CDMA, Wireless And Watermarking

Oscar Moreno
Gauss Research Laboratory
&
Andrew Tirkel
Scientific Technology

ICANN 43 San Jose, Costa Rica
Tech Day
12 /March /2012

WATERMARKS

Visible

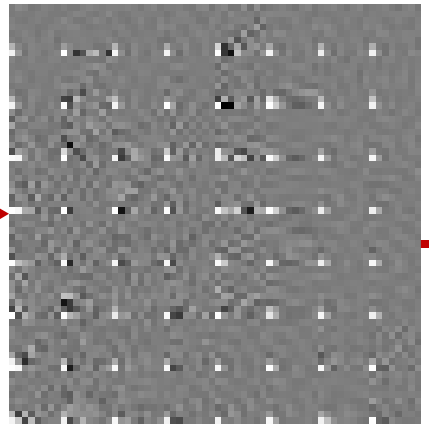
Invisible

WATERMARKING APPLICATIONS

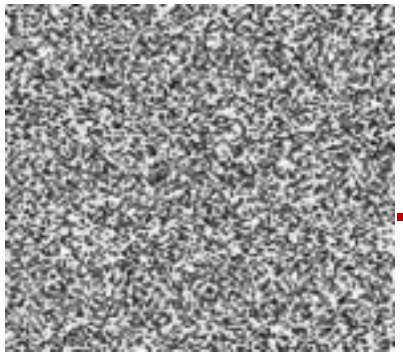
- **Content identification and management**
- **Content protection for audio and video content**
- **Forensics and piracy deterrence**
- **Content filtering (includes blocking and triggering of actions)**
- **Communication of ownership and copyrights**
- **Document and image security**
- **Authentication of content and objects**
- **Broadcast monitoring**
- **Locating content online**
- **Rich media enhancement for mobile phones**
- **Audience measurement**
- **Fingerprinting/Audit Trail/Traitor Tracing**

WATERMARK EMBEDDING

DATA FILE = IMAGE



TRANSFORMED IMAGE



WATERMARK
(CONTAINS HIDDEN DATA)
MODIFIED BY HVS

INVERSE TRANSFORM

WATERMARKED IMAGE

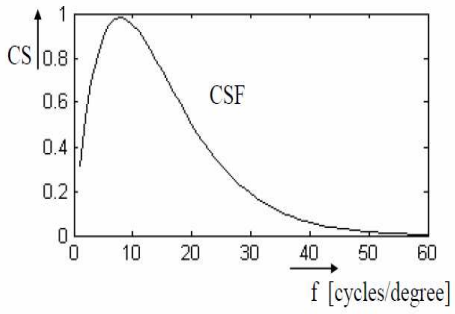


Fig. 1. Contrast Sensitivity Function.

