Group-22

Discrete Wavelet Transform based Steganography

-SHUBHANG BHATNAGAR(160020019)
-ANIKET BHATIA(160020001)

-VINEET ASHOK KOTARIYA(16D110009)

-CHINMAY GURJARPADHYE(160020016)

Steganography – Seeing the Unseen

- → Steganography is a technique of hiding/concealing information within another ordinary, non-secret file, message, image or video.
- → Steganographic coding is generally done over media files owing to their large size.
- → Steganography can be used to conceal almost any type of digital content, including text, image, video or audio content inside almost any other type of digital content.
- → The biggest advantage of using Steganographic methods is that any interceptor would not realize that there is some form of encryption and hence the message sent avoids suspicion. To provide an analogy, writing with invisible ink on a letter by post would correspond in principle to Steganography. Some ways of achieving the above would be concealing messages within the lowest bits of noisy images or sound files.
- → In usual practise, steganography is combined with cryptography as an extra "layer" of protection or the cipher is obfuscated using some algorithm to make to make it difficult to decipher.

What is Wavelet Transform?

- → Wavelet Transform is the representation of a function by wavelets, where a wavelet is a scaled and/or translated version of a wave like oscillation which begins with a zero amplitude increases and then decreases back to zero.
- → The wavelet transform is similar to the Fourier transform (or much more to the windowed Fourier transform) with a completely different basis functions. The main difference is this: Fourier transform decomposes the signal into sines and cosines, i.e. the functions localized in Fourier space; in contrary the wavelet transform uses functions that are localized in both the real and Fourier space.
- → This transform is advantageous over possibly Fourier Transform, in the sense that it can incorporate the abrupt changes in the signal.
- → CWT works on every possible scale and transition, while DWT works on a specific subset of them.

What is Wavelet Transform?

Mathematically, CWT of a signal *x(t)* denoted as $X_w(a,b)$, is given as:

$$X_w(a,b) = \frac{1}{|a|^{1/2}} \int_{-\infty}^{\infty} x(t)\overline{\psi}\left(\frac{t-b}{a}\right) dt$$

where a (>0) is the

b ∈ R is the transitional value and $\Psi(t)$ is the 'mother' wavelet whose complex conjugate is present in the above equation.

CWT is the convolution of the input data sequence with the scaled and translated version of the mother wavelet. Inverse CWT is calculated in the following fashion,

$$x(t) = \frac{1}{2\pi\overline{\hat{\psi}}(1)} \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \frac{1}{a^2} X_w(a,b) \exp\left(i\frac{t-b}{a}\right) db\, da$$

Haar Transform

The family of Haar transforms h□(t) are defined on the interval 0 ≤ t ≤ N-1. The shape of h□(t) depends on parameters p & q which are defined using the following equation: $k = 2^p + q - 1$ where 2^p is the largest power of 2 less than k while q-1 is the remainder. For example if N=16, the values of p,q,k are as follows:

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
p	0	0	1	1	2	2	2	2	3	3	3	3	3	3	3	3
q	0	1	1	2	1	2	3	4	1	2	3	4	5	6	7	8

The haar functions are defined as

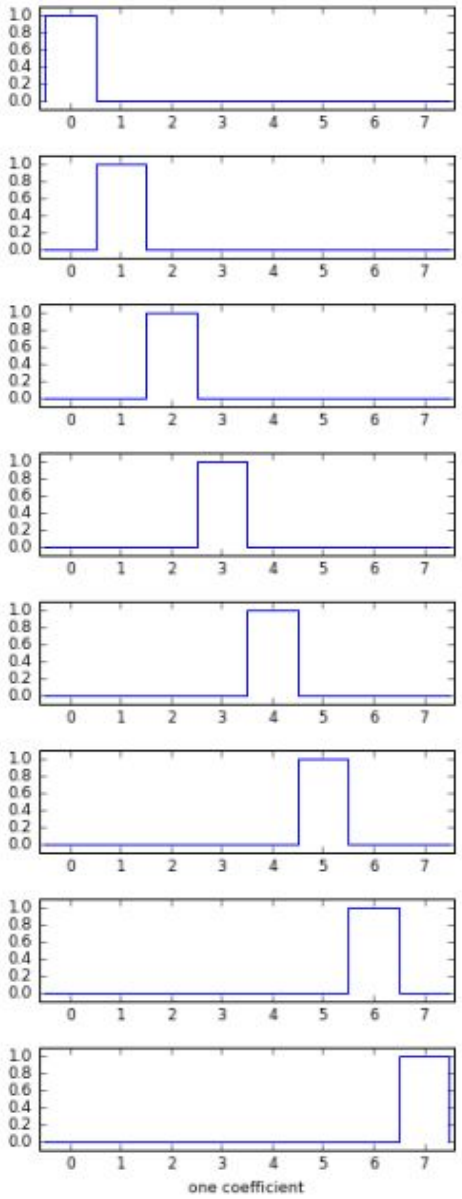
$$h_k(t) = \frac{1}{\sqrt{N}} \begin{cases} 2^{p/2} & (q-1)/2^p \le t < (q-0.5)/2^p \\ -2^{p/2} & (q-0.5)/2^p \le t < q/2^p \\ 0 & \text{otherwise} \end{cases}$$

