

3rd SPLab Workshop 2013

October 30 to November 1, 2013

BRNO, Czech Republic, European Union

Lecture on

Ownership of Digital Signals using Biometric features

M.K. Dutta

Dept. of Electronics & Communication Engineering.

Amity School of Engineering and Technology

Amity University, Sector – 125, Noida (U.P.) – 201303 , India



AMITY
UNIVERSITY

The Problem

Illegal reproduction and unauthorized distribution of digital media has become a high alarming problem in protecting the copyright of digital media, due to faster data transmission rates on the Internet, which has allowed the often-illegal proliferation of digital audio files.



Security of Digital Data:

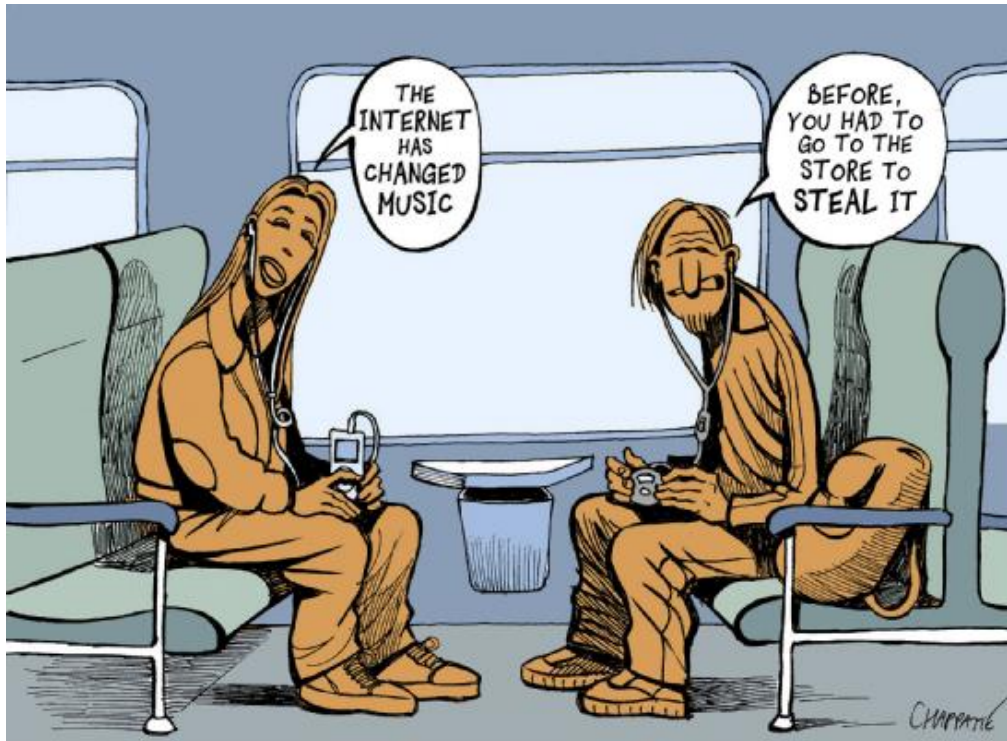
Encryption of digital multimedia prevents access to the multimedia content without a proper decryption key. Once the multimedia has been decrypted, it can be repeatedly copied and distributed without any obstacles. Hence, encryption techniques are not sufficient for digital right management control.

Security questions are becoming urgent for digital media !

- Replication of digital works is very easy.
- The copy is identical as original. (perfect copy)
- The ease of transmission and multiple uses is worrying.
- Manipulations are really easy for a pirate and put many copyright protection methods at risk.
- Any mischievous user can modify an digital media at will.



Digital Right Management Control is a challenging issue !



Security and Ownership of Digital Data is a huge matter of concern and there is a need to find suitable methods method of protecting copyright issues and ownership of digital content.

How to address this Security issue of Digital Data !



Confidentiality

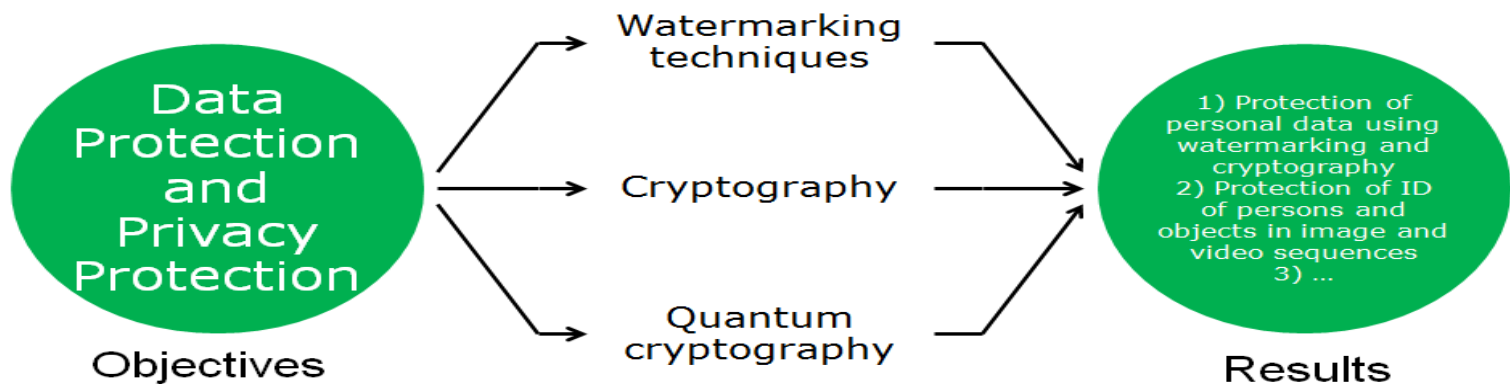
Steganography / Watermarking

(hide existence of the secret message,
but do not use encryption)

Encryption

(encrypt the message,
but do not hide the message)

- Ideally nobody can see both parties are secretly communicating.
 - Innocent.
- Anybody can see both parties are communicating in secret.
 - Suspicious.



History



440 B.C.

Histiaeus shaved the head of his most trusted slave and tattooed it with a message which disappeared after the hair had re-grown. To instigate a revolt against Persians.

1st and 2nd World Wars

German spies used invisible ink to print very small dots on letters.

Microdots – Blocks of text or images scaled down to the size of a regular dot.

Current

Special inks are used to write a hidden messages on bank notes.

Industry demands for digital watermarking and fingerprinting of digital image, audio and video.



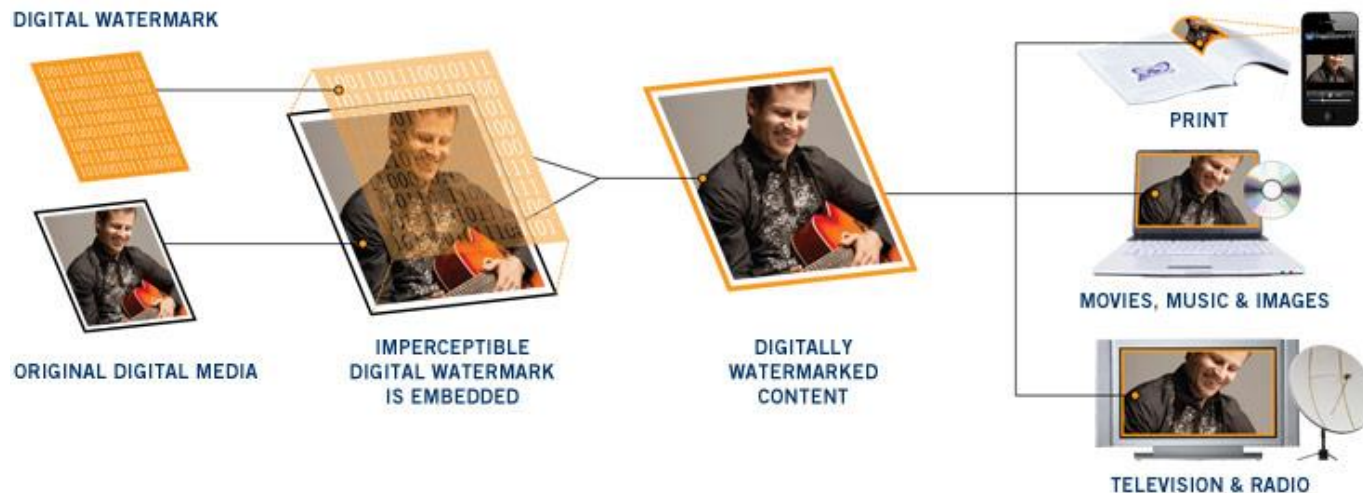
What is Digital Watermarking

“Digital Watermarking “means embedding information into digital material in such a way that it is imperceptible to a human observer but easily detected by computer algorithm.

A digital watermark is a transparent, invisible information pattern that is inserted into a suitable component of data source by using a specific computer algorithm. Digital watermarks are signal added to digital data that can be detected or extracted later to make an assertion about the data.

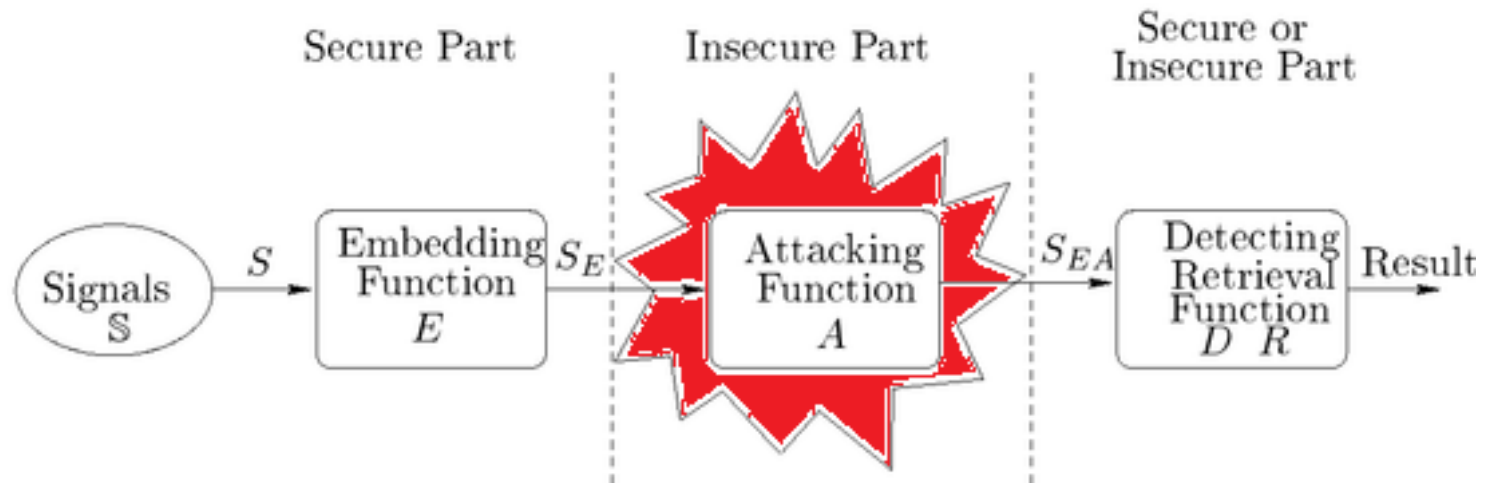
Digital watermarking is a possible solution for copyright Protection of Digital Data.

It can be considered as a method to enforce the intellectual property rights, to protect digital media from tampering and digital right management control

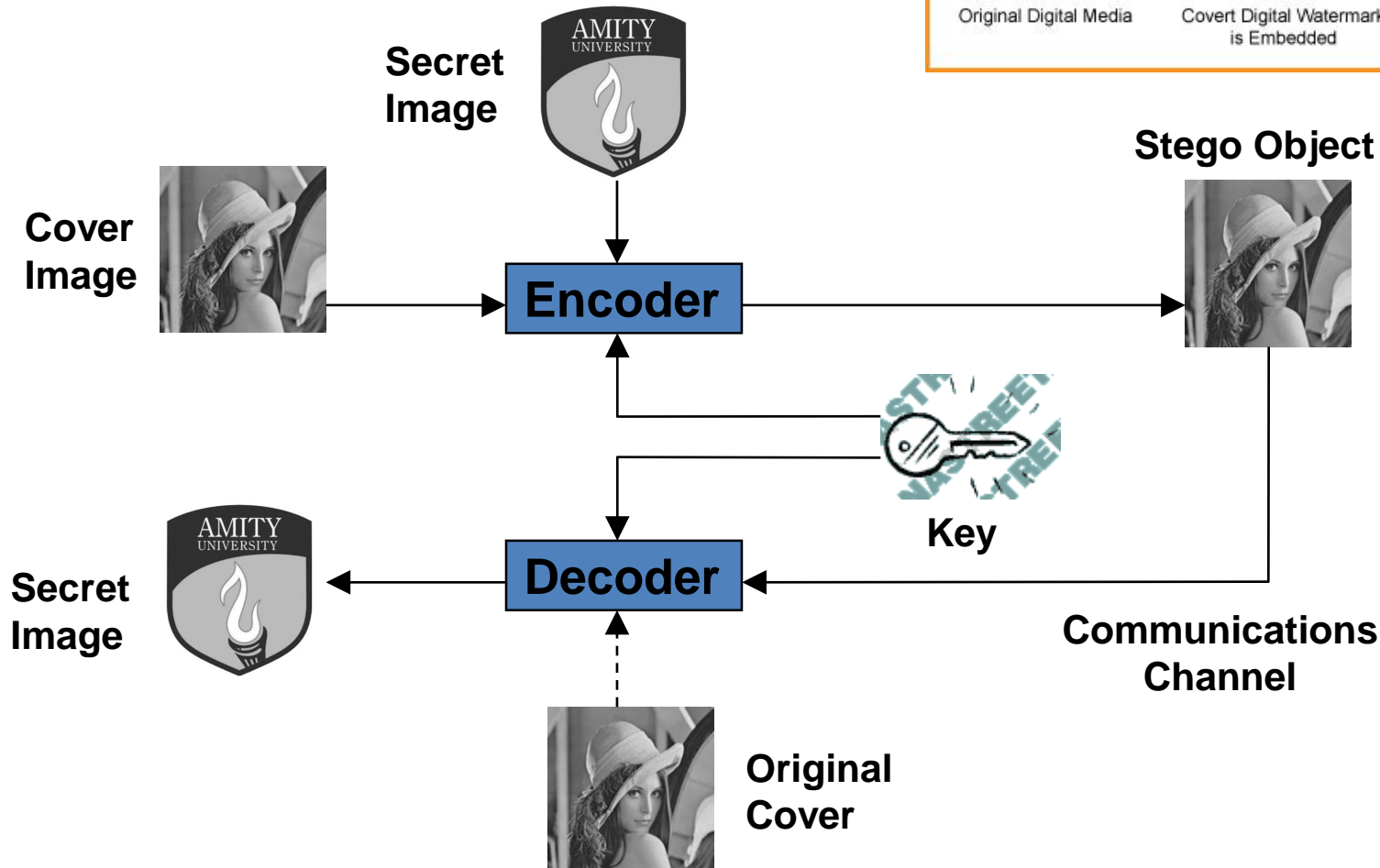
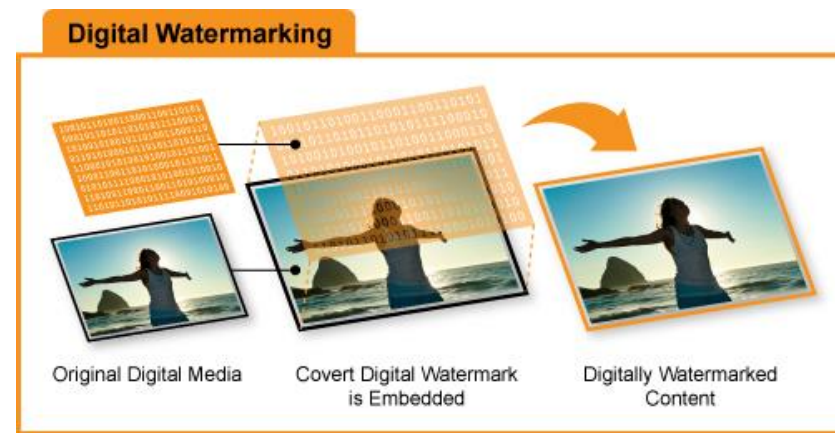


The important Question :

