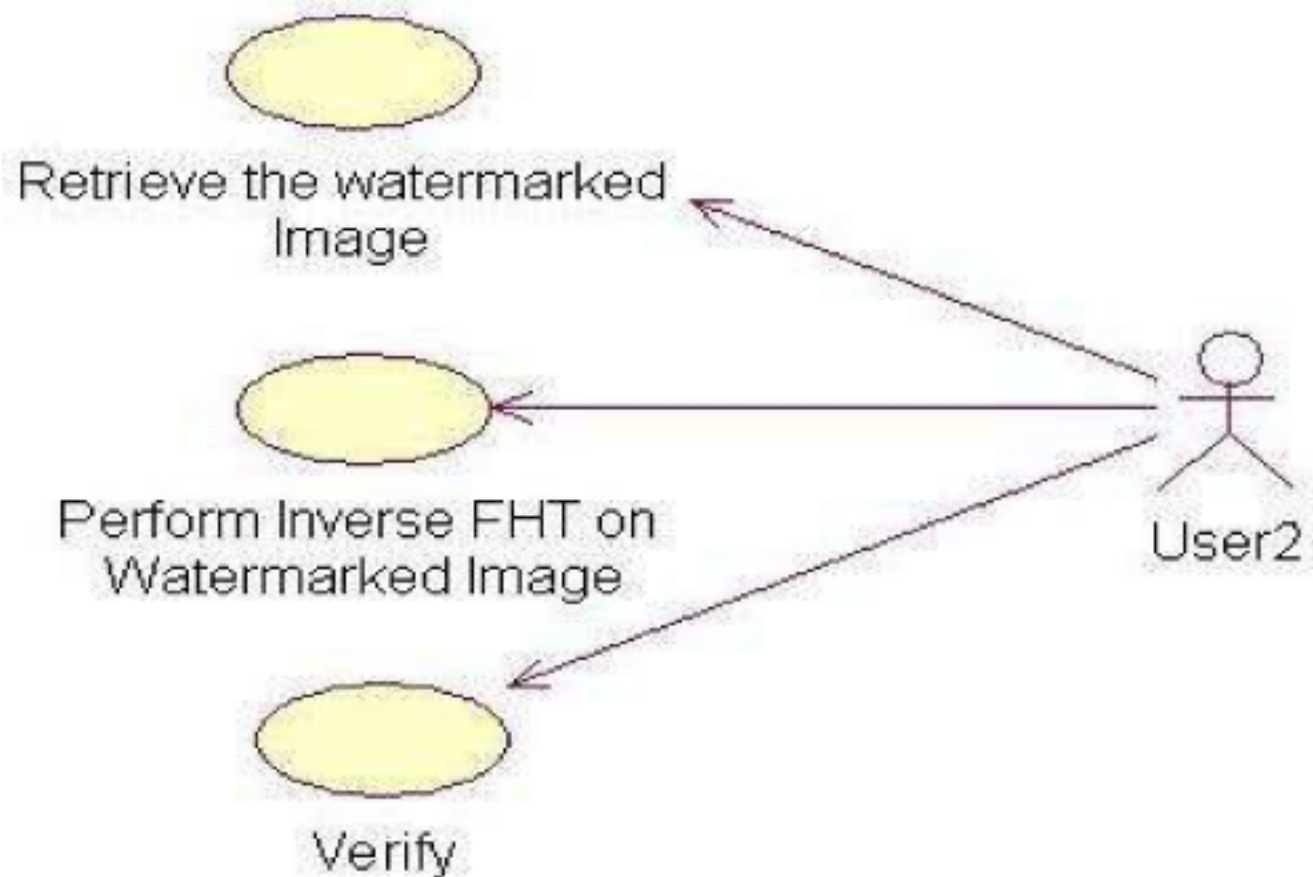
## Sequence diagram2 (Extraction):



## Use case diagrams1 (Insertion):



## Use case diagrams2 (Extraction):



## WATERMARKING IN FHT DOMAIN

### FAST HADAMARD TRANSFORM(FHT)

$$[V] = \underline{H_n} [U] \underline{H_n}$$

N

V ➡ Transformed image

U ➡ Actual image

$H_n$  ➡ N x N Hadamard matrix,  $N=2^n$ ,  $n=1,2,3...$  with element values either +1 or -1