If k>0

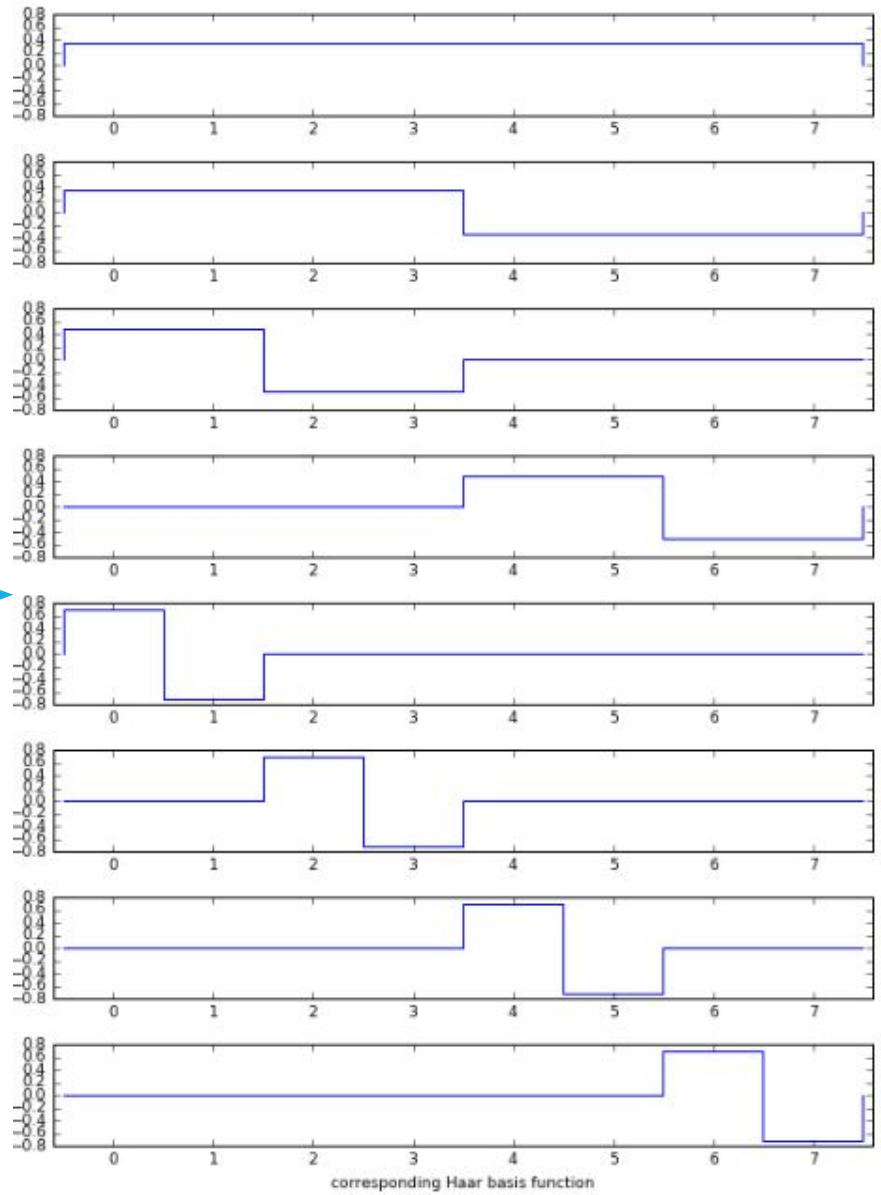
$$h_0(t) = 1/\sqrt{N}$$

if k = 0

Haar Transform



Inverse Haar transform



Haar Matrix

→ The N Haar functions can be sampled at t = m/N, where m=0,1,2…,N-1 to form an NxN matrix for discrete Haar transform. For example if N=2, 4 the matrices will be:

$$\mathbf{H}_2 = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad \mathbf{H}_4 = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ \sqrt{2} & -\sqrt{2} & 0 & 0 \\ 0 & 0 & \sqrt{2} & -\sqrt{2} \end{bmatrix}$$

The Haar transform(1 D)(**X**) of a given vector **x**=(x[0],x[1],.....,x[N-1]) is computed as ***X=Hx.***

The 2D Haar transform if an image 'I' is given by, $\boldsymbol{X = H\,I\,H^T}$.

The Haar transform matrix is real and orthogonal: $H=H^*$, $H^{-1} = H^T$ i.e. $H^TH = I$

To compute the 2D-Haar transform(Haar transform of matrix) first compute the Haar transform of all the rows of the matrix followed by the Haar Transform of the columns of the resulting matrix.

Implementation/ Techniques

We have implemented and tried various techniques of steganography of images, each having its own advantages and disadvantages-

- → Least Significant Bit (LSB) substitution
- → Encoding information in certain coefficients of the wavelet transform of the whole image
- → Encoding information in wavelet transform coefficients of each 4*4 patch of the image, after dividing it into non overlapping patches.
- → Lossy transmission (taking half the number of bits each of the carrier and hidden image)

Least Significant Bit (LSB) Substitution

It involves direct substitution of the least significant bits of each pixels R,G,B values by the bits of the sequence we want to encode.

ADVANTAGES:

-> It is a very lightweight technique and can be easily and quickly applied with even minimal computing power and good results upto certain bit lengths.

DISADVANTAGES:

-> It is easy to detect in most cases if such a technique is being used

-> It also has a limited capacity to store data if we want to restrict perceptual errors

Haar Transform of the complete image

In this technique, we first take the wavelet transform of the image. Then, in the coefficients with lowest values, we change the least significant bits. This means that we only corrupted the wavelet components which have the least effect on the image.

ADVANTAGES:

-> The use of wavelets to encode enables us to store much more data without causing significant visual degradation to the image.

-> They are also much more robust to detection as compared to LSB substitution

DISADVANTAGES:

-> Calculating the wavelet transform and its inverse is more computationally intensive then using direct LSB substitution

Patch-based Haar transform

In this method we divide the image into non overlapping 4*4 patches (or any other suitable size) and then take the wavelet transform of each of these patches. In these transforms, we encode our data in the wavelets with smallest coefficients, thus preventing major changes in the patch and the image.

ADVANTAGES:

-> This technique stores the maximum amount of data in the ones we used, as there are a larger number of small coefficients available