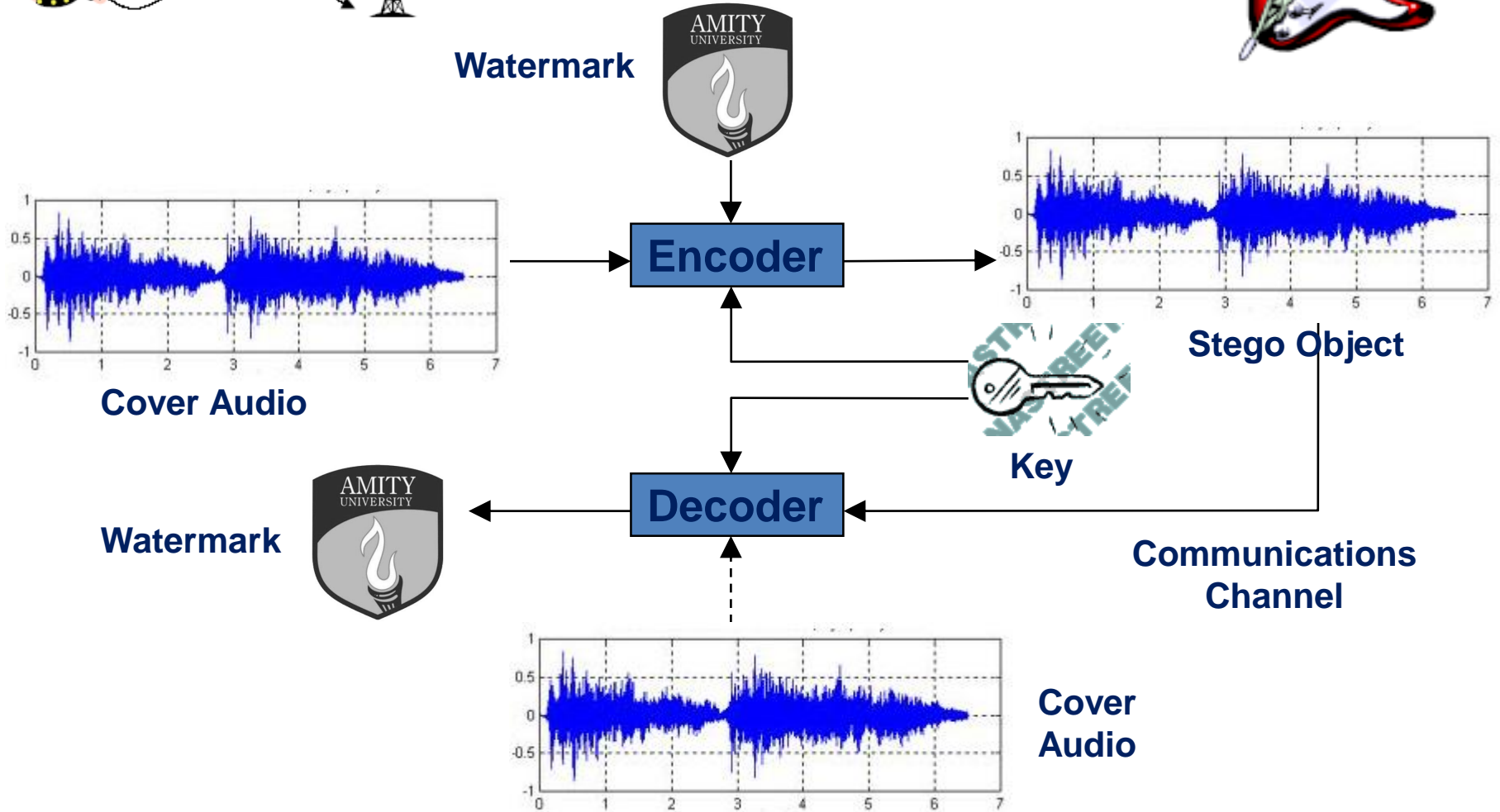
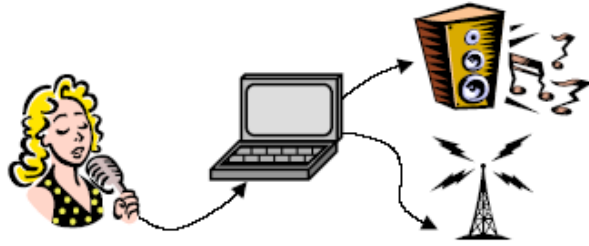
- How can information be hidden in digital data???
- By exploiting “perceptual properties.”
 - Human perception is imperfect
 - Make modification to the original data without changing its perceptual quality, exploit masking principle.
 - Modifications can be detected via signal processing.



Basic Principle in Image Watermarking



Basic Principle in Audio Watermarking



Digital Watermarking: Trade-off

Imperceptibility



Robustness



Capacity

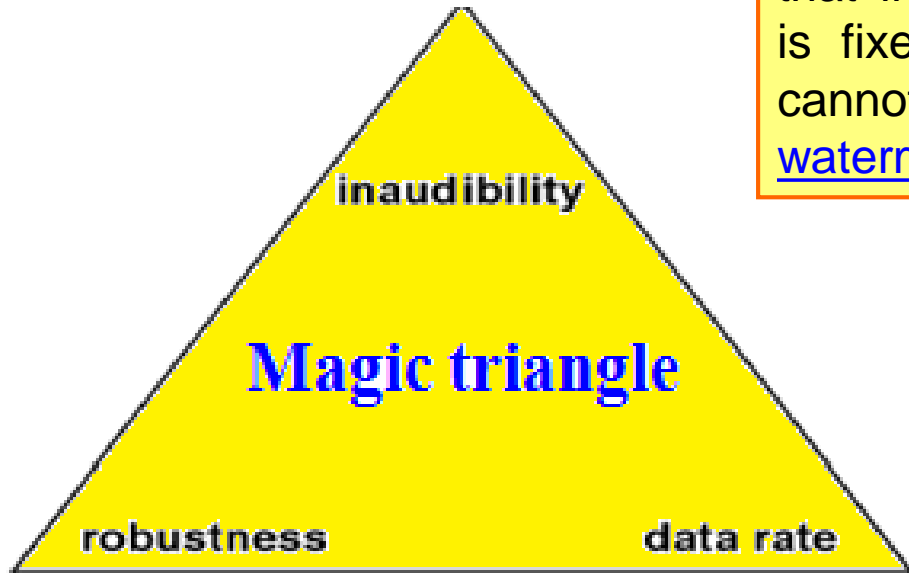


Imperceptibility: One of the main requirements for watermarking is the perceptual transparency. The data embedding process should not introduce any perceptible change into the host data.

Robustness: Robustness refers to the ability of the watermark to survive signal processing attacks, it means that even if the attacker is aware about the presence of the watermark still he will not be in a position to remove the watermark.

Capacity : Capacity refers to the watermark payload in the host file. This is a measure of the amount of watermark data which can be inserted keeping the perceptual parameters unchanged.

The Challenge: Optimization of the Trade off requirements



Magic triangle: Three trade-off requirements of watermarking.

The main challenge in digital watermarking is that if the perceptual transparency parameter is fixed, the design of a watermark system cannot obtain high robustness and a high watermark data rate at the same time.

Design Issues.

1. Perceptual transparency.
2. High Data rate.
3. Robustness to signal processing.
4. No Distortion of Original Signal.
5. Efficient Computation.
6. Undetectable.
7. High security.

Research Trends and Focus of Digital Watermarking.

1. Watermarking has been tried and experimented in different Domains like wavelet domain, Fourier domain, DCT domain, SVD Domain etc.
2. A lot of efforts has been done for the Optimization of the conflicting design parameters of perceptual transparency, robustness to attacks and payload of the watermark.
3. Some work has also been reported in which the watermarking algorithm has been designed and parameters optimized for a specific application

Types of Audio Watermarking

Temporal watermarking : Temporal watermarking hides watermarks directly into digital audio signals in the time domain.

Spectral water-marking: The spectral audio watermarking applies certain frequency transform, such as FFT, DCT, and DWT, etc, to the data block of the audio signal, and hides the watermark information Into the transformed data block.

Types of Image Watermarking

Spatial watermarking (spatial domain)

Spectral watermarking (frequency-domain)

- Many types due to variety of transforms
- Adjustments made in frequency domain
- More robust

One Major Limitation in the Existing Methods of Watermarking

In various methods, the watermark is generated from random numbers or chaotic encryptions. Sometime a logo or a symbol is used as a seed to generate the watermark. However, if there is a piracy dispute on the ownership of the watermark, the symbol or the logo may not be considered as an adequate proof of ownership.

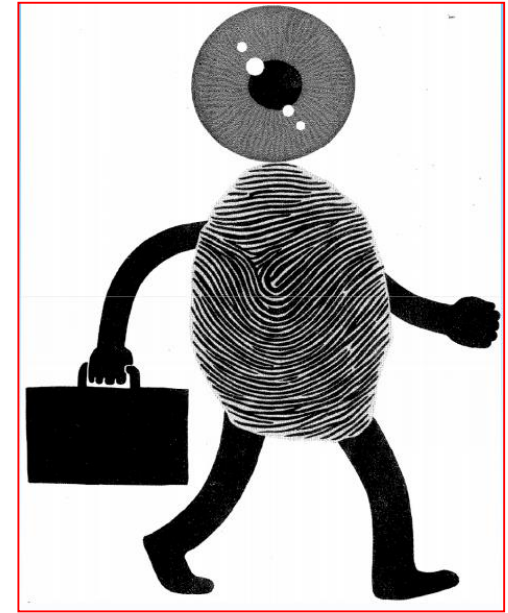


In addition to that a malicious attacker may embed a watermark of a rival counterpart in a digital signal in pirated media files to mislead.

Possible Solution of this Limitation

To overcome this limitation, there is a need of mapping a digital watermark to an entity that can be physically or logically owned.

This entity should be such that it cannot be generated or copied and has to be unique for all reasons. For example, generally binary images are used as a watermark which cannot be an ideal entity for proof of ownership because it is easy to replicate.

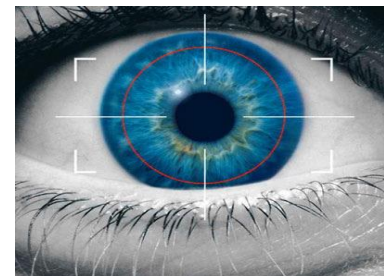


Keeping this limitation in mind, one can think to incorporate **biometric data** as the seed of the watermark. Biometric features, termed as bio-key, can be used for the generation of the watermark key.

The proposed Solution

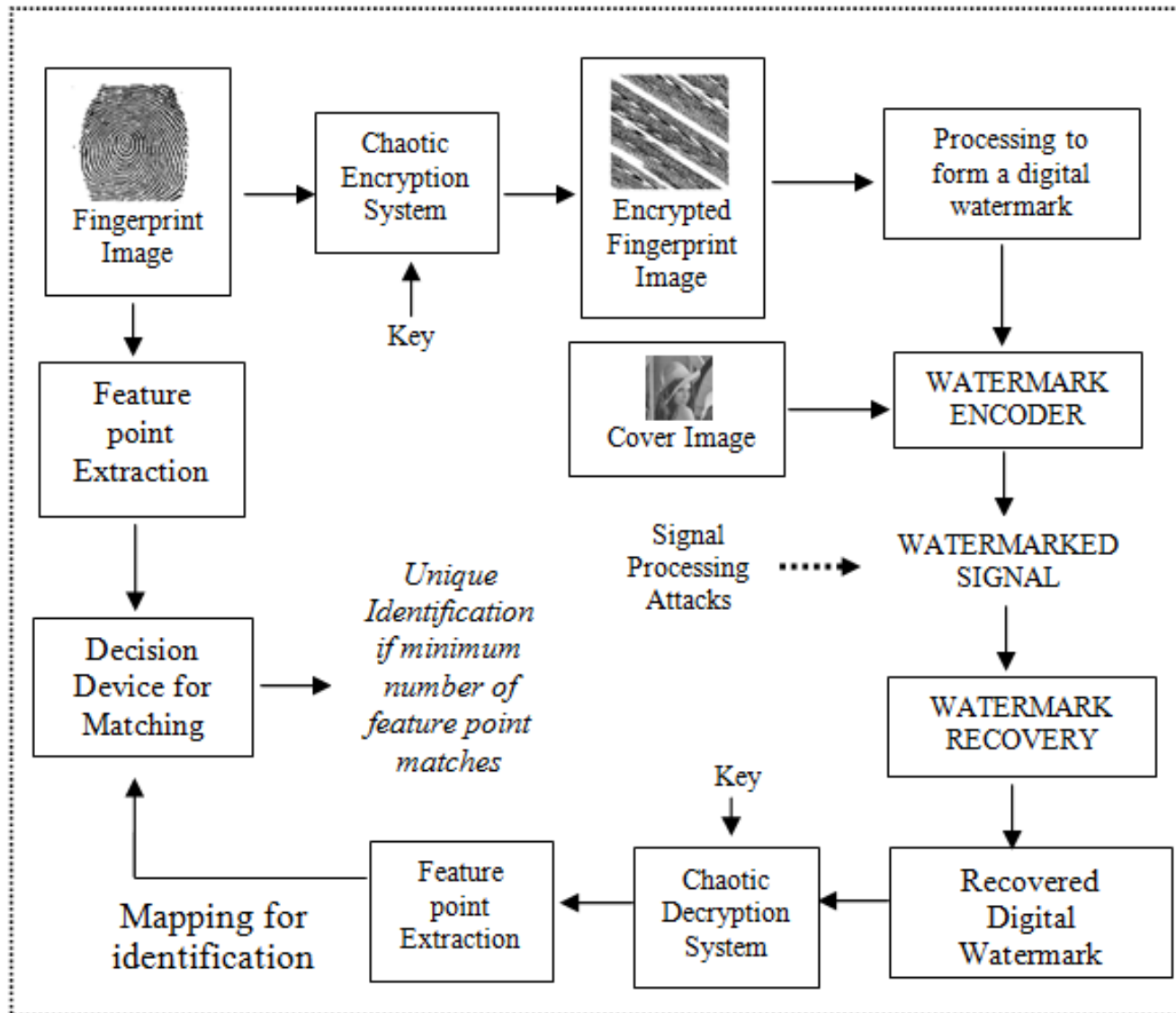
The Bio-Key

To overcome these limitations it is proposed to incorporate **biometric data** as the seed of the watermark. Biometric features, termed as bio-key, can be used for the generation of the watermark key.



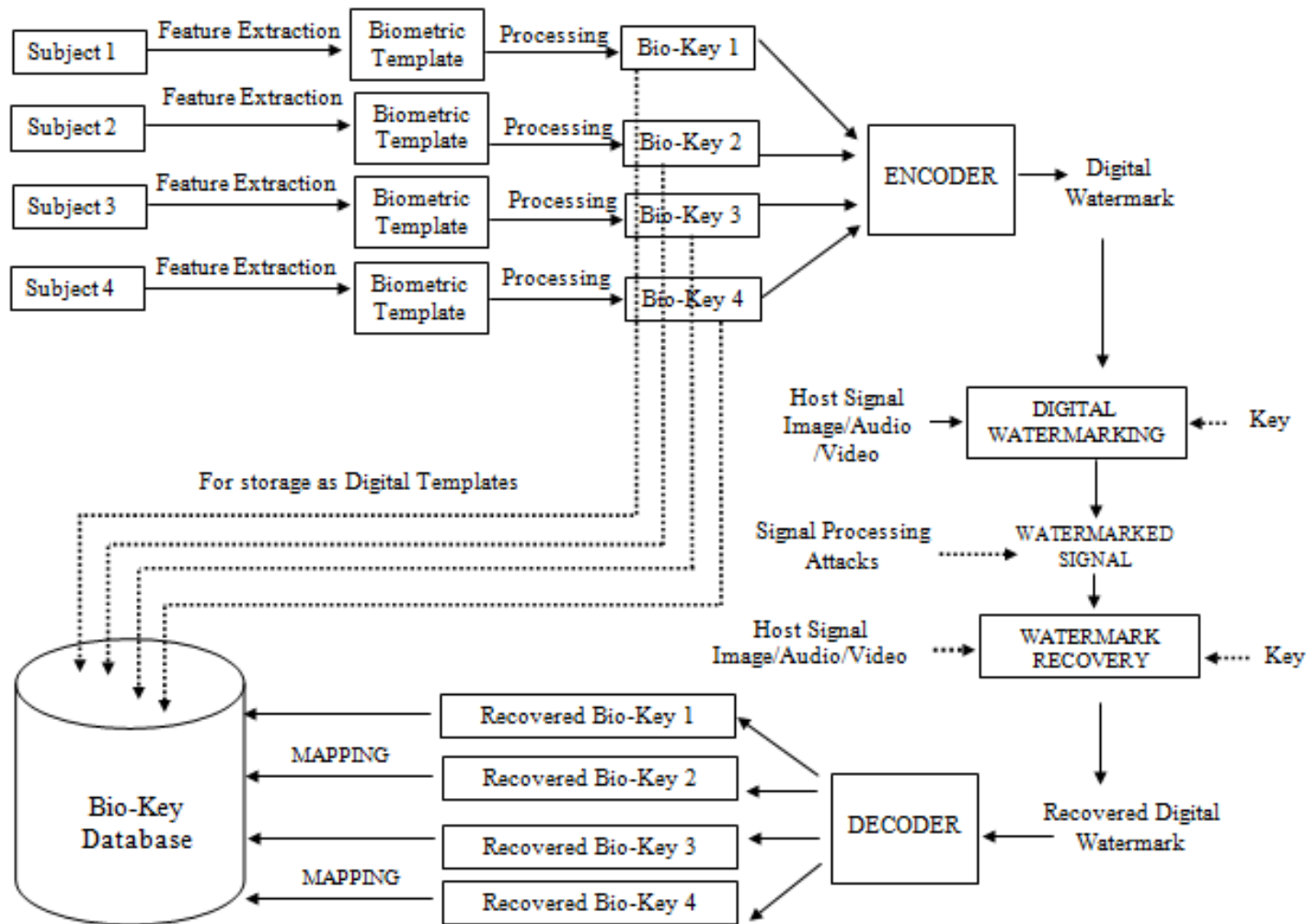
Since the biometric features are unique for any individual and can easily be mapped in a database biometric features can be used as a key in a watermarking system. So the authentication and ownership issues can automatically be addressed.

The Basic Model of use of Bio-Key



If biometric features are used as a key in a watermarking system then the authentication and ownership issues can automatically be addressed, as the biometric features are unique for any individual and can be mapped in a database. Hence, such biometric based key will have a stamp of ownership and may provide a potential solution to the limitation of ownership issue of digital watermark.

The Model of Bio-Key For Joint Ownership

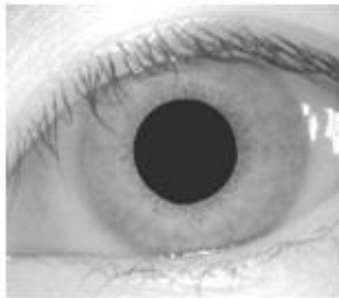


Method to establish joint ownership of digital images by embedding imperceptible digital pattern in the image. This digital pattern is generated from biometric features of more than one subject in a strategic matter so that the identification of individual subject can be done and the multiple ownership of the digital images can be established.