The Hadamard matrix of the order  $n$  is generated in terms of Hadamard matrix of order  $n-1$  using Kronecker product,  $\otimes$ , as

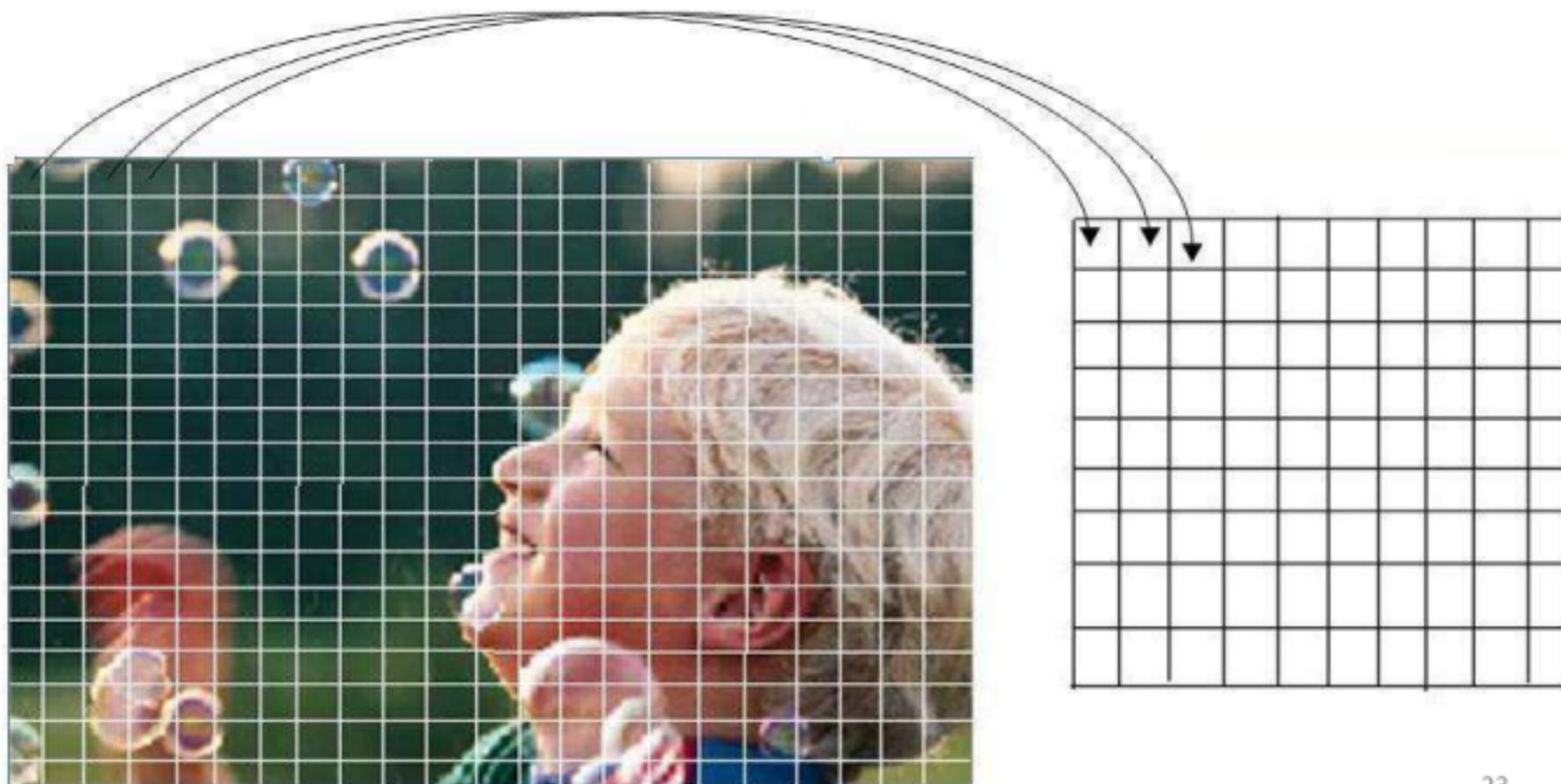
$$H_n = \begin{bmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{bmatrix}$$

Considering  $8 \times 8$  sub-blocks of the whole image, the third order Hadamard transform matrix  $H_3$  becomes:

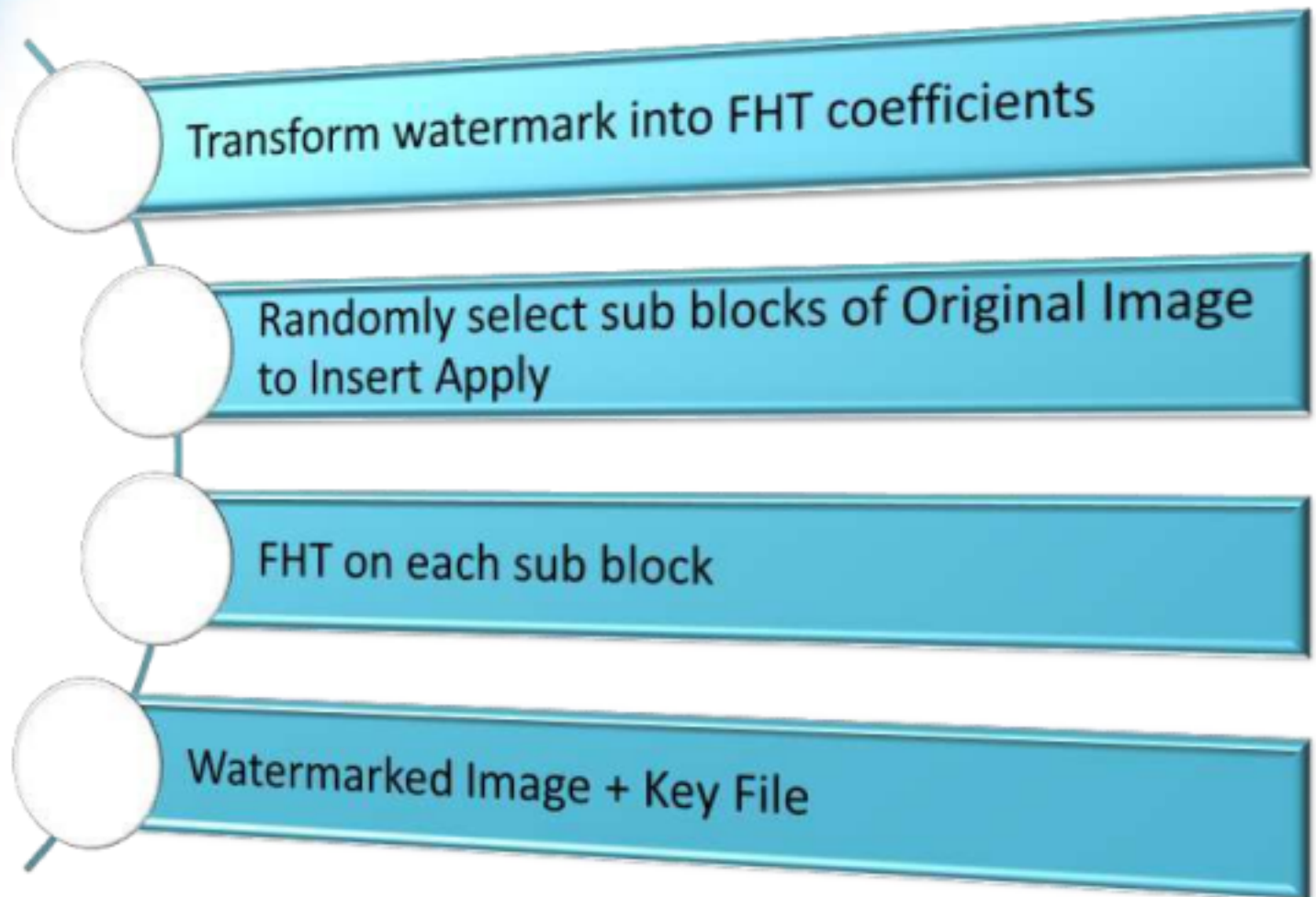
$$H_3 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix}$$