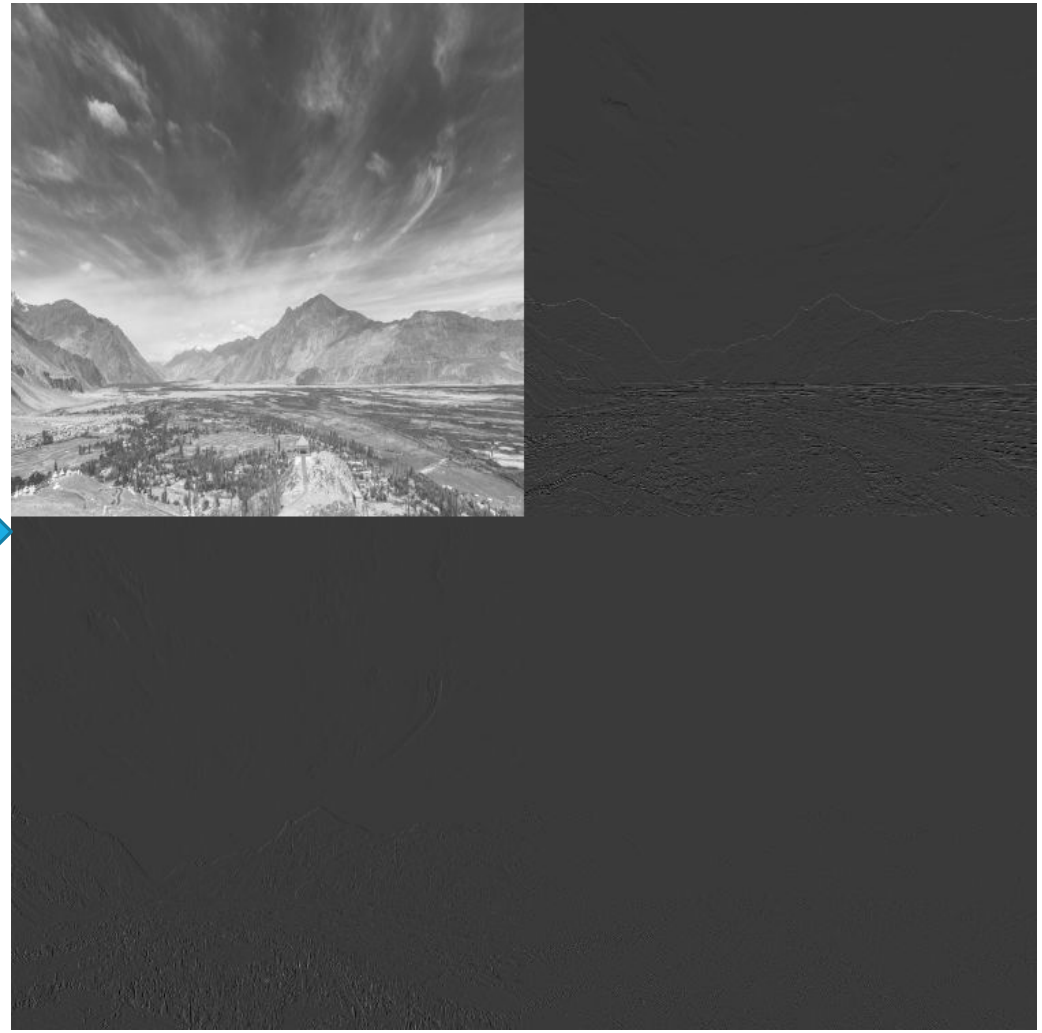
-> It is even harder t detect especially if we vary the patch size or combine it with cryptography

DISADVANTAGES:

-> This is also the most computationally expensive among the 3

2D-Haar transform (Example)