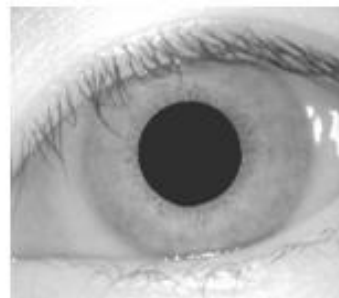
Feature extraction from iris image and digital watermark generation.

1. The first stage of iris image processing is to isolate the actual iris region from the whole digital eye image [9].
2. Circular Hough transform is used for detecting the iris and pupil boundaries. This involves first employing canny edge detection to generate an edge map. Gradients were biased in the vertical direction for the outer iris/sclera boundary, as suggested by Wildes et al. [10].
3. Vertical and horizontal gradients were weighted equally for the inner iris/pupil boundary. In order to make the circle detection process more efficient and accurate, the Hough transform for the iris/sclera boundary was performed first, then the Hough transform for the iris/pupil boundary was performed within the iris region, instead of the whole eye region, since the pupil is always within the iris region. After this process was complete, six parameters are stored, the radius, and x and y centre coordinates for both circles.
4. Eyelids are isolated by first fitting a line to the upper and lower eyelid using the linear Hough transform. A second horizontal line is then drawn, which intersects with the first line at the iris edge that is closest to the pupil. For isolating eyelashes a thresholding technique is used, since analysis reveals that eyelashes are quite dark when compared with the rest of the eye image.

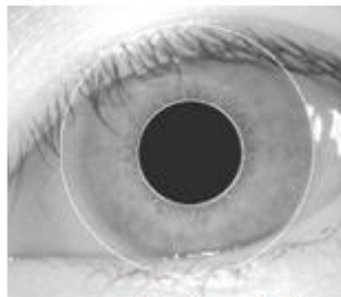




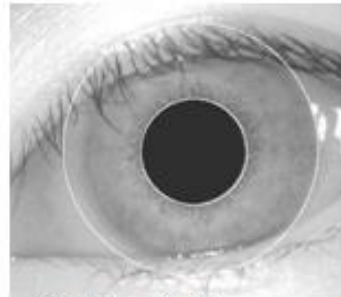
Iris Sample 1



Iris Sample 2

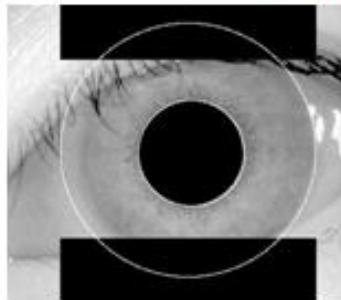


(For Sample 1)

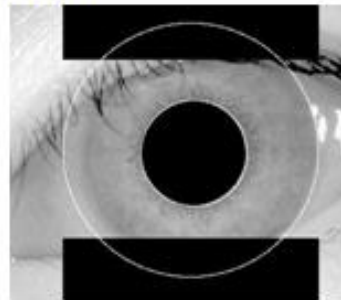


(For Sample 2)

Hough Transformation



(For Sample 1)



(For Sample 2)

Noise Removal from eye-lashes.

A method based on Daugman's rubber sheet model was employed for normalisation of iris regions. The centre of the pupil was considered as the reference point, and radial vectors pass through the iris region. A number of data points are selected along each radial line and this is defined as the **radial resolution**. The number of radial lines going around the iris region is defined as the **angular resolution**.

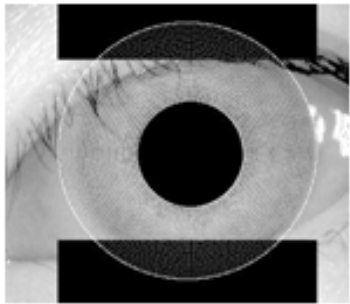
Iris Samples, Hough Transformation and the noise removal from the eye-lashes for 2 samples of iris image.

A constant number of points are chosen along each radial line, so that a constant number of radial data points are taken, irrespective of how narrow or wide the radius is at a particular angle.

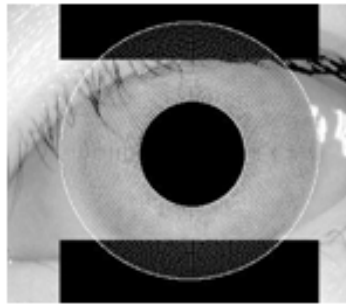
Feature encoding is implemented by convolving the normalised iris pattern with 1D Log-Gabor wavelets. The 2D normalised pattern is broken up into a number of 1D signal, and then these 1D signals are convolved with 1D Gabor wavelets.

The output of filtering is then phase quantised to four levels using the Daugman method, with each filter **producing two bits of data for each phasor**. The output of phase quantisation is chosen to be a gray code, so that when going from one quadrant to another, only 1 bit changes.

Since the phase information will be meaningless at regions where the amplitude is zero, these regions are also marked in the noise mask [9] and the **total number of bits in the template will be the angular resolution times the radial resolution**.



(For Sample 1)



(For Sample 2)

Selection of 20 points radial for 240 radii along 360°



(For Sample 1)



(For Sample 2)

The rectangular strip stretched after noise removal.



(For Sample 1)



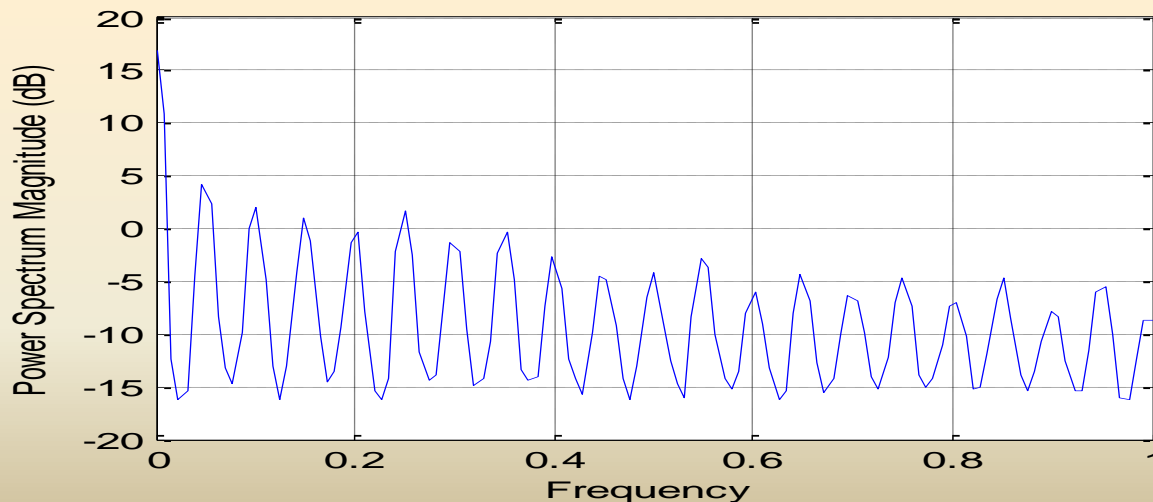
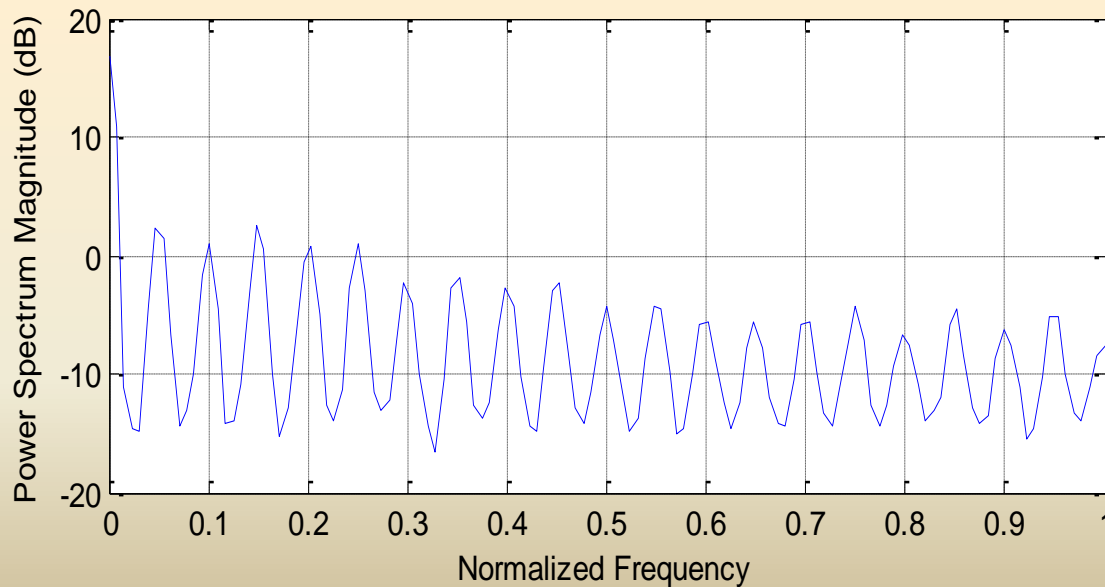
(For Sample 2)

Gabor Filter transformation of the strip.

Gabor Filter transformation of the strip.

The template generated using the log Gabor filter is converted into a one dimensional vector. This one-dimensional vector is used as the digital watermark for watermarking the audio signal. The **power spectral density** (PSD) of the sample watermark is given in Fig. in next slide.

The PSD of the watermark reveals that the power of the signal is approximately equally distributed in the entire frequency spectrum. This property is attractive for **spread spectrum techniques** [13], [14] where the watermark is needed to be spread across the entire spectrum. A certain degree of randomness is present which is indicated by the PSD that makes it suitable to be the secret key for watermarking.

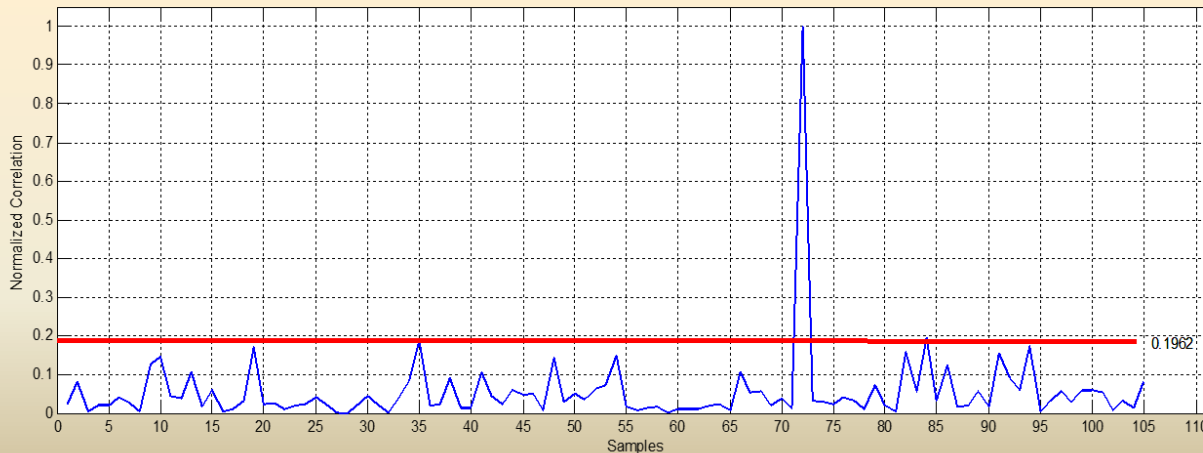


PSD of two Sample Iris based watermark generated

The PSD of the watermark reveals that the power of the signal is approximately equally distributed in the entire frequency spectrum.

This property is attractive for **spread spectrum techniques** [13], [14] where the watermark is needed to be spread across the entire spectrum. A certain degree of randomness is present which is indicated by the PSD that makes it suitable to be the secret key for watermarking.

Uniqueness of the Bio-Keys in the Database



Normalized Correlation of the 50th and 72nd Biometric generated watermark with other Samples

The fig. shows the NC) of the 50th sample with all other biometric watermark in the database. The high spike indicates the autocorrelation of the biometric watermark. Subsequent to the highest spike in the figure the next highest spike is 0.1231 that is the best correlation with some other biometric watermark in the database. Similarly, Fig. 8 shows the NC of the 72nd sample with other biometric watermarks.



Feature extraction from Fingerprint Image.

Step 1: Read fingerprint image gray scale format.

Step 2: Convert grayscale image into binary image.

Step 3: We apply a morphological operation on the binary image so that using this operation ridges in the fingerprint image will be just one pixel wide.

Step 4: Identification of the feature points called minutiae points is done by computing the number of one value neighbor of each 3×3 window:

If the central is one and has only 1-one value neighbor, then the central pixel is Termination. If the central is one and has 3-one value neighbor, then the central pixel is Bifurcation.

If the central is one and has 2-one value neighbor, then central Pixel is a usual pixel.

Step5: Apply filtering operation on this thinned image and extract all termination points and bifurcation points.

Step 6: Next we calculate the distance between the minutia points with the following algorithm:

- Define a distance value D .
- Calculation of distance between two feature points:

Let $a = (x_1, y_1)$ and $b = (x_2, y_2)$ are two feature points then Euclidean distance between feature points a and b is
$$D = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$$

where (x_1, y_1) and (x_2, y_2) are Cartesian coordinates of feature points a and b respectively.

- Process all minutiae points and remove some of these minutiae points (By comparing with the distance value D)

Process 1: if the distance between a termination and a bifurcation is smaller than D , we remove this feature point.

Process 2: if the distance between two bifurcations is smaller than D , we remove this feature point.

Process 3: if the distance between two terminations is smaller than D , we remove this feature point.

Step 7: Define region of Interest and suppress minutiae points external to this region of Interest.

The coordinates and orientation of these minutiae is the biometric template.

Use of the Bio-Keys !

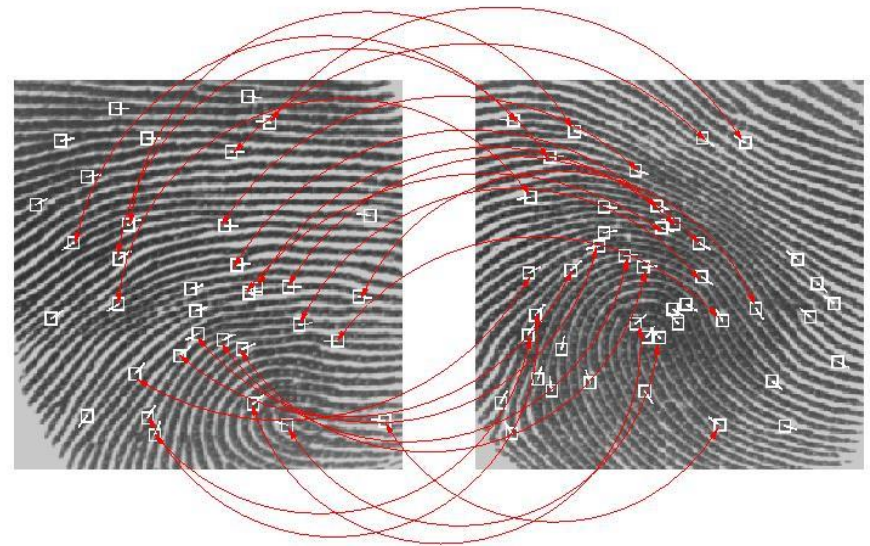
The use of biometric features as a digital watermark and its unique identification under various signal processing attacks are explained in the following steps:

- Pre-processing of the fingerprint image and feature point extraction.
- A digital watermark is generated from the fingerprint features. The binary image of fingerprint was used as the digital watermark in this proposed method.
- The feature points are to be extracted from the binary image (used as digital watermark).
- The biometric based watermark is embedded in the cover file using a watermarking algorithm.
- The watermarked image is exposed to the signal processing attacks and the watermark is recovered from this attacked watermarked image.
- Feature points are extracted from the recovered watermark.
- Feature point matching is done between feature points of the original watermark and the feature points of the recovered watermark.

Unique Identification is done when the feature points match for a minimum number of points.

As per US standard- When two fingerprints have a **minimum of 12 matched feature points** they are considered to have come from the same finger.

Hence the goal of this method is to extract feature points from the recovered watermark and uniquely map it to the feature points of the original biometric image for identification where at **least 12 matches** for clear and unique identification.



Feature extraction from Fingerprint Image – Results !

Gray Scale Image



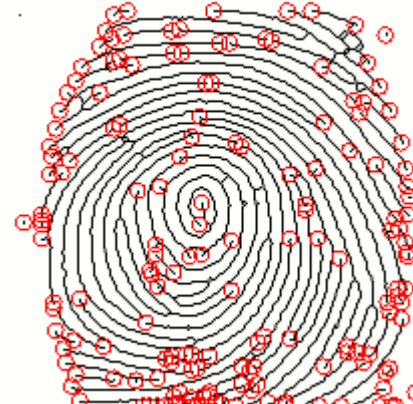
Binary Image



Thinned Image



Ridge Termination Points



Ridge Bifurcation Points



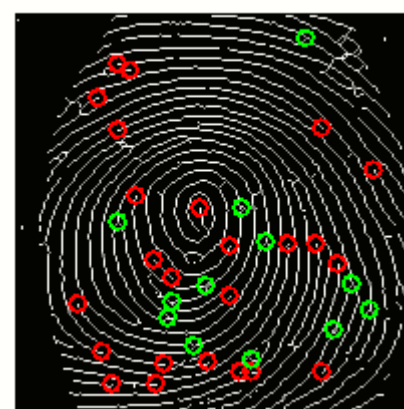
Remaining Ridge Termination Points



Remaining Ridge Bifurcation Points



Minutiae Points inside the defined ROI



Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition.