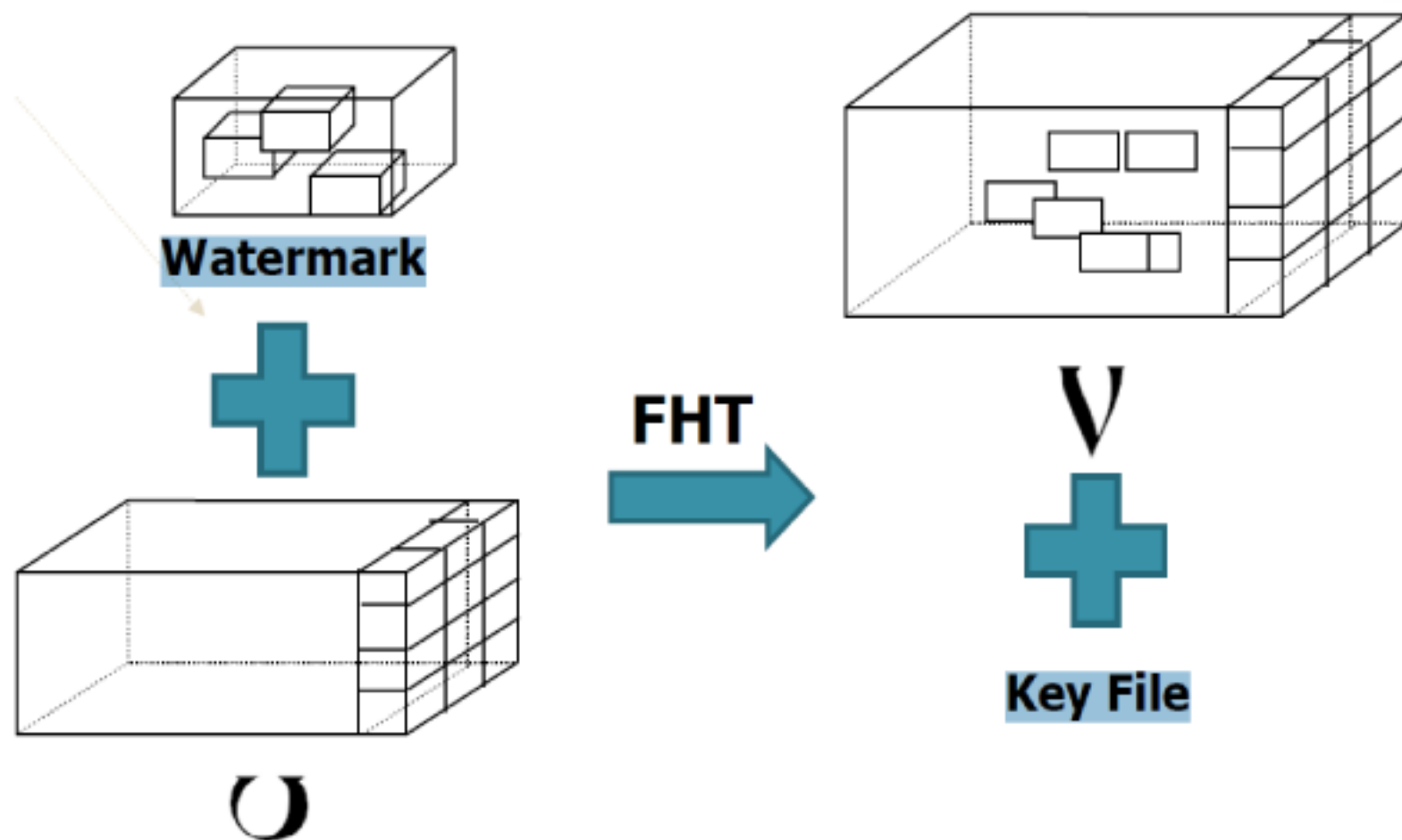
# Original image pixel portions being taken into matrix "U"