Human Visual System Models in Digital Image Watermarking

WATERMARK EXTRACTION

WATERMARKED IMAGE

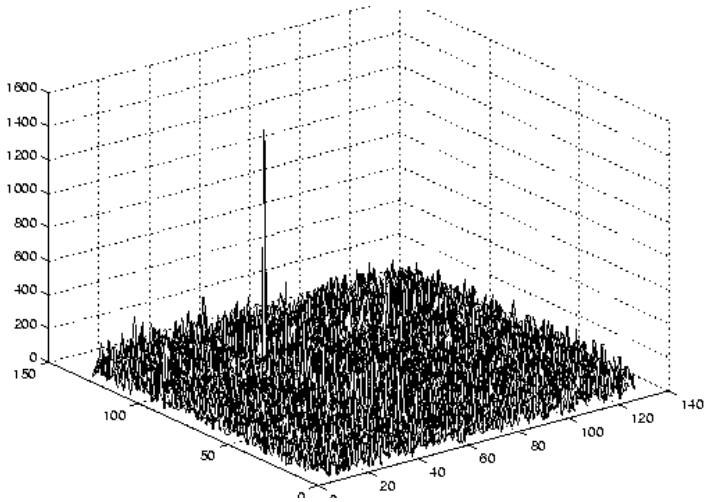
TRANSFORM

CYCLIC SHIFT

WATERMARK

CORRELATOR

DECODE DATA



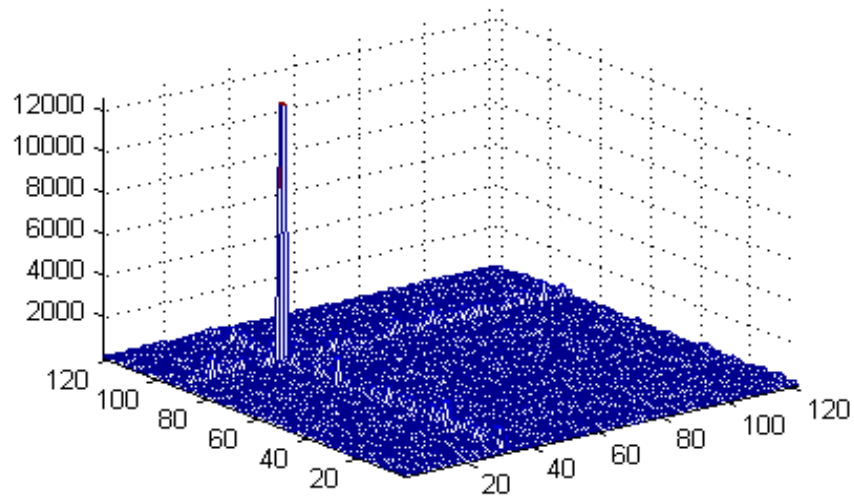
2D CORRELATION

An Example

D

128x128 JPEG

D_w



WATERMARK DETECTION USING CORRELATION

WATERMARK WAS APPLIED WITH ENOUGH POWER TO MAKE IT JUST VISIBLE

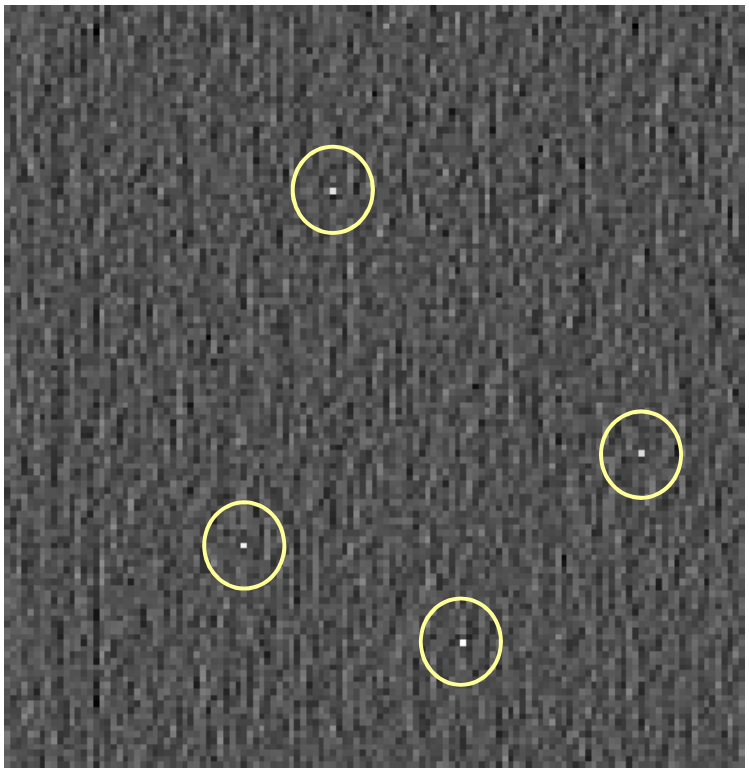
HIGH CAPACITY WATERMARKS

Original 127x127x8 bit

127x127 binary watermarks added in spatial domain

OUR ARRAYS HAVE LOW CROSS-CORRELATION. HERE, 4 ARRAYS ARE EMBEDDED IN AND EXTRACTED FROM THE SAME IMAGE.