One method tried and experimented is DWT-SVD based watermarking algorithm

Watermark Embedding:

- (1) Use **one-level Haar DWT** to decompose the cover image A into four subbands: (cA, cH, cV, cD) . Where cA represents approximation coefficients matrix and cH, cV, cD represents details coefficients matrices (horizontal, vertical, diagonal, respectively).
- (2) Apply SVD to cD subband
$$cD = U S V^T \tag{1}$$
- (3) Modify the singular values in cD subband with watermark image and then **apply SVD** to them: $S + \alpha W$ (2)
where W is digital watermark and α denotes the scale factor. The scale factor is used to control the strength of the watermark to be inserted.
- (4) Obtain modified DWT coefficient cD^w
$$cD^w = U S_w V^T \tag{3}$$
- (5) Obtain the watermarked image A_w by performing the inverse DWT using one set of modified DWT coefficient (cD^w) and three sets of unmodified DWT coefficients (cH, cV, cD).

The results obtained of perceptual transparency in this method for embedding a watermark was very encouraging for a watermark **Data rate of 256:1 in spatial domain.**

256:1 is a enough data rate for watermarking for conventional reasons. Almost all the reports in the literature has used a minimum data rate of 256:1 and the results for perceptual transparency and robustness are optimized !

The Design Challenge !

A Bio-key will have a minimum amount of information and we cannot reduce it beyond a certain limit for unique identification purpose.

For example a typical iris template has the following resolution:

Radial resolution : 20

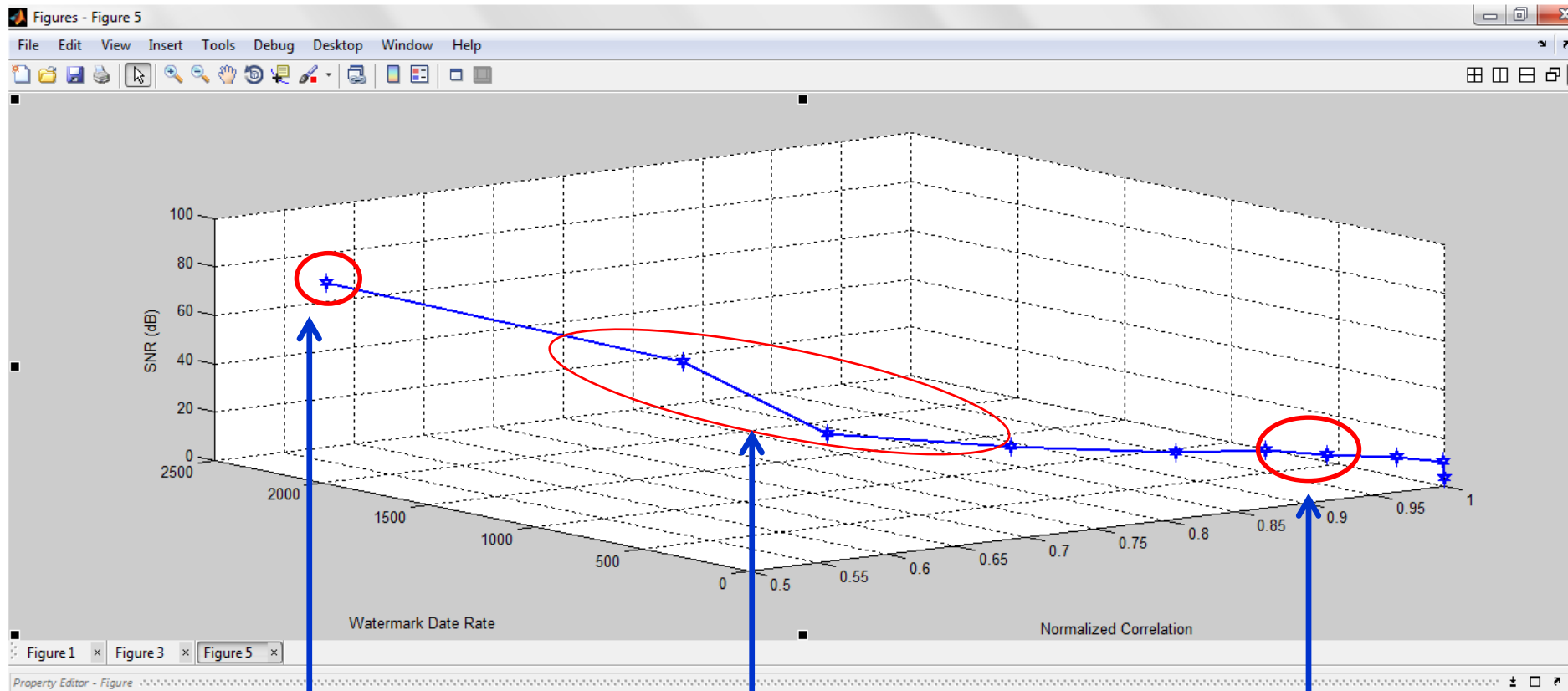
Angular resolution : 240

This gives 4800 feature points. The application of Gabor filter gives 2 bits per point and hence it will generate 9600 bits for this template.

Now in an image of $512 * 512$ the 9600 bit bio-key will need a
watermark data rate of 27:1 !

Maintaining perceptual transparency under such a watermark data rate for embedding a bio-key is a seriously challenging issue !

Accuracy of Detection, Perceptual Transparency, Watermark data rate under signal processing attacks – Median Filtering Attack - In the SVD based Method.



High SNR

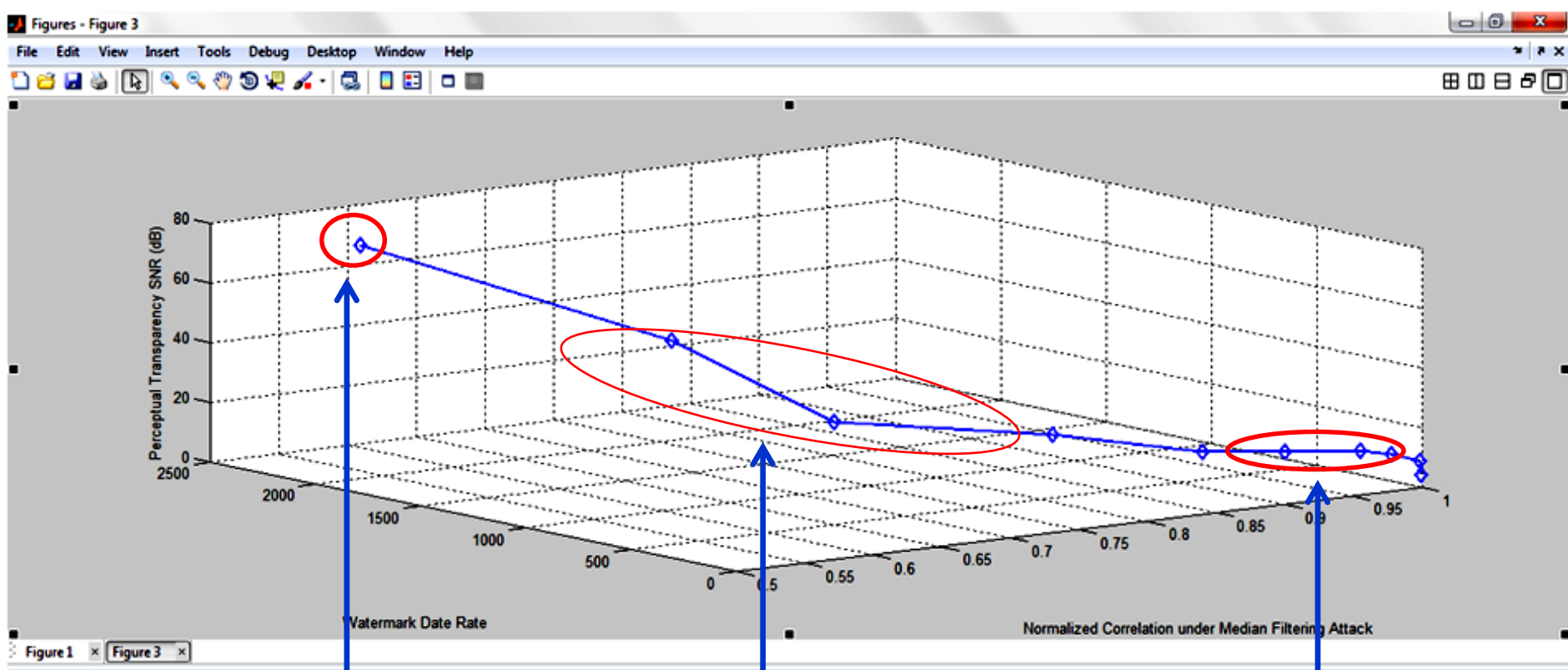
Low Watermark Data rate
Poor Detection under

Region where optimization
is to be done !

Low SNR

High Watermark Data rate
Good Detection under
Median Filtering attack

Accuracy of Detection, Perceptual Transparency, Watermark data rate under signal processing attacks – Histogram Equalization Attack - In the SVD based Method.



High SNR

Low Watermark Data rate
Poor Detection under

Region where optimization
is to be done !

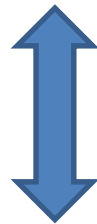
Low SNR

High Watermark Data rate
Good Detection under
Median Filtering attack

The Challenge in the Research Problem for Bio-Key.

The main challenge in embedding a Bio-key is that if the **perceptual transparency parameter is fixed**, the design of a watermarking system cannot obtain high robustness and a high watermark data rate **at the same time**.

So one key area of Bio-Key embedding is to find the highest watermark bit rate obtainable under perceptual transparency and developing algorithm to approach the limit.



OPTIMIZATION of both these issues.

This of course has to comply with the minimum size of the biometric template for unique identification and there has to be efforts for decreasing the size of the biometric template.

Algorithm -1 for - Digital watermarking (Images) of Bio-Keys

Discrete-Cosine-Transform (DCT) is one of the transformation methods which provides embedding of watermark by maintaining the requirements of watermarking like robustness and perceptual transparency. In this method the watermarking is done using the DCT transformation. The DCT allows an image to be broken up into different frequency bands, making it much easier to embed watermarking information into the middle frequency bands of an image. Two-dimensional DCT for an input image A and output image B is

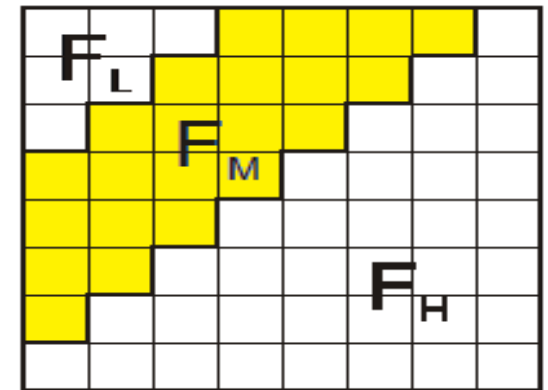
$$B_{pq} = \alpha_p \alpha_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \left(A_{mn} \cos \frac{\pi(2m+1)p}{2M} \cos \frac{\pi(2n+1)q}{2N} \right)$$

$$0 \leq p \leq M-1, 0 \leq q \leq N-1$$

$$\text{where } \alpha_p = 1/\sqrt{M}, p = 0 \text{ and } \sqrt{2/M}, 1 \leq p \leq M-1$$

The mid-frequency bands are chosen for watermarking such that they have minimum effect on the perceptual components and they avoid the most visual important parts of the image (low frequencies) without over-exposing themselves to removal through normal signal processing attacks like compression and noise attacks (high frequency).

In this technique the middle-band DCT coefficients are used to encode a single bit into a DCT block. The middle-band frequencies of an 8×8 DCT block as shown the Figure.



Definition of DCT Regions for 8×8 Block

Next two locations $B_i(u_1, v_1)$ and $B_i(u_2, v_2)$ are chosen from the F_M region for comparison. Rather than arbitrarily choosing these locations, extra robustness to compression can be achieved if the choice is based on coefficients on the recommended **JPEG quantization table**. If two locations are chosen such that they have identical quantization values, we can feel confident that any scaling of one coefficient will scale the other by the same factor and hence preserving their relative size.

The DCT block will encode a “1” if $B_i(u_1, v_1) > B_i(u_2, v_2)$; otherwise it will encode a “0”. The coefficients are then swapped if the relative size of each coefficient does not agree with the bit that is to be encoded [18]. The swapping of such coefficients should not alter the watermarked image significantly, **as it is generally believed that DCT coefficients of middle frequencies have similar magnitudes.**

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Quantization values used in JPEG compression scheme.

During the detection of the watermark, the watermarked image is divided into 8×8 blocks and then for each block if $B_i(u_1, v_1) > B_i(u_2, v_2)$ then a 1 is decoded else 0 is decoded. This is repeated for all the blocks and the digital watermark is decoded.

Experimental results on Perceptual Transparency Using bio-key generated from Iris and FP Features

PSNR between Original Image and Watermarked Image

S. No.	Image Sample	PSNR (dB) Bio Key from FP features	PSNR (dB) Bio Key from Iris features
1.	Lena gray	81.2121	79.8832
2.	Lena_color	91.9343	90.9354
3.	Baboon_gray	73.7805	77.4005
4.	Baboon_color	85.7172	85.7172
5.	Peppers_gray	78.2117	77.7517
6.	Peppers_color	89.1234	88.921
7.	House_gray	76.2112	78.9878
8.	House_color	92.1211	90.3239
9.	Cameraman_gray	86.0976	80.5460
10.	Pirate_gray	81.0098	79.0584



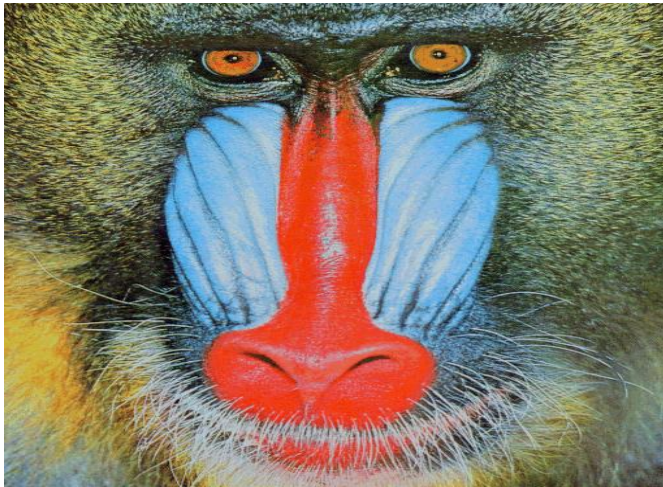
Watermarking Using the Bio-Key Generated from Fingerprint Image



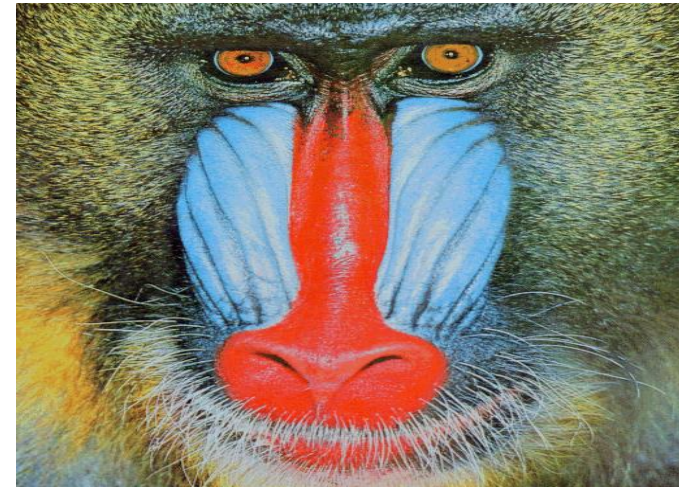
Cover Image Sample "Lena"



Watermarked Image Sample "Lena"



Cover Image Sample "Baboon"



Watermarked Image Sample "Baboon"



Watermarking Using the Bio-Key Generated from Fingerprint Image



Cover Image Sample "Peppers"



Watermarked Image Sample "Peppers"



Cover Image Sample "House"



Watermarked Image Sample "House"



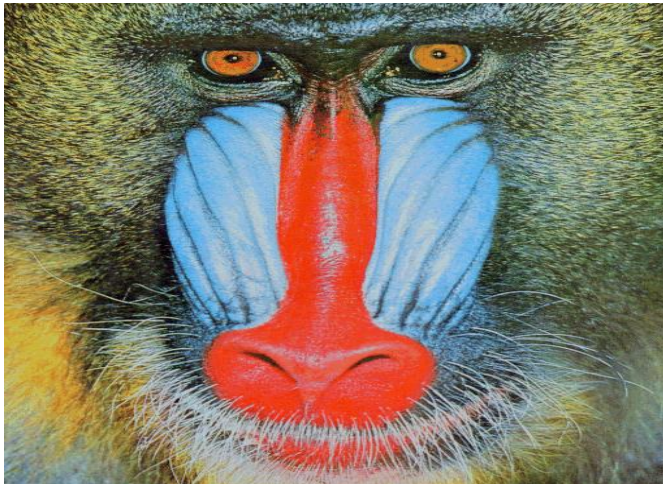
Watermarking Using the Bio-Key Generated from Iris Image