Input

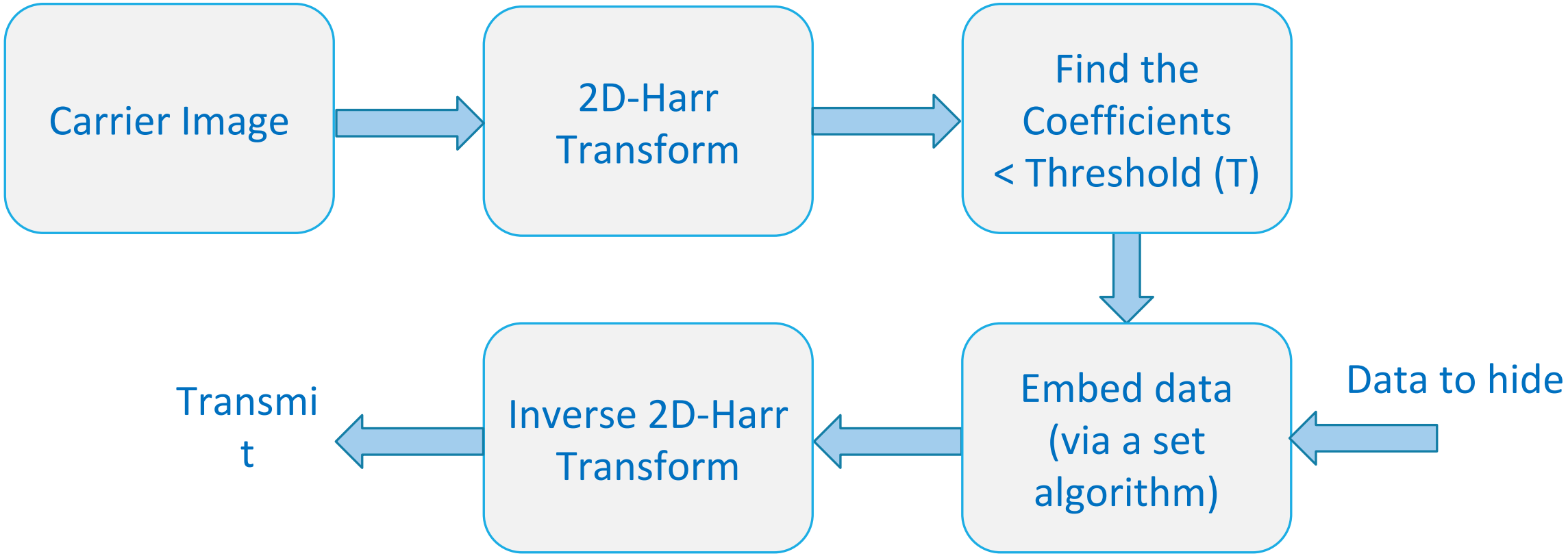


2D-Haar Transform

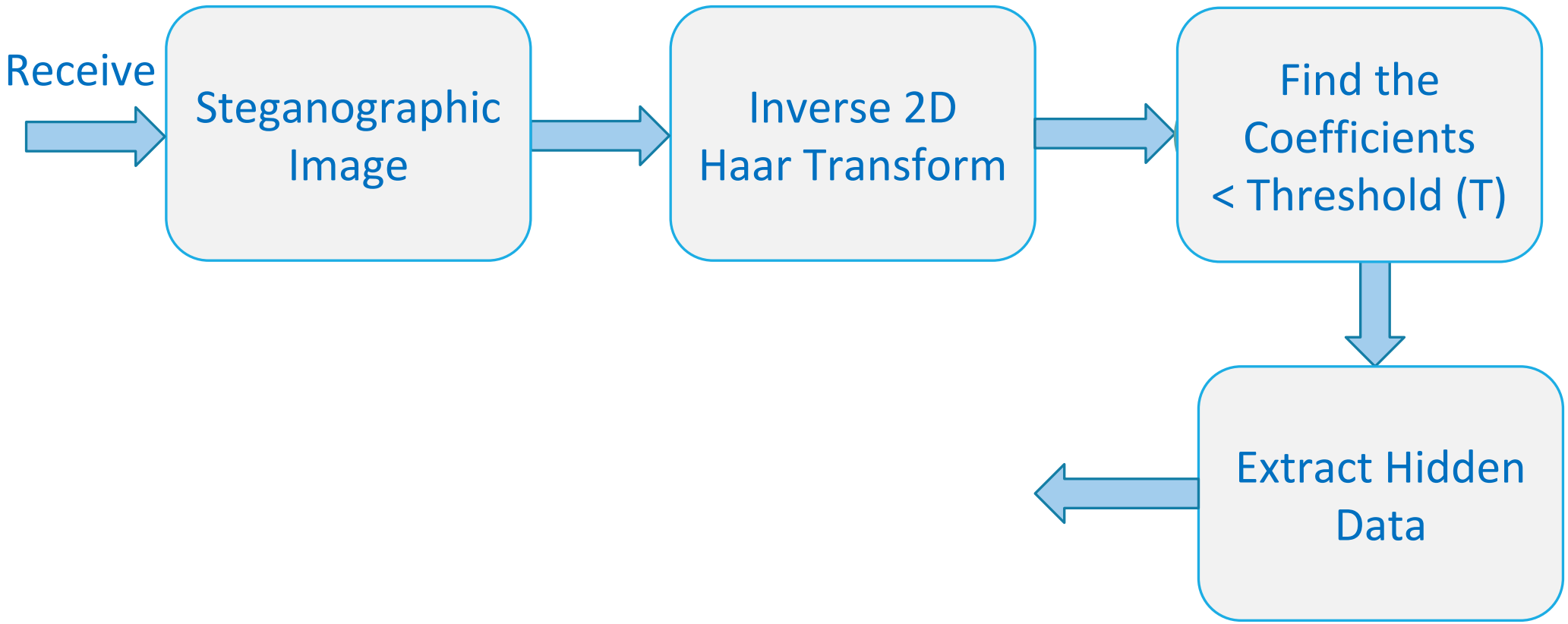
Application in ‘Make in India’