THIS INCREASES DATA CAPACITY 4 TIMES!!!

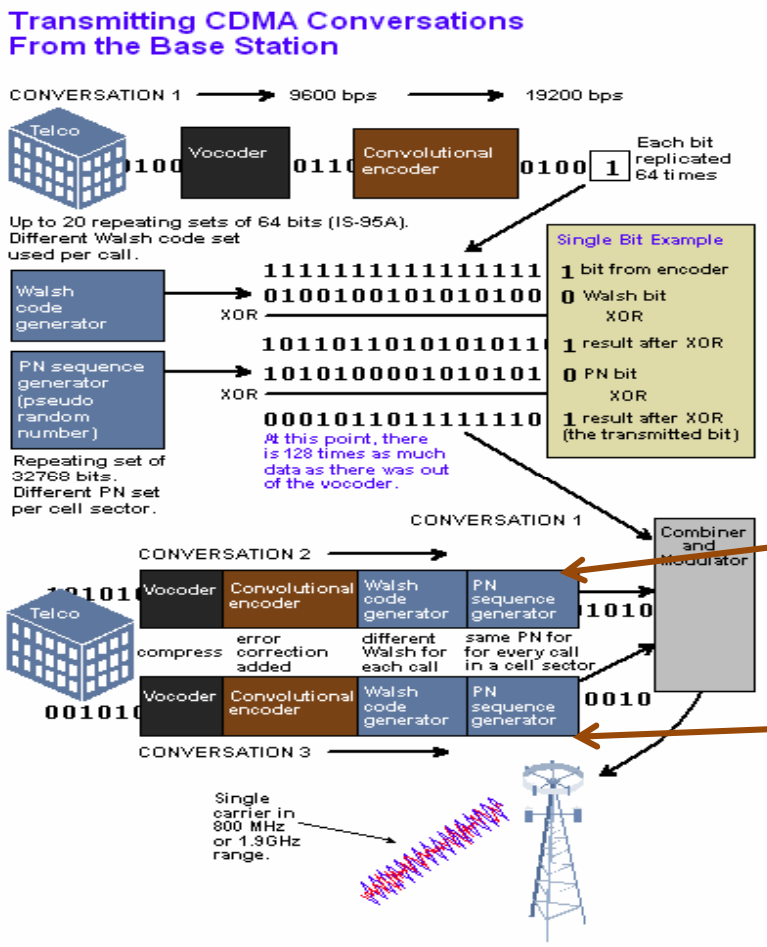


Filtered Correlation Output showing the location of 4 peaks for *m* = 1

A UNIQUE WATERMARK FOR EVERY IMAGE?

- OUR ARRAYS ARE GENERATED ALGEBRAICALLY AND ARE ALL DISTINCT
- WE CAN GENERATE AT LEAST ONE ARRAY FOR EVERY IMAGE WHICH CURENTLY EXISTS
- SUCH ARRAYS CAN BE EMBEDDED USING A SIMM CARD OR AN FPGA IN THE CAMERA
- WATERMARKS CREATED BY RANDOM NUMBER CANNOT GUARANTEE UNIQUENESS