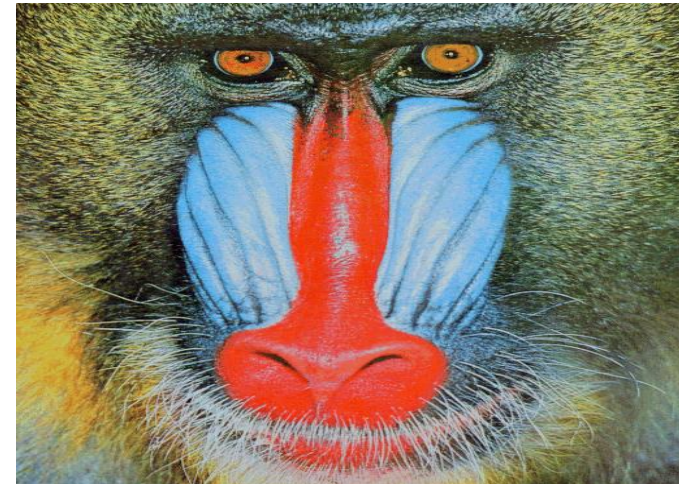
Cover Image Sample "Lena"



Watermarked Image Sample "Lena"



Cover Image Sample "Baboon"



Watermarked Image Sample "Baboon"



Watermarking Using the Bio-Key Generated from Iris Image



Cover Image Sample "Peppers"



Watermarked Image Sample "Peppers"



Cover Image Sample "House"



Watermarked Image Sample "House"



Experimental results of Robustness to signal Processing attacks for bio-key generated from Iris features

NC between original Bio-Key and Extracted Bio-Key

		Lena	House	Peppers
S. No.	Signal Processing Attack	NC	NC	NC
1.	Median filter	0.9990	0.9971	0.9742
2.	Gaussian noise	0.9994	0.9971	0.9745
3.	Histogram equalization	0.9990	0.9965	0.9724
4.	Intensity Adjustment	0.9994	0.9812	0.9749
5.	Gamma corrected	0.9994	0.9711	0.9749
6.	Gaussian LPF	0.9994	0.9912	0.9749
7.	Jpeg compression	0.9994	0.9812	0.9749
8.	Contrast Adjustment	0.9994	0.9812	0.9749
9.	Brightness 5%	0.9994	0.9862	0.9749
10.	Brightness 10%	0.9994	0.9761	0.9747
11.	Image Sharpening	0.9994	0.9812	0.9749
12.	Image Blurring Attack	0.9841	0.9861	0.9629



Experimental results of Robustness to signal Processing attacks for bio-key generated from FP features





NC between original Bio-Key and Extracted Bio-Key





		Lena	House	Peppers
S. No.	Signal Processing Attack	NC	NC	NC
1.	Median filter	0.9761	0.976	0.9721
2.	Gaussian noise	0.9231	0.9989	0.9871
3.	Histogram equalization	0.9121	0.9871	0.9876
4.	Intensity Adjustment	0.9234	0.9897	0.9891
5.	Gamma corrected	0.9911	0.9671	0.9981
6.	Gaussian LPF	0.9231	0.9561	0.9765
7.	Jpeg compression	0.9981	0.9871	0.9321
8.	Contrast Adjustment	0.9876	0.9765	0.9671
9.	Brightness 5%	0.9234	0.9871	0.9871
10.	Brightness 10%	0.9987	0.9871	0.9212
11.	Image Sharpening	0.9912	0.9231	0.9312
12.	Image Blurring Attack	0.9786	0.9762	0.9218



Experimental results of Robustness to signal Processing attacks for bio-key generated from FP features

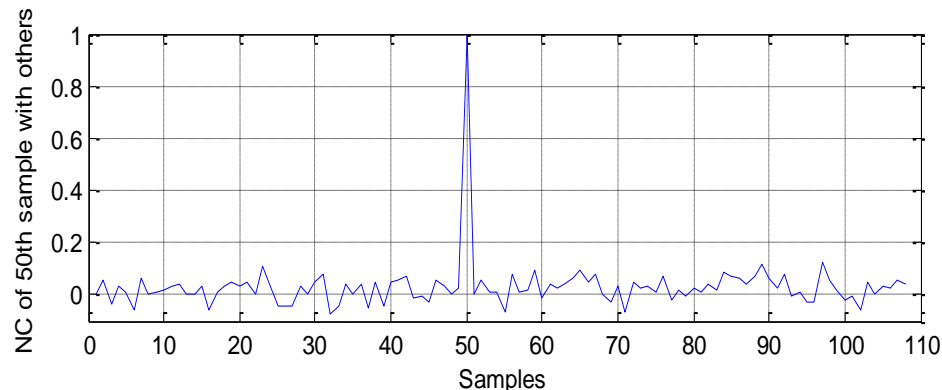
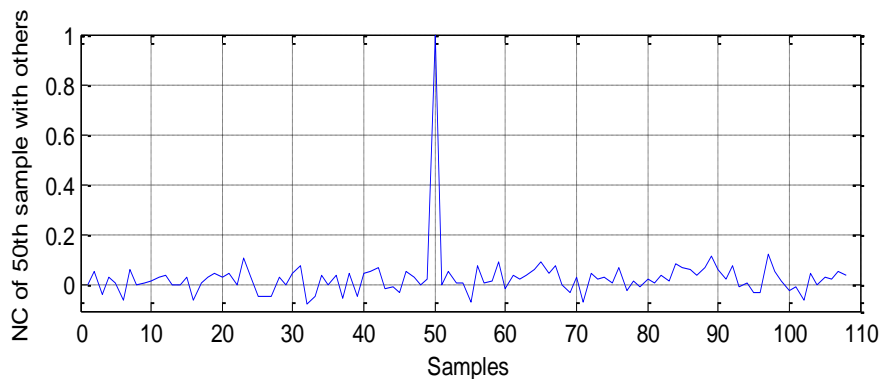
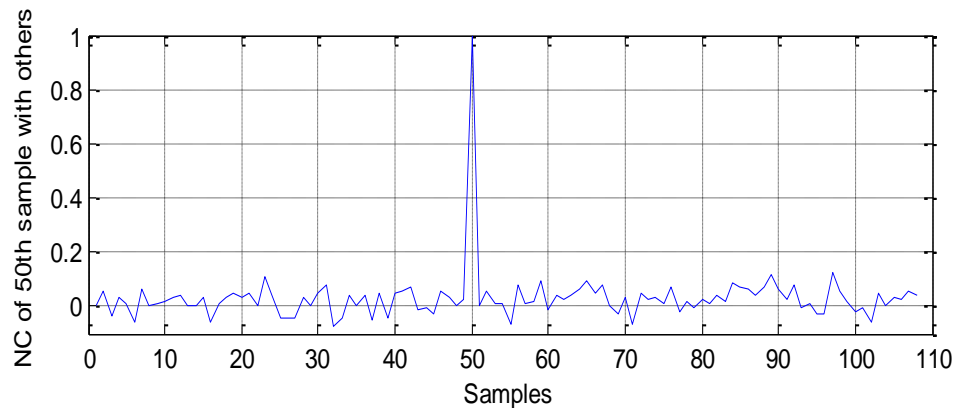
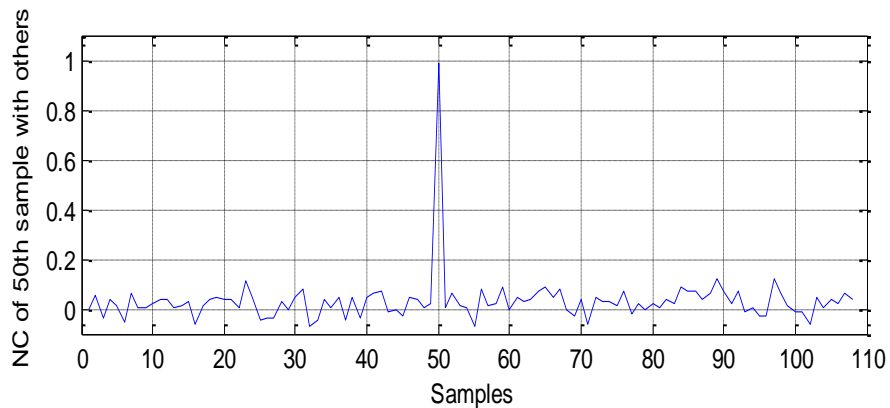
NC between original FP- Bio-Key and Extracted FP-Bio-Key

Total Number of Minutia Points : 32				
Sl No	Attack	NC	Recovered watermark	No. of feature Points matched
1.	Brightness 5%	0.9928		28
2.	Brightness 10%	0.9121		15
3.	Contrast 5%	0.9938		28
4.	Contrast 10%	0.9930		28

Total Number of Minutia Points : 32				
Sl No	Attack	NC	Recovered watermark	No. of feature Points matched
5.	Median Filter 2	0.9937		28
6.	Gaussian Low Pass Filter	0.9938		28
7.	JPEG Compression	0.9581		15
8.	Uniform Noise	0.9938		27

Experimental results of Robustness to signal Processing attacks for bio-key generated from Iris features

NC based identification of the Bio-Keys



Identification of Biometric watermark under signal processing attacks

(a) Median Filtering (b) Intensity Adjustment (c) Low pass filtering (d) Histogram Equalization



Algorithm -2 for - Digital watermarking (Audio) of Bio-Keys

The watermarking method used to watermark an audio signal by using dither modulation quantization in SVD domain.

Malay Kishore Dutta, Anushikha Singh, Radim Burget, Hicham Attasi, Ankur Choudhary & K.M. Soni "Generation of Biometric Based Unique Digital Watermark from Iris Image" 36th International Conference on Telecommunications and Signal Processing (TSP-2013) July 2013, Rome, Italy, pp 685-689.

Embedding the Bio-Key in the Audio Signal

The watermarking method is explained as follows:

Divide the audio sample in to number of frames equal to number of bits in the watermark. Convert each frame into 2-D matrix, say A_i . Embedding watermark in to the audio sequence is done as following :

for $i=1:N$

$SV(i) = \text{Apply SVD on } A(i);$

$En(i) = \text{Evaluate Euclidean norm of } SV(i);$

Evaluate $\alpha = En(i) / \delta;$

If $l(i) == 1, \text{ then}$

$\acute{\alpha} = \alpha + 1 - \text{rem}(\alpha, 2);$

else

$\acute{\alpha} = \alpha + 1 - \text{rem}(\alpha + 1, 2);$

end if;

*Evaluate $En'(i) = (2 * \acute{\alpha} + 1) / 4;$*

*Evaluate $SV'(i) = SV(i) * En'(i) / En(i);$*

ISV(i) = Apply ISVD using $SV'(i);$

end for

#Merge all the frames to get the watermarked signal.

Extraction of the Bio-Key

WS = Divide WS in to different Partition and Convert each Partition vector into 2D matrix.

for i=1:N

Ext_SV(i) = Apply SVD on WS(i);

Ext_En(i) = Evaluate Euclidean norm of Ext_SV(i);

Evaluate Ext_α = Ext_En(i)/ δ;

if Ext_α is even,

Ext_wm (i) = 0;

else

Ext_wm(i)=1;

end if;

end for

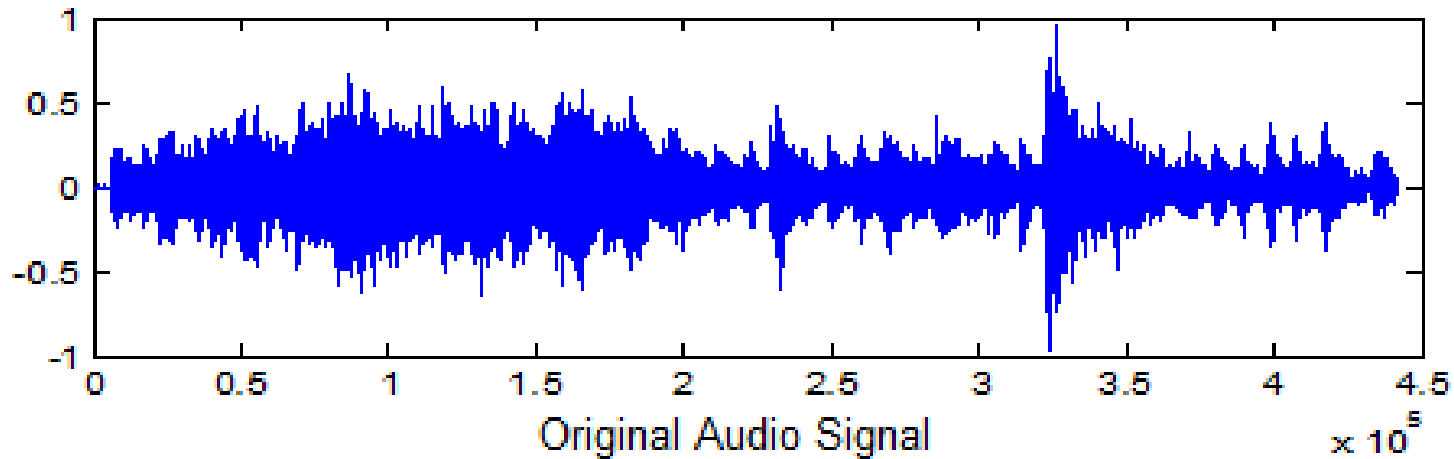
Convert Ext_wm to 2D matrix

This watermarking algorithm is blind in nature which means that the original signal is not needed during the extraction of the watermark

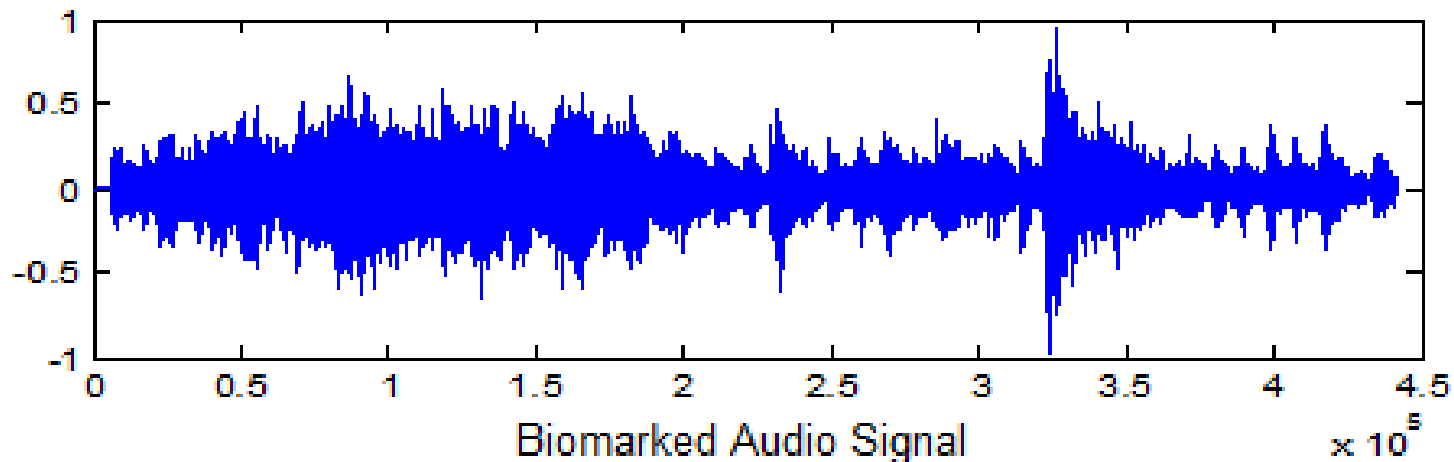
This algorithm was tested in sample audio signals and the recovered watermark was tested **for identification and authentication** which is described in the next section.

Experimental results of Perceptual Transparency of the Audio Signals

Original Audio and Bio-Marked Audio Signal.



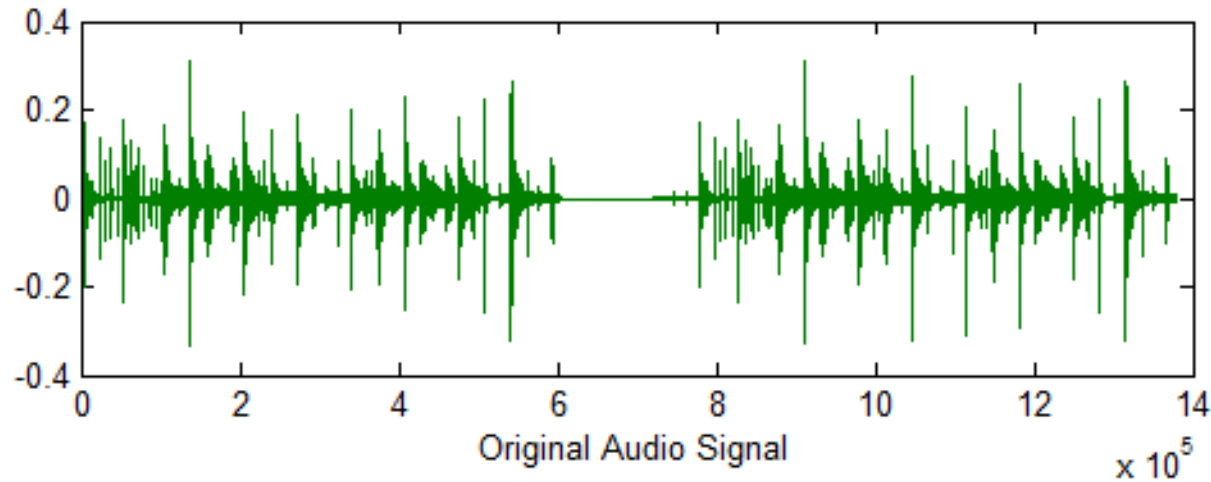
Click
here to
play



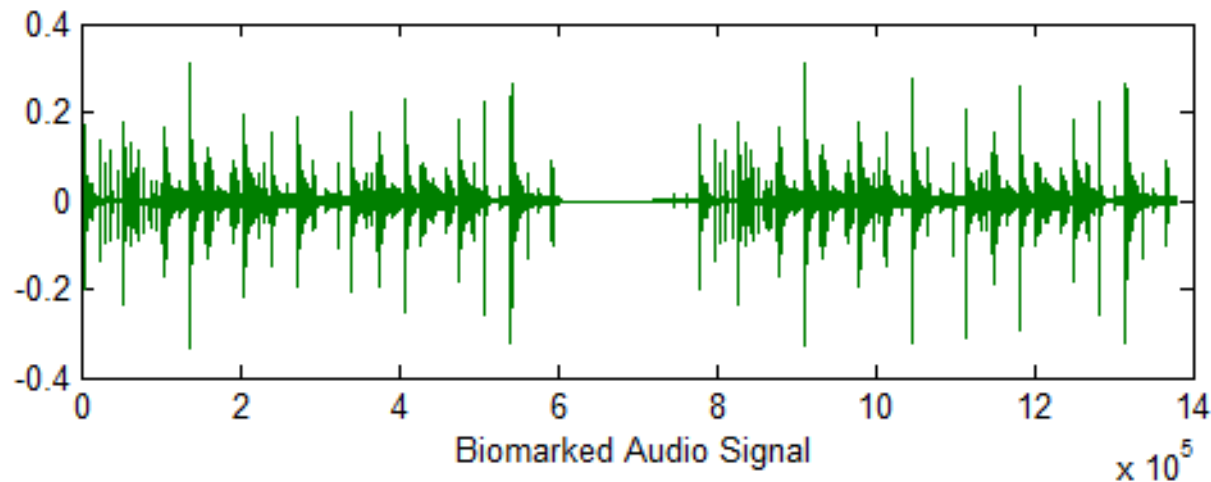
Click
here to
play

Experimental results of Perceptual Transparency of the Audio Signals

Original Audio and Bio-Marked Audio Signal.