- In the light of current terrorist events security has become essential and cannot be underlooked under any circumstances. Being self sufficient is thus very important and hence we need to develop in-house applications to benefit the country from within. Steganography is very useful for military purposes (spying) where secret communication is of utmost importance and complex infrastructure like pseudorandom generators and computers are unavailable, hence implementing modern cryptographic techniques is not possible. Messages can be sent through ‘stego’ images without attracting attention by interceptors.
- Steganography can be used on modern IoT(Internet of Things) devices to provide data security and privacy to the data they transmit. Such embedded systems can use a combination of simple cryptography and steganography to communicate securely.
- Another important use of steganography for make in India is for the puropose of digital watermarking. The world is quickly changing to be more and more digital. Also, digital data can be easily copied and misused. Watermarking using steganography is very to prevent such cases of misuse, copyright violations and piracy. Invisible watermarks placed using steganography can be used to detect pirates, detect and authenticate files etc.
- Medical data of patients such as medical records along with personal identification information is very sensitive and confidential. Steganography can be used to hide HIV reports, fetus information, etc.

Block diagram (Encoding)



Block diagram (Decoding)



Message to be transmitted

→ We transmitted text messages over three channels of a coloured image

→ The R,G,B components of the image being the carrier for each of the channels.

→ TRANSMITTED MESSAGE (Hidden Message):

msg_r='Extraordinary things are always hiding in places people never think to look'

msg_g='There is no greater agony than bearing an untold story inside you’

msg_b='Inside everybody is hiding something‘

Input (Carrier) Image

Image after Steganography

Technique-1: LSB Substitution

Message After Decoding:

→ Decoded Message:

msg_r='Extraordinary things are always hiding in places people never think to look'

msg_g='There is no greater agony than bearing an untold story inside you'

msg_b='Inside everybody is hiding something‘

→ So we successfully achieved concealment, transmission and decoding of the message text in each of the three lossless techniques.

→ Note: For text there is no other option but to do lossless transmission (unlike in images)

Message Transmitted

Message

Decoded message

Technique: LSB Substitution with down-sampling

Technique-2: Haar transform

Input (Carrier) Image

Image with hidden message

Technique-4: Lossy

Carrier image

Image after Steganography

(Notice the artifacts)

Technique-4: Lossy

Hidden image: Transmitted

Decoded image

(Notice the artifacts)

Challenges Faced

- → Steganography faces and has to overcome three main challenges, the Invisibility "Security of Hidden Communication ", Robustness and the size of embedded data. There is no steganographic technique, capable of resolving all the three challenges at a high level of accuracy. It is not possible to attain high robustness to signal modifications and high insertion capacity at the same time.
- → Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) are two of the most common steganographic domain transformation methods, the complexity is $O(N^2 log(N))$ v/s $O(N^2)$.

References

- Johnson, Neil F., Sushil Jajodia. Exploring Steganography: Seeing the Unseen. IEEE Computer, 26-34, 1998.
- Morimoto, Norishige, Walter Bender, Daniel Gruhl. Techniques for data hiding MIT, Media Laboratory.
- Dr.Adwan,Mr.Nizar, Shehab, Dr.Muath, Mariam Yasin. An Enhanced Steganographic Model Based on DWT Combined with Encryption and Error Correction Techniques. IJACSA, Vol. 6, No. 12, 2015
- Adnan Gutub ; Ayed Al-Qahtani ; Abdulaziz Tabakh. Triple-A: Secure RGB image steganography based on randomization 2009 IEEE/ACS International Conference on Computer Systems and Applications.
- https://www.semanticscholar.org/paper/A-Discrete-Wavelet-Transform-3A-A-Steganographic-for-Waku re-Aurangabad/
- http://www.cs.cornell.edu/topiwala/wavelets/report.html#note1
- http://wikipedia.com/Discrete_wavelet_transform/
- https://unix4lyfe.org/haar/
- http://gwyddion.net/documentation/user-guide-en/wavelet-transform.html
- http://fourier.eng.hmc.edu/e161/lectures/Haar/index.html