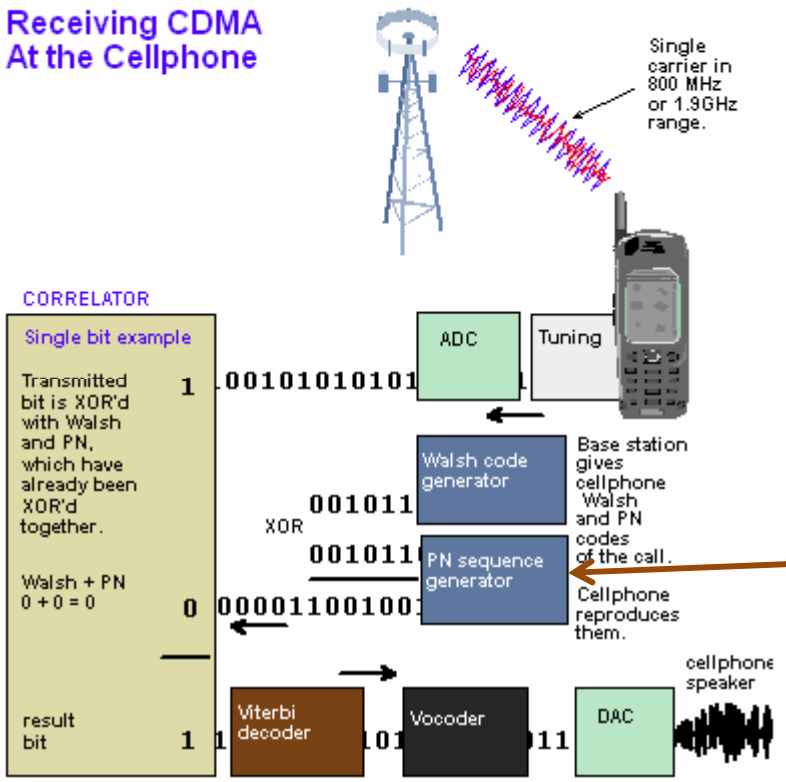
CDMA TRANSMITTER



A KEY COMPONENT OF CDMA IS THE PN SEQUENCE GENERATOR:

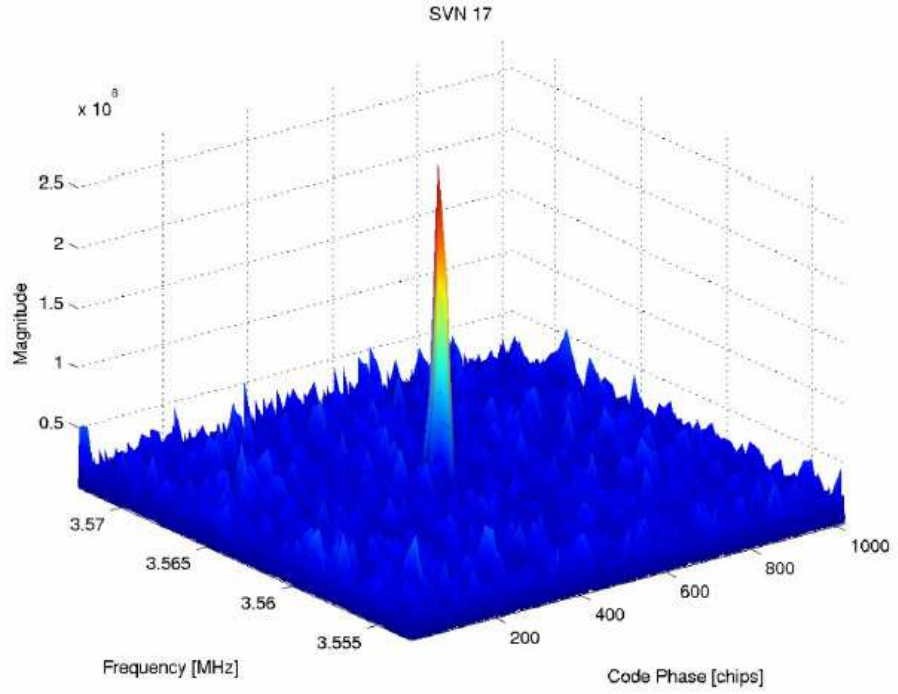
OUR SEQUENCES ARE MORE SECURE, AND BALANCED THAN CONVENTIONAL ONES

CDMA RECEIVER



THE PROCESS OF EMBEDDING AND EXTRACTION OF A PN SEQUENCE IS A ONE DIMENSIONAL VERSION OF OUR WATERMARK EMBEDDING AND EXTRACTION SCHEME