**Click
here to
play**



**Click
here to
play**

Experimental results for perceptual transparency :

Subjective Listening Test

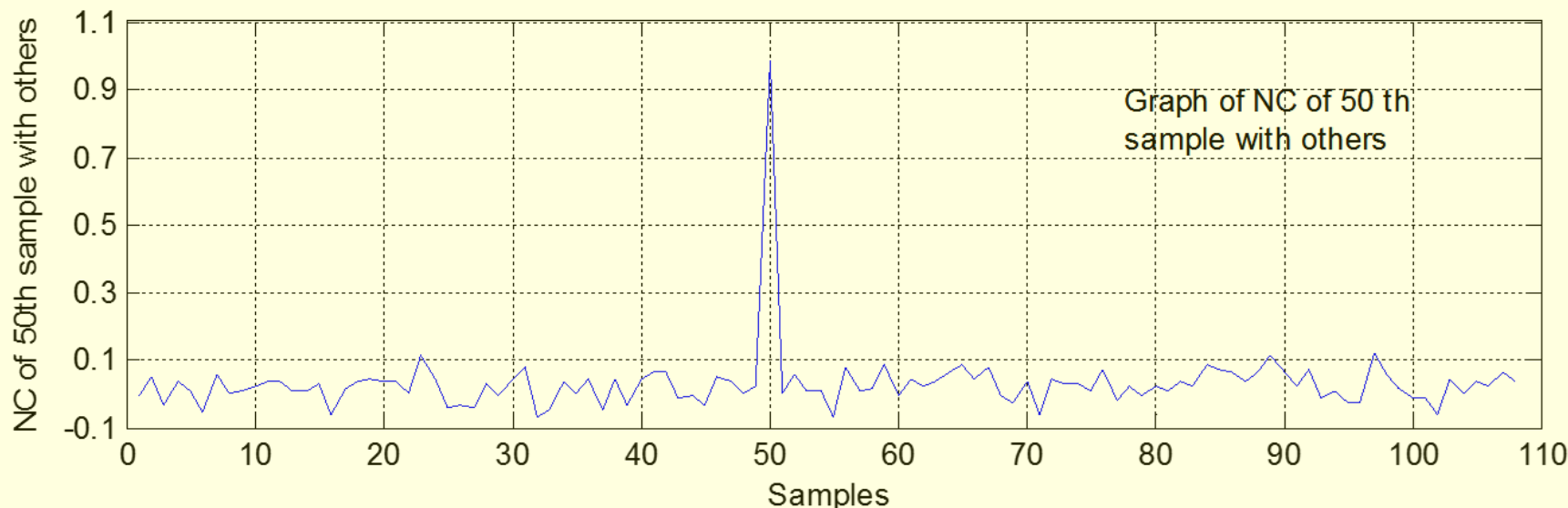
A method to evaluate the audio quality, subjective listening tests have been performed using the mean opinion score (MOS). The definitions of the scores are defined as: 0 for Imperceptible, -1 for Perceptible but not Annoying, -2 for Slightly Annoying, -3 for Annoying, -4 for Very Annoying.

	Sample	SNR		MOS
		50 TH Sample	72 TH Sample	
1	Classical2.wav	25.1 dB	25.17 dB	-0.2
2	Hiphop.wav	30.0 dB	30.1 dB	-0.1
3	Blues1.wav	35.8295 dB	35.8511 dB	-0.3
4	Classical1.wav	29.4491 dB	29.4462 dB	-0.1
5	Country1.wav	36.9755 dB	37.1218 dB	-0.3
6	Country2.wav	33.3003 dB	33.3044 dB	-0.2
7	Folk1.wav	37.9822 dB	37.9822 dB	-0.1
8	Folk2.wav	37.8883 dB	37.8880 dB	-0.1
9	Pop1.wav	40.4801 dB	40.4659 dB	0.0
10	Pop2.wav	36.7900 dB	36.8074 dB	-0.1

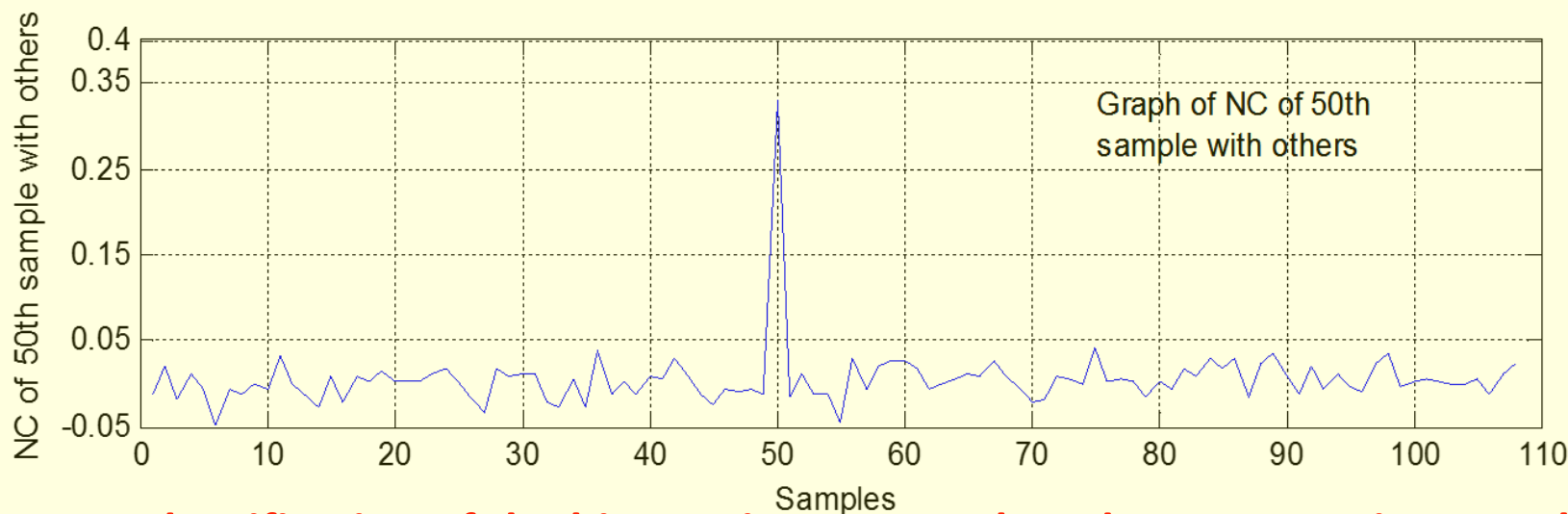
Experimental results of Robustness to signal Processing attacks for bio-key generated from Iris features

Audio File	Type of attack	NC		BER %	
		50 TH	72 TH	50 TH	72 TH
Sample 1 (Classical2)	Attack free	1	1	0	0
	Low pass (8 KHz)	1	1	0	0
	Re-sampling (22 KHz)	1	1	0	0
	Gaussian Noise	0.98	.98	.82	.89
	Re-quantization	1	1	0	0
Sample 2 (Hip-hop)	Attack free	1	1	0	0
	Low pass (8 KHz)	1	1	0	0
	Re-sampling (22 KHz)	1	.98	.75	.75
	Gaussian Noise	0.7	.7	14	14
	Re-quantization	1	1	0	0
Sample 3 (Tabla)	Attack free	1	1	0.12	0.2
	Low pass (8 KHz)	1	1	0	0.1
	Re-sampling (22 KHz)	1	.93	.78	.73
	Gaussian Noise	0.78	.71	12	16
	Re-quantization	1	1	0	0
Sample 4 (Folk)	Attack free	1	1	0	0
	Low pass (8 KHz)	1	1	0	0
	Re-sampling (22 KHz)	1	.91	.75	.73
	Gaussian Noise	0.77	.87	12	11
	Re-quantization	1	1	0	0

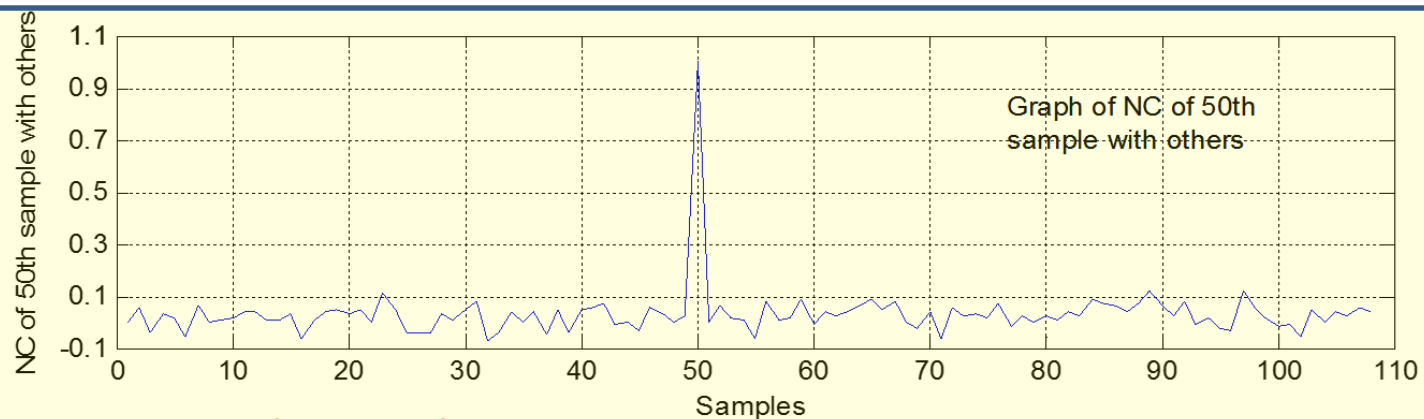
Experimental results **Identification of the Bio-Keys** under various signal Processing attacks



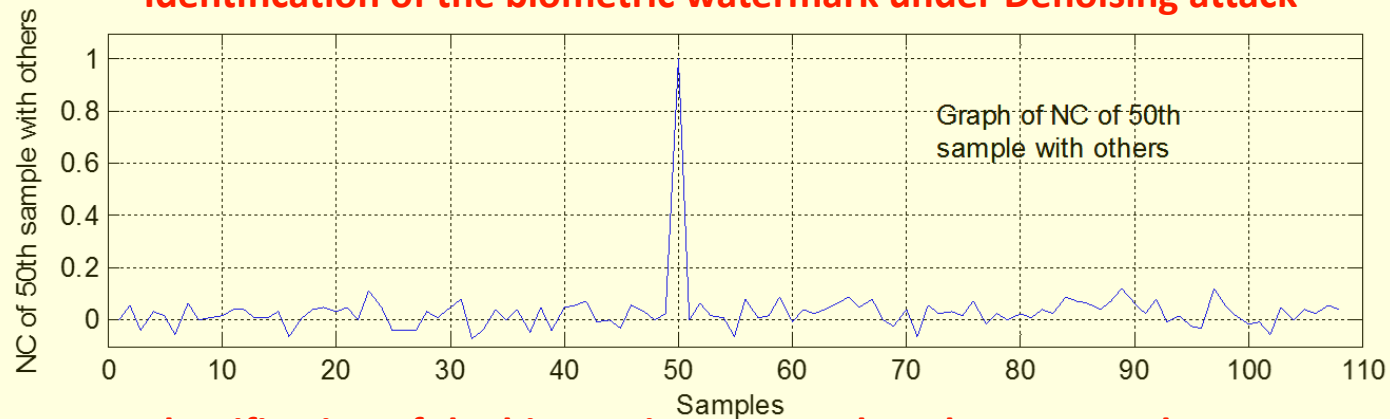
Identification of the biometric watermark under AWGN attack



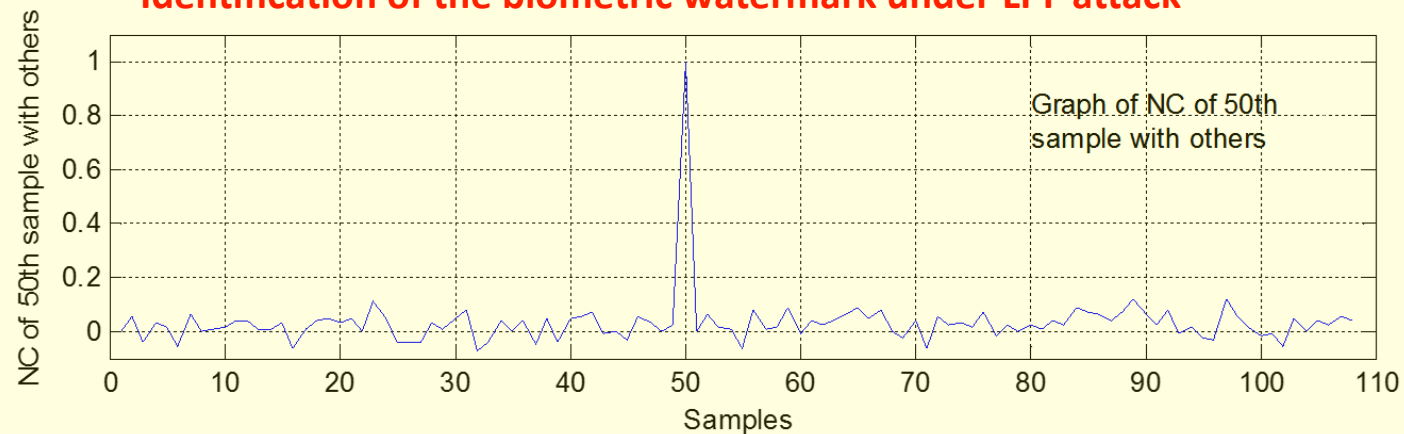
Identification of the biometric watermark under compression attack



Identification of the biometric watermark under Denoising attack



Identification of the biometric watermark under LPF attack



Identification of the biometric watermark under Re-sampling attack

The GUI Model developed for Joint **Bio-Marking** with Bio-Keys from Using Bio-Keys generated from Iris Features.