# The process of Insertion



## Processing the original image...



### Inverse Fast Hadamard Transformation

$$[U] = H_n^{-1} [V] H_n^* = \frac{H_n [V] H_n}{N}$$

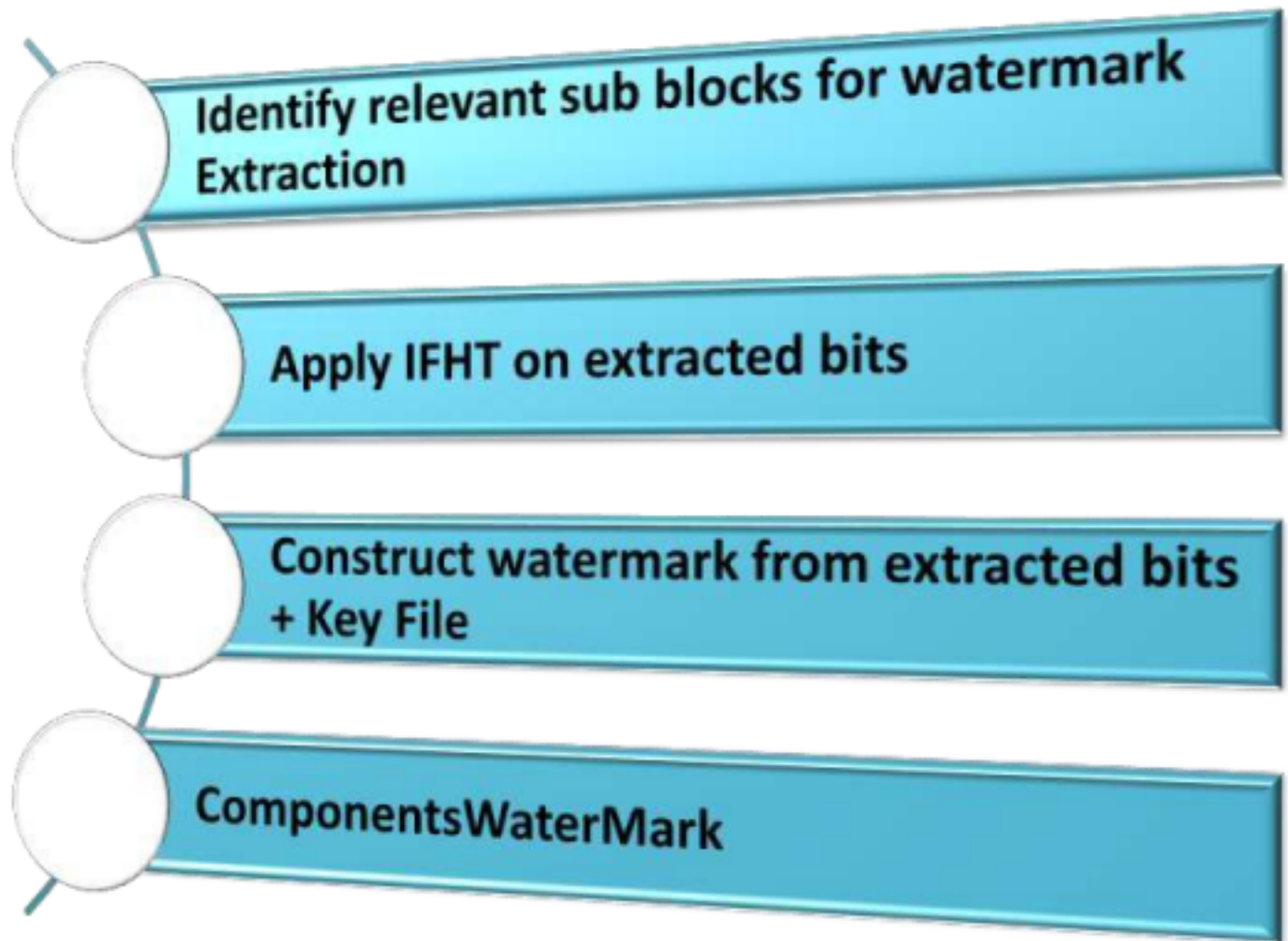
V → Transformed image

U → Actual image

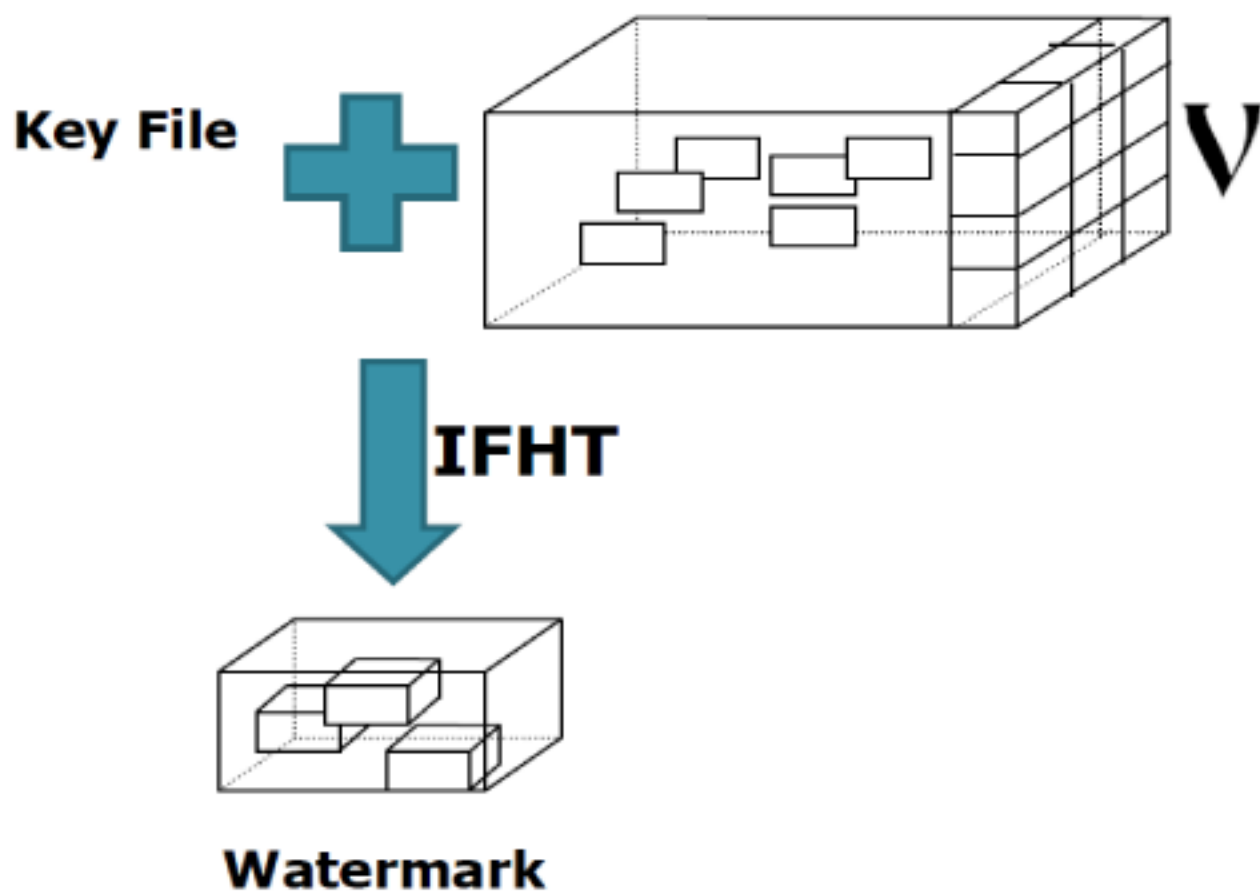
$H_n$  → N x N Hadamard matrix

$H_n^{-1}$  → Inverse Hadamard matrix

# The process of Extraction



## Processing the original image...





# Attacks on the Watermarked image



Original watermarked image



Cropping 50%



Rotation 30°



Changing aspect ratio  
x-1 y-0.8









3×3 median filtering



JPEG compression  
factor 35



## Experiment Results

Image operations	Extracted watermark	Correlation
Sharpening 3×3		0.9573
1 rows 1 column removed		0.9866
Frequency Mode Laplacian removal		0.9580
Scaling 0.75		0.9354
JPEG Compression of factor 30		0.8688
Change aspect ratio x_1.00_y_1.20		0.8199

## Conclusion

- The experimental results show that the proposed method is robust against approximately 70% of attacks.
- For sure when compared with previous, it is found to be more robust against various attacks. It also refers significant advantage in terms of shorter processing time and the ease of hardware implementation than many common transform techniques.

## REFERENCES

- [1] M. Swanson, B. Zhu, A. Tewfik, and L. Boney, "Robust audio watermarking using perceptual masking," *Signal Process., Special Issue on Watermarking*, 1997, pp. 337-355.
- [2] L. Boney, A. Tewfik, and K. Hamdy, "Digital watermarks for audio signals," in *IEEE Proc. Multimedia*, 1996, pp. 473-480.
- [5] Keshav S Rawat, Dheerendra S Tomar, "Digital watermarking schemes for authorization Against copying or piracy of color images" in *IEEE*, Vol. 1 No. 4 295-300
- [6] Anthony T.S.Ho, Jun Shen, Soon Hie Tan "A Robust Digital Image-in-Image Watermarking Algorithm Using the Fast Hadamard Transform" *Proceedings of SPIE Vol. 4793 (2003) © 2003 SPIE · 0277-786X/03/\$15.00*



Thank You

***Any Queries***