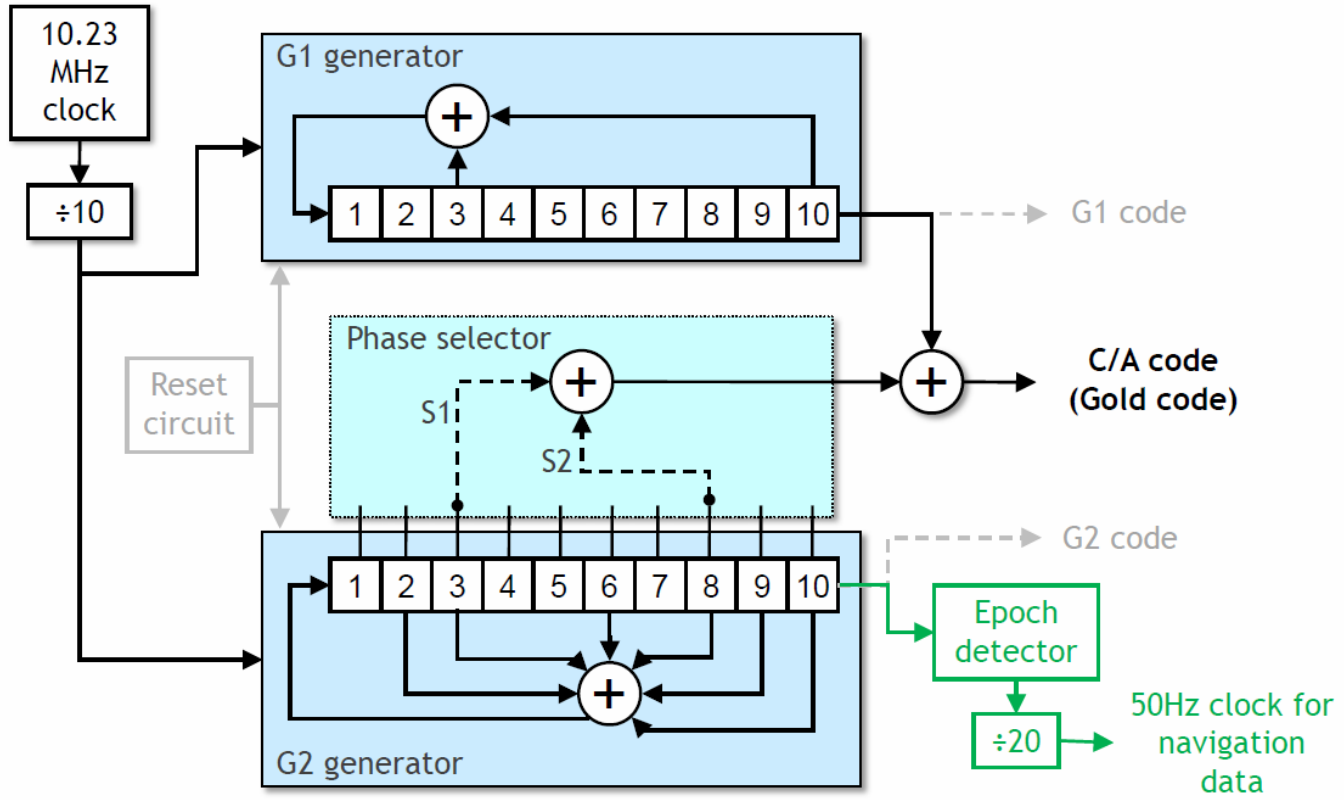
GPS PRINCIPLE



CORRELATION PEAK BETWEEN CODE PHASE AND CARRIER FREQUECY YIELDS TIME AND POSITION INFORMATION FROM THE RECEIVED GNSS SIGNAL