GUI3

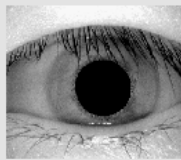
Image Watermarking Using Iris Features As A Digital Watermark

Biometric Watermark Generation

Watermark Generator

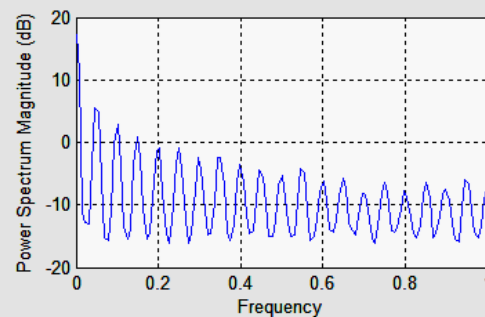
Select A Iris Image

Iris Image



Show Biometric Watermark

Show PSD of Watermark



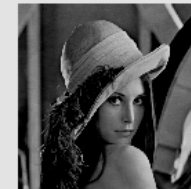
Watermark Extraction

Select A Image Processing Attack

- No Attack
- Median Filter
- Gaussian Low Pass Filter
- Gaussian Noise
- Intensity Adjustment
- Gamma Correction
- JPEG Compression
- Image Blurring

Apply Attack

Select Watermarked Image for Image Processing Attack



Show Attacked Image

Watermark Extractor

Select Watermarked Image or Attacked Image

Calculate BER (%)

0.0416667

BER of Original and Extracted Watermark

Calculate Correlation

0.999161

NC of Original and Extracted Watermark

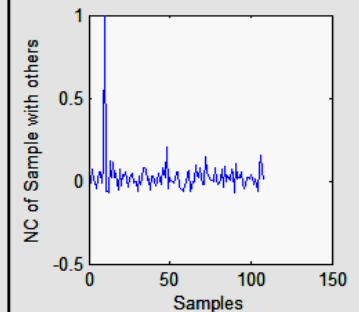
Identification of Watermark

Identification

Select Recovered Watermark for Identification

Show Identification Curve

Matched with Iris Sample10



Watermark Embedding

Select a Host Image

Show Watermarked Image



Watermark Embedder



Calculate PSNR (dB)

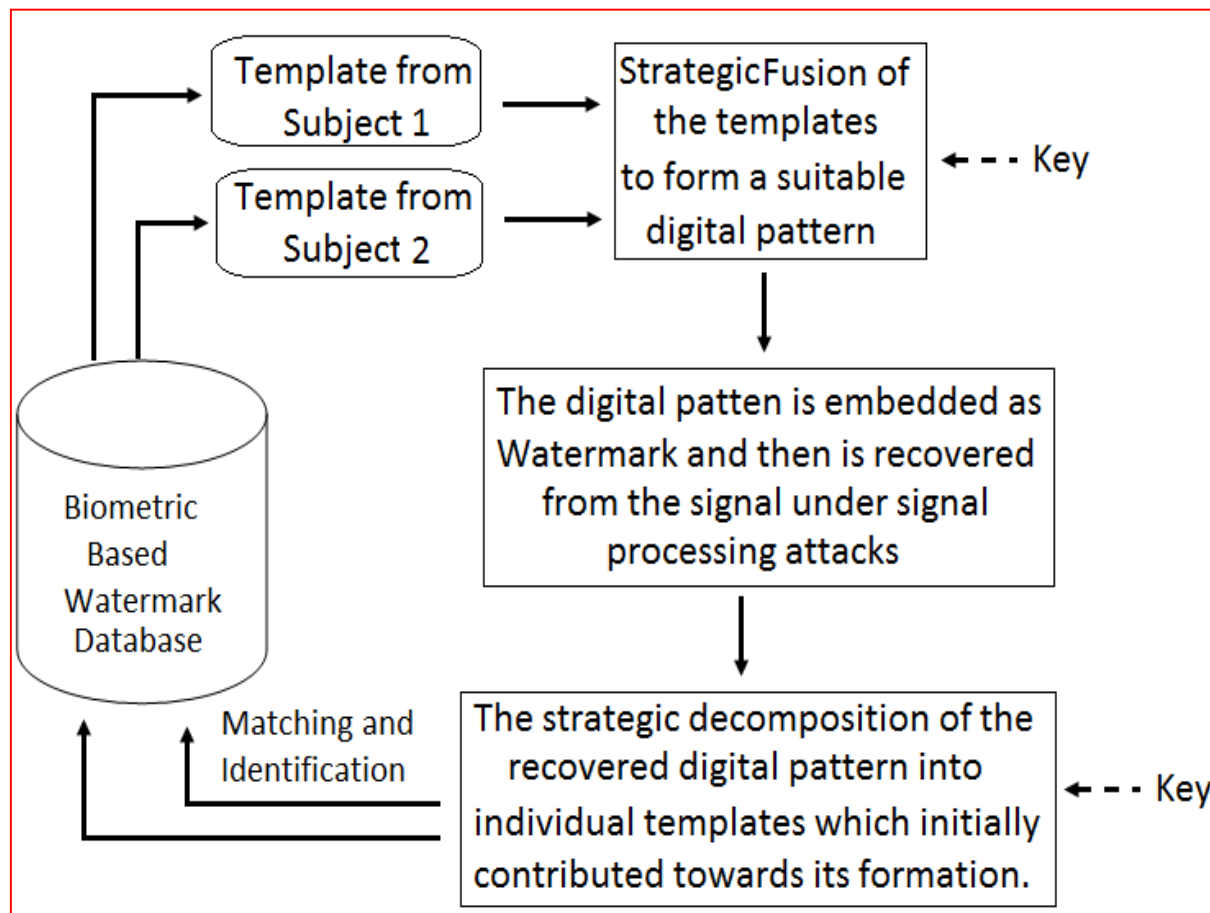
PSNR of original and Watermarked Image

34.6878

The next Question :

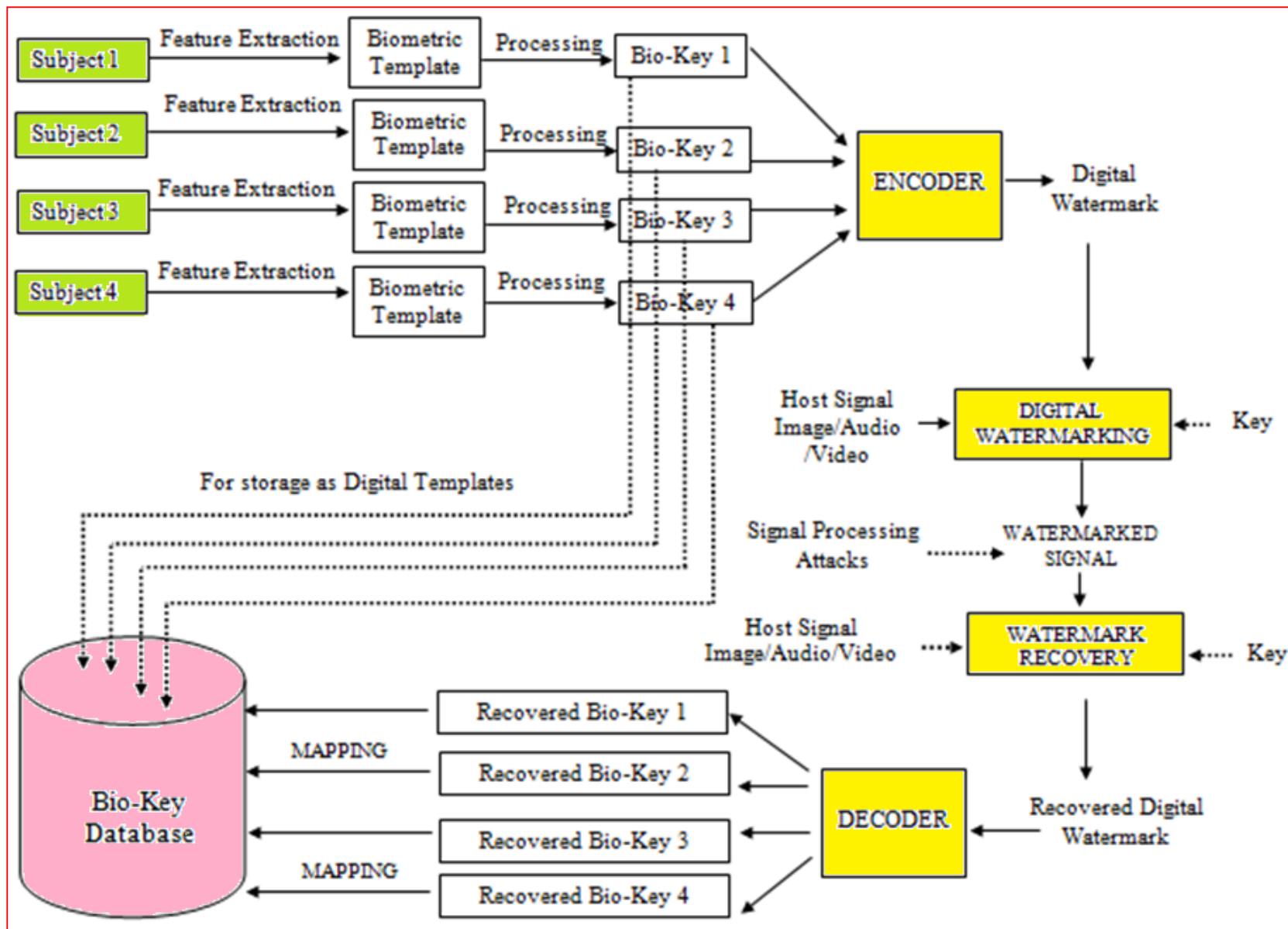
What if a Digital Signal is Jointly Owned by many ?

The Model of Bio-Key For Joint Ownership

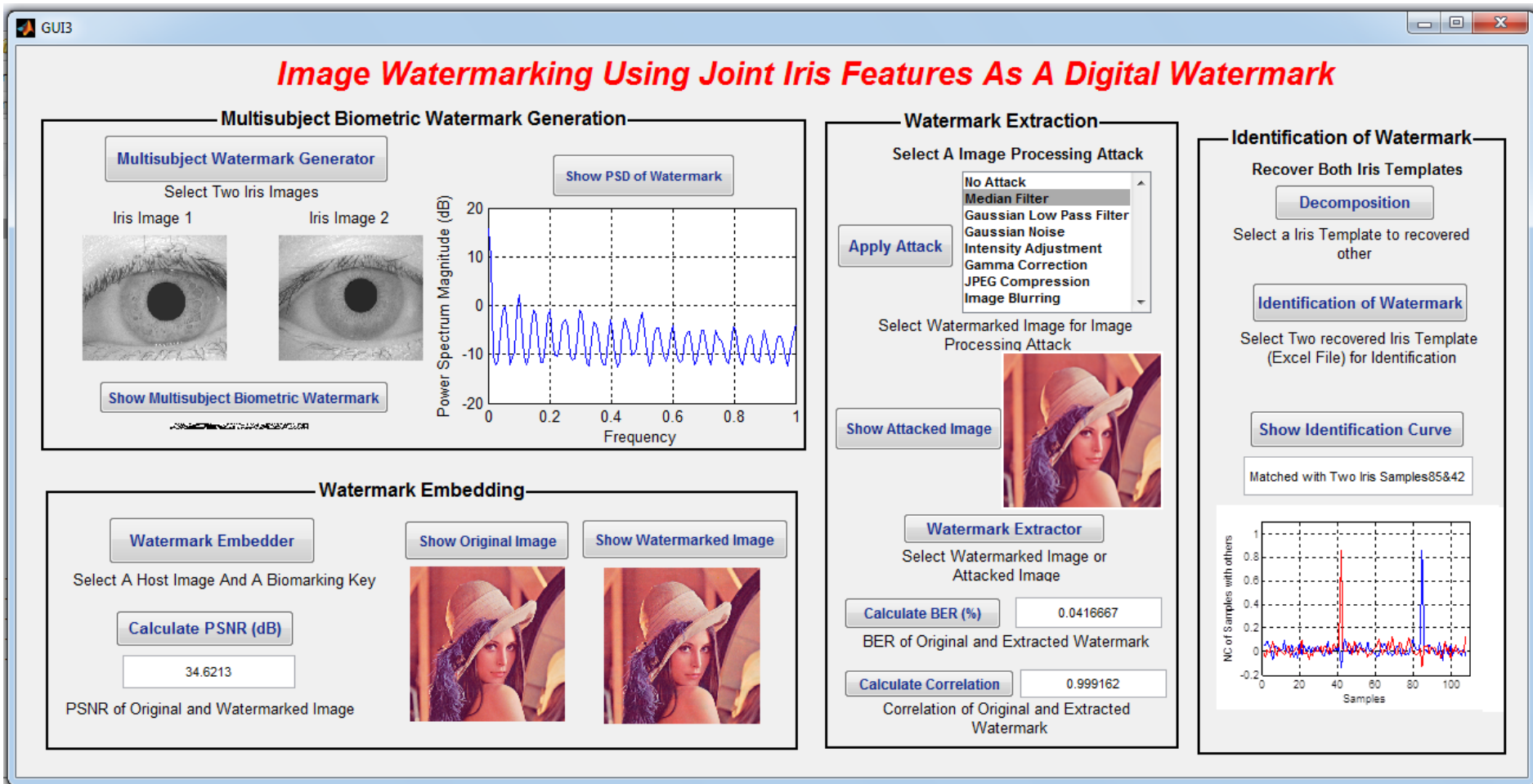


Method to establish joint ownership of digital images by embedding imperceptible digital pattern in the image. This digital pattern is generated from biometric features of more than one subject in a strategic matter so that the identification of individual subject can be done and the multiple ownership of the digital images can be established.

The Watermarking Model of Bio-Key For Joint Ownership



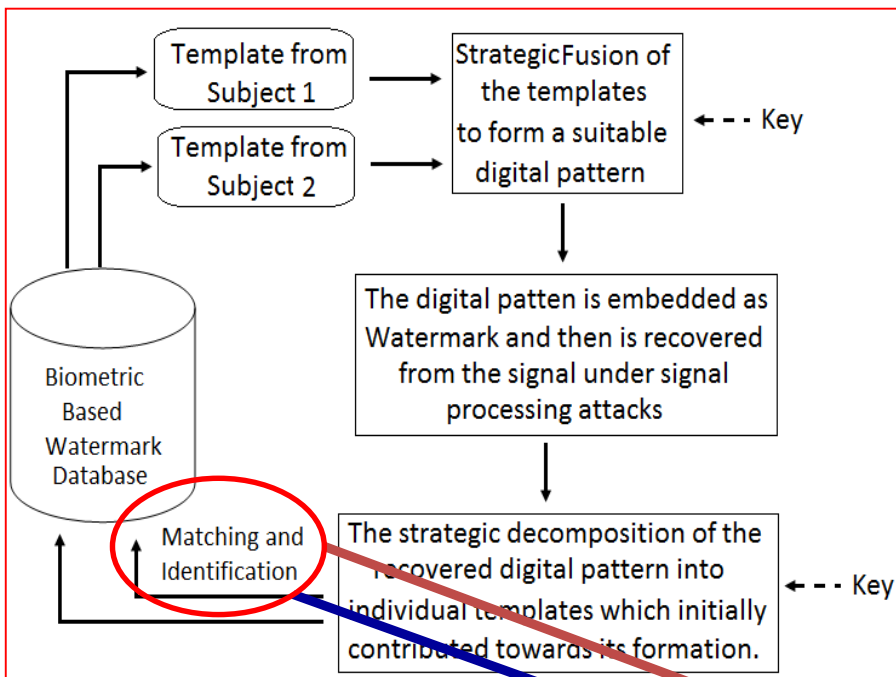
The GUI Model developed for Joint Bio-Marking with Bio-Keys from Multiple Subjects



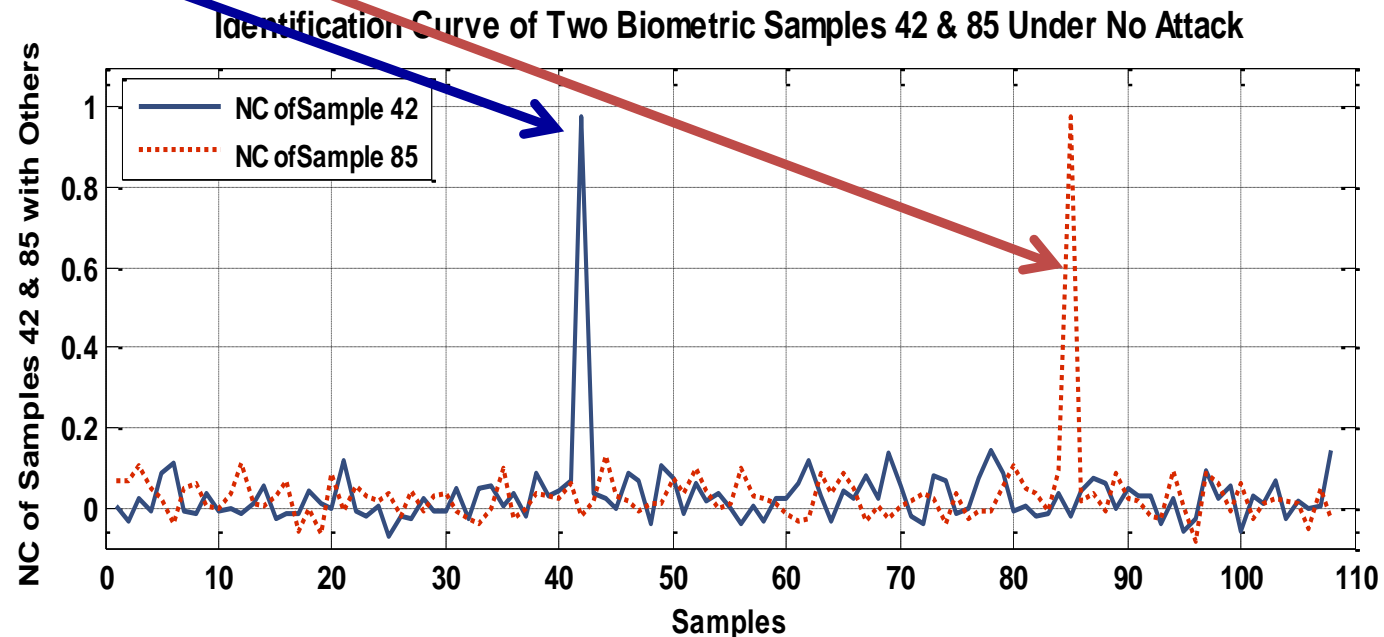
This GUI based Software is developed which can take multiple biometric images as input and then make a bio-key from these multiple images and embed the same in a digital image. This GUI based SW calculates the **perceptual property parameters** like **PSNR** also has the testing facilities against the **robustness to signal processing attacks**. The NC based unique identification of the bio-keys are also plotted with a text box message for identification.

Unique & Distinct Identification of the Bio-Keys

Once the digital watermark is extracted from the signals we need to have a clear, distinct and unique identification of each component of the watermark. It means the extracted watermark has to be decomposed into the individual templates and then each template has to be uniquely mapped to the database. Normalized correlation has been used for identification as given in Fig. in this Slide.



The peaks in the graph indicate that the biometric templates have been uniquely mapped to a particular sample. Hence two peaks for the two templates establish the unique identification of both the templates and a joint ownership is uniquely done.