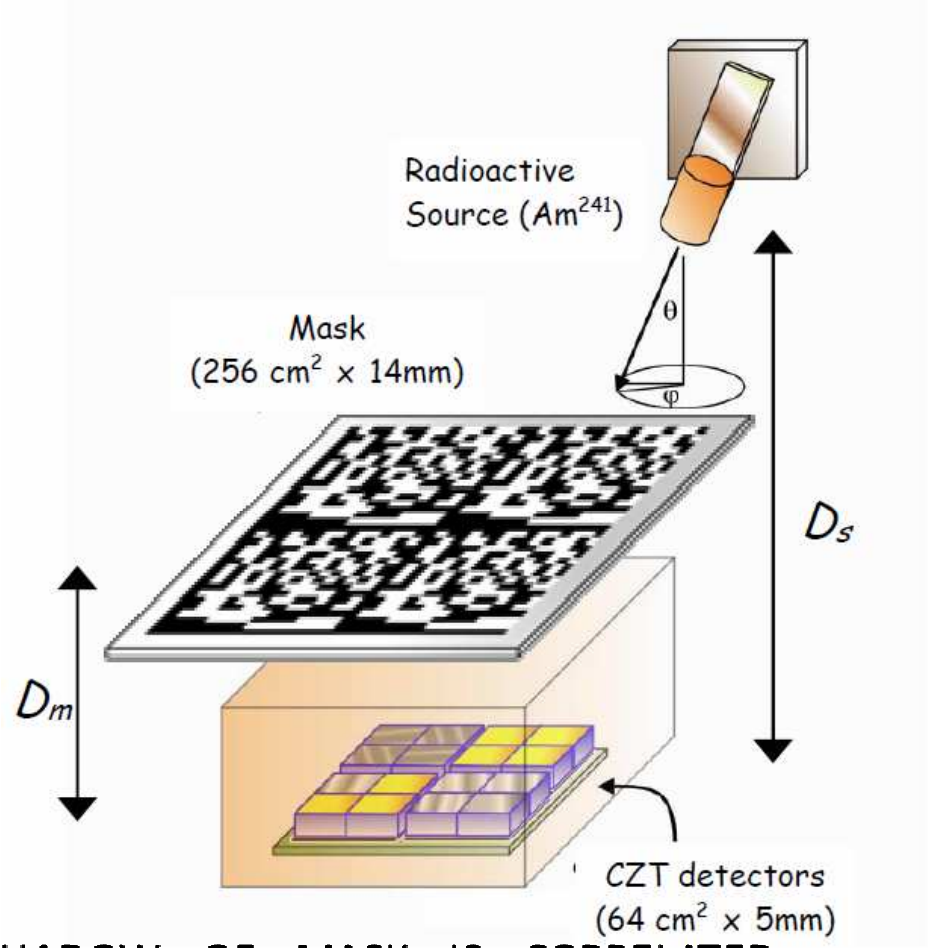
GPS SHORT CODE

The C/A (COARSE ACQUISITION) code is a 1,023 bit GOLD CODE which, when transmitted at 1.023 Megabits per second, repeats every millisecond.

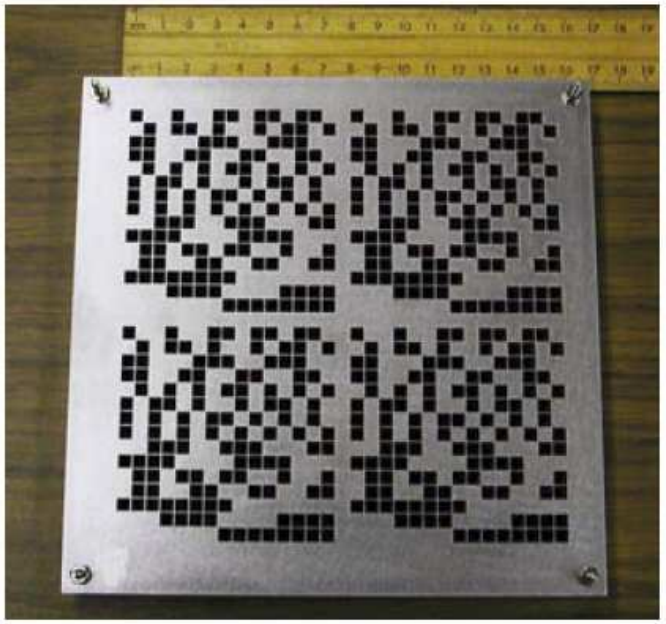


OUR CONSTRUCTION PRODUCES NEW AND SUPERIOR SEQUENCES

CODED APERTURE IMAGING



SHADOW OF MASK IS CORRELATED WITH APERTURE PATTERN. DISPLACEMENT OF AUTOCORRELATION PEAK DETERMINES θ AND φ



METAL MASK

OUR PATENTED TWO-DIMENSIONAL LEGENDRE ARRAY CAN BE USED TO CONSTRUCT CODED APERTURE MASKS THAT ENABLE IMAGING OF X RAYS AND GAMMA RAYS, WHERE NO LENSES EXIST

WATERMARK CONSTRUCTION

- CONVENTIONAL

USE A DIGITAL OR ANALOG RANDOM NUMBER GENERATOR

SIMPLE, BUT **CANNOT** GUARANTEE UNAMBIGUOUS DETECT

- OUR METHOD

USE A FAMILY OF ARRAYS WITH GOOD AUTO AND CROSS-CORRELATION

REQUIRES FINITE FIELD THEORY, AND **CAN** GUARANTEE UNAMBIGUOUS DETECT

ARRAY FAMILIES FOR FINGERPRINTING

- Large array size

So that correlation peak is larger than cross-correlation with image

- Large peak auto-correlation

So that correlation peak is largest at the correct cyclic shift

- Low off-peak auto-correlation

So that correlation values for other shifts are smaller

- Low cross-correlation

So that it is not possible to confuse one fingerprint with another

- Large family size

So that a large number of recipients can be accommodated

- Balance

So that watermarked image has the same mean value as the original so watermark is imperceptible

NOTE: WE USE MULTI-PERIODIC CORRELATIONS

CONSTRUCTION METHOD

WE USE A COMPOSITION OF TWO SEQUENCES/ARRAYS

1. A MULTI-PERIODIC SHIFT SEQUENCE/ARRAY

2. A COMMENSURATE MULTI-PERIODIC COLUMN SEQUENCE/ARRAY

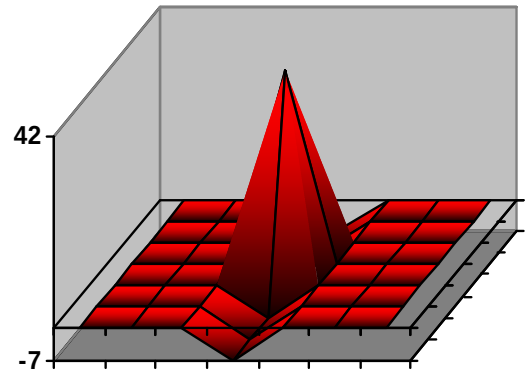
BOTH ARE OBTAINED FROM FINITE FIELDS

CONSTRUCTION OF ARRAY FAMILY

Shift Sequence

LEGENDRE →

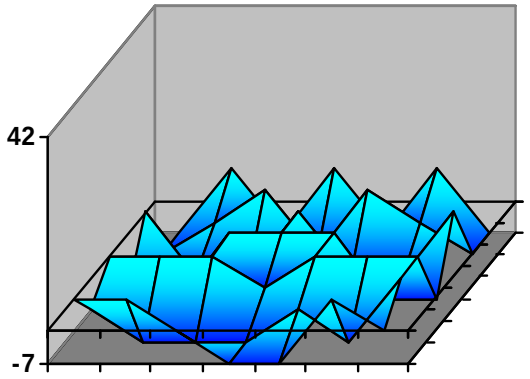
0	6	4	1	4	6	0
0	1	-1	-1	-1	1	0
1	1	1	0	1	1	1
1	-1	-1	1	-1	-1	1
-1	1	-1	1	-1	1	-1
1	-1	0	-1	0	-1	1
-1	-1	1	1	1	-1	-1
-1	0	1	-1	1	0	-1