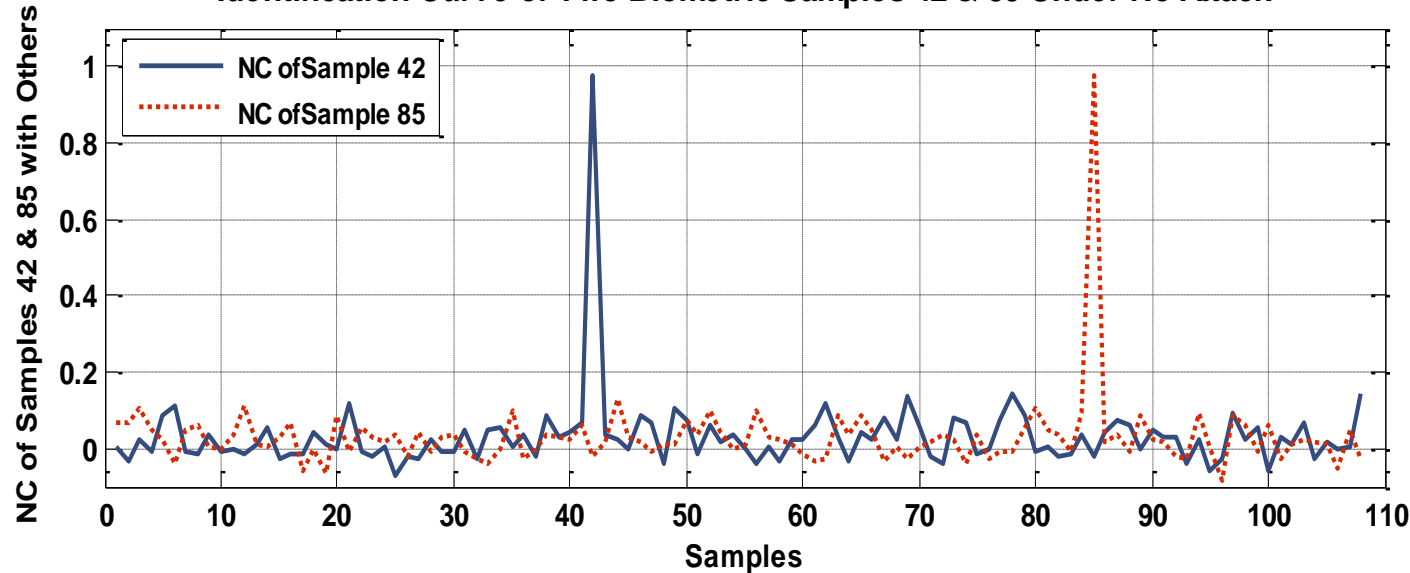
Robustness tests under Multi-Subject Biomarking

The image which was bio-marked with a bio-key generated from multi-subjects was subjected to signal processing attacks and the bio-key was recovered from the attacked image. The NC and the BER between the original watermark and the recovered watermark under signal processing attacks is tabulated in Table . The results given in Table clearly indicate that the watermarking scheme is robust in nature and the results are encouraging for the signal processing attacks.

S. No.	Type of Attack	WM from Iris Sample 1 and 22		WM from Iris Sample 5 and 100	
		NC	BER	NC	BER
1	No attack	0.99937	0.03125%	0.99896	0.052083%
2	Median Filter	0.99833	0.08333%	0.99792	0.10417%
3	Gaussian LPF	0.99937	0.03125%	0.99896	0.052083%
4	Intensity Adjustment	0.99376	0.3125%	0.99315	0.34375%
5	Gaussian Noise	0.99937	0.03125%	0.99896	0.052083%
6	Gamma Correction	0.99937	0.03125%	0.99896	0.052083%
7	JPEG Compression	0.99937	0.03125%	0.99896	0.052083%
S. No.	Type of Attack	WM from Iris Sample 85 and 42		WM from Iris Sample 2 and 74	
		NC	BER	NC	BER
1	No attack	0.99875	0.0625%	0.97755	1.1354%
2	Median Filter	0.99812	0.09375%	0.97733	1.1458%
3	Gaussian LPF	0.99875	0.0625 %	0.97531	1.25%
4	Intensity Adjustment	0.99272	0.36458%	0.86708	7.0625%
5	Gaussian Noise	0.99875	0.0625%	0.97531	1.25%
6	Gamma Correction	0.99875	0.0625%	0.96262	1.8854%
7	JPEG Compression	0.99875	0.0625%	0.97531	1.25%
S. No.	Type of Attack	WM from Iris Sample 24 and 95		WM from Iris Sample 8 and 36	
		NC	BER	NC	BER
1	No attack	0.99979	0.010417%	0.99958	0.020833%
2	Median Filter	0.99958	0.02083%	0.99833	0.08333%
3	Gaussian LPF	0.99875	0.010417%	0.99958	0.020833%
4	Intensity Adjustment	0.90067	5.2188%	0.99459	0.27083%
5	Gaussian Noise	0.99979	0.010417%	0.99958	0.020833%
6	Gamma Correction	0.99462	0.01933%	0.99931	0.02905%
7	JPEG Compression	0.99979	0.010417%	0.99958	0.020833%
S. No.	Type of Attack	WM from Iris Sample 38 and 60		WM from Iris Sample 18 and 76	
		NC	BER	NC	BER
1	No attack	0.99917	0.041667%	0.99910	0.032287%
2	Median Filter	0.99792	0.10417%	0.99433	0.13562
3	Gaussian LPF	0.99917	0.041667%	0.99910	0.032287%
4	Intensity Adjustment	0.99453	0.22917%	0.99281	0.43192
5	Gaussian Noise	0.99917	0.041667%	0.99910	0.032287%
6	Gamma Correction	0.99917	0.041667%	0.99910	0.032287%
7	JPEG Compression	0.99917	0.041667%	0.99910	0.032287%

Identification of the Individual Bio-Keys from the Extracted Digital Watermark

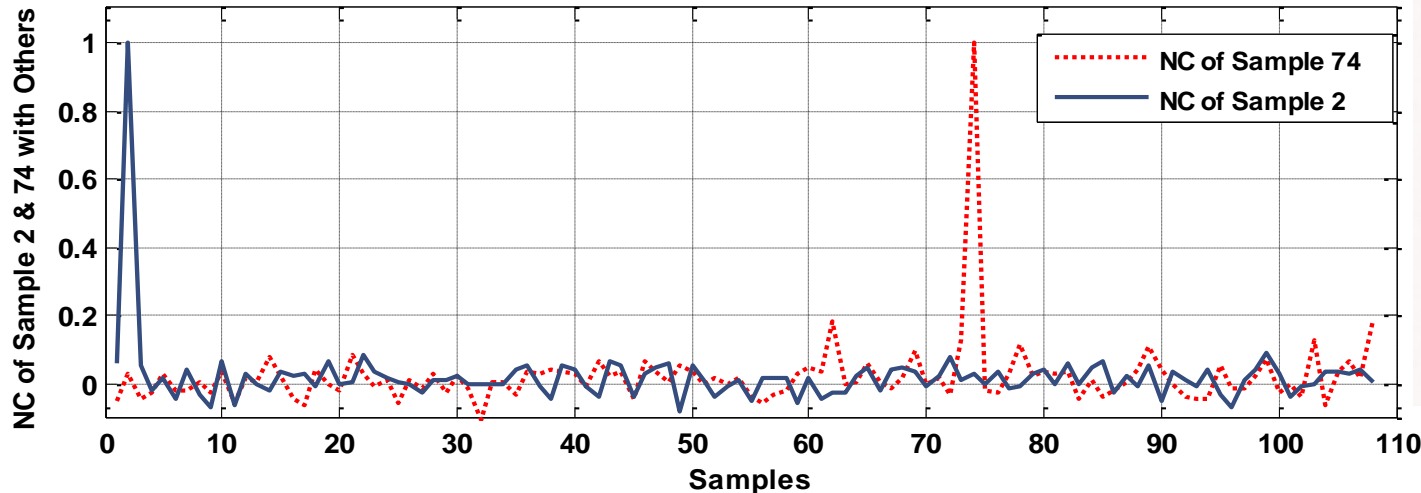
Identification Curve of Two Biometric Samples 42 & 85 Under No Attack



The first peak corresponds to a NC of 0.9990 followed by a next best of 0.1483 for the 42nd biometric template and the second peak corresponds to a NC of 0.9990 followed by a next best of 0.1362 for the 85th biometric template.

This result clearly indicates a unique identification of these two samples in the database.

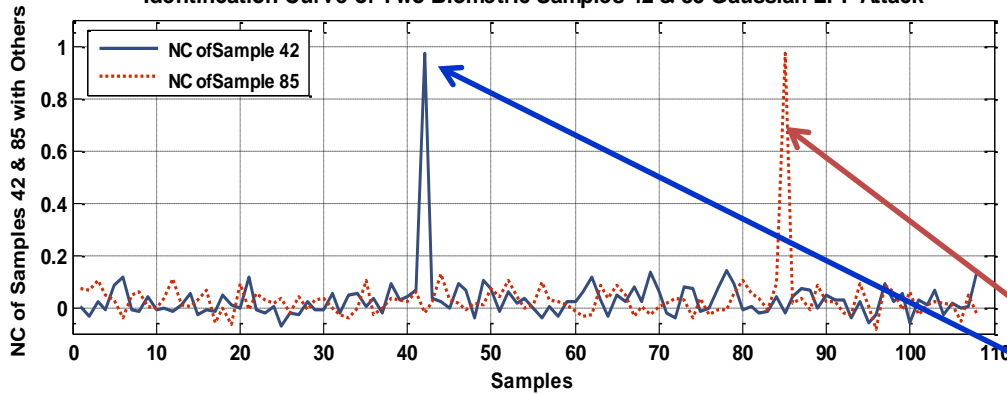
Identification Curve of Two Biometric Samples 2 & 74 Under No Attack



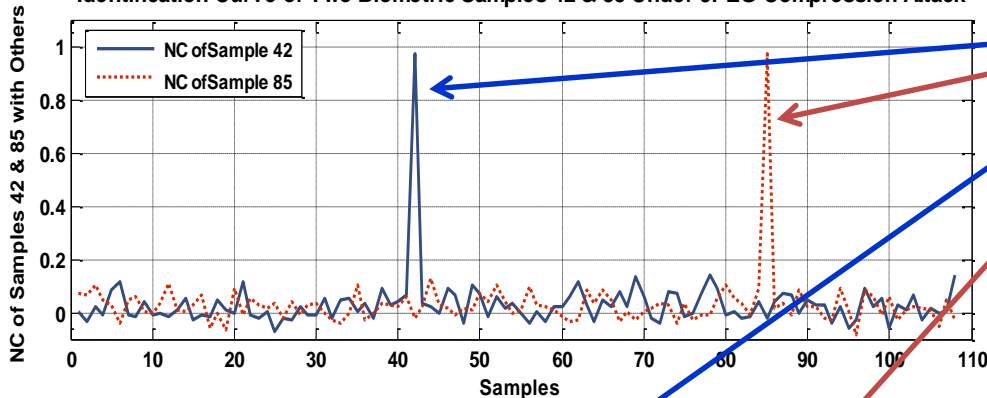
A similar result can be seen for unique identification for the two samples 2 & 74.

Identification of the Individual Bio-Keys Under Signal Processing Attacks

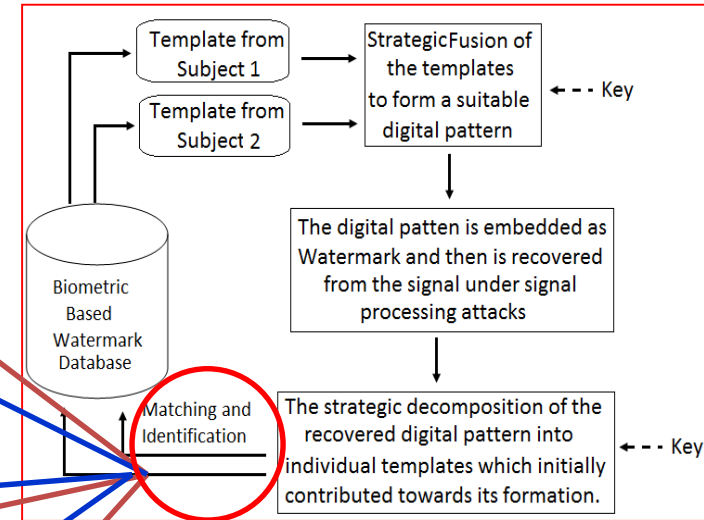
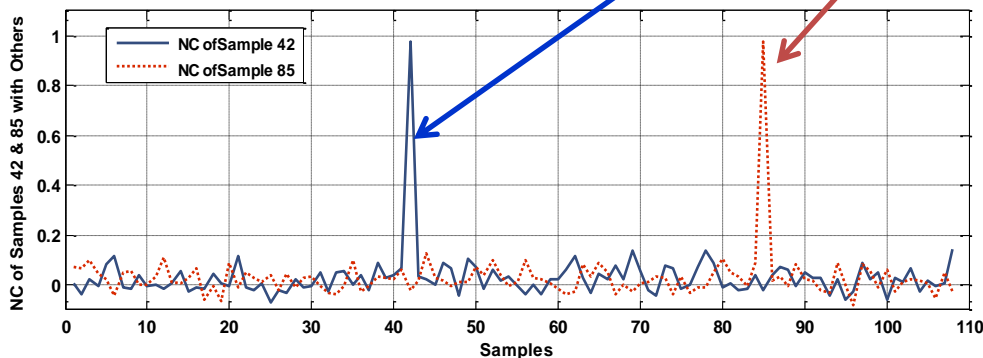
Identification Curve of Two Biometric Samples 42 & 85 Gaussian LPF Attack



Identification Curve of Two Biometric Samples 42 & 85 Under JPEG Compression Attack



Identification Curve of Two Biometric Samples 42 & 85 Under Gaussian Noise Attack

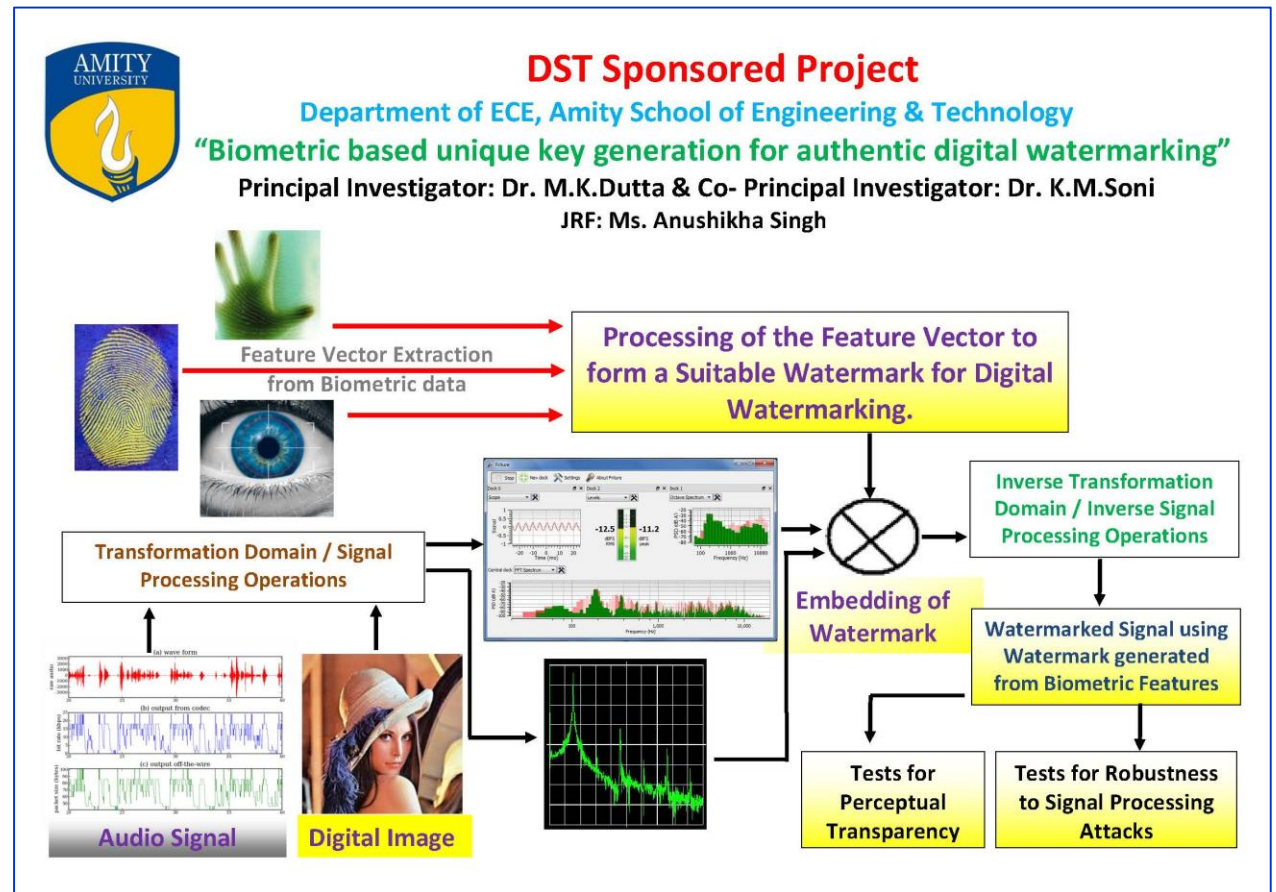


The results under the signal processing attacks of Gaussian LPF attack, JPEG compression attack and Gaussian noise attack is also presented and in these cases also the highest peak is followed by a very low value and hence **unique identification** is done.

These peaks in the NC curves clearly map the biometric templates in the database.

Acknowledgement

This work is supported in part by the Grants from
Department of Science and Technology, No.
DST/TSG/NTS/2011/173”, Government of India



**Thank you for your
attention, Any
Questions Please !!!!!**