Autocorrelation 7×7 Array

Another Array

0	5	1	2	1	5	0
0	1	-1	-1	-1	1	0
1	-1	0	-1	0	-1	1
1	1	1	0	1	1	1
-1	-1	1	1	1	-1	-1
1	-1	-1	1	-1	-1	1
-1	0	1	-1	1	0	-1
-1	1	-1	1	-1	1	-1



Cross-correlation 7×7 Arrays

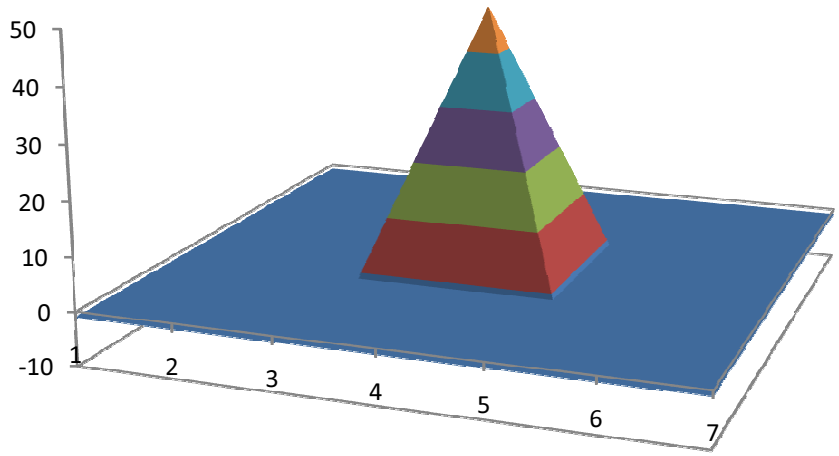
6 such arrays with quadratic shift sequence have the auto and cross-correlation properties as above

MULTI-DIMENSIONAL LEGENDRE ARRAY

b

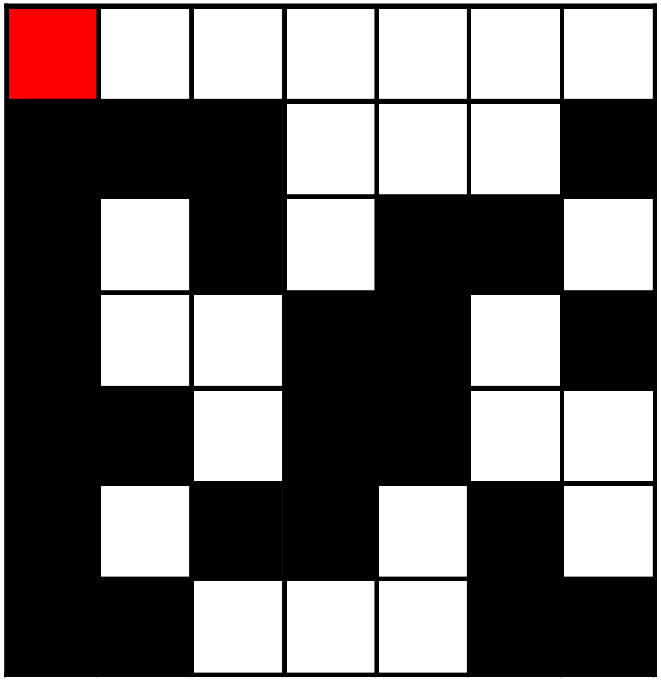
	0	1	2	3	4	5	6
0	*	0	16	8	32	40	24
1	1	31	11	26	12	14	5
2	17	28	47	30	27	21	42
3	9	22	34	39	13	20	19
4	33	43	44	37	15	10	46
5	41	18	45	3	6	23	4
6	25	29	38	36	2	35	7

$$\alpha^i = b\alpha + c \in GF(p^2)$$



Autocorrelation

c



$$c_i = (-1)^{i \bmod 2}$$

2D LOG QUADRATIC CONSTRUCTION

SHIFT SEQUENCE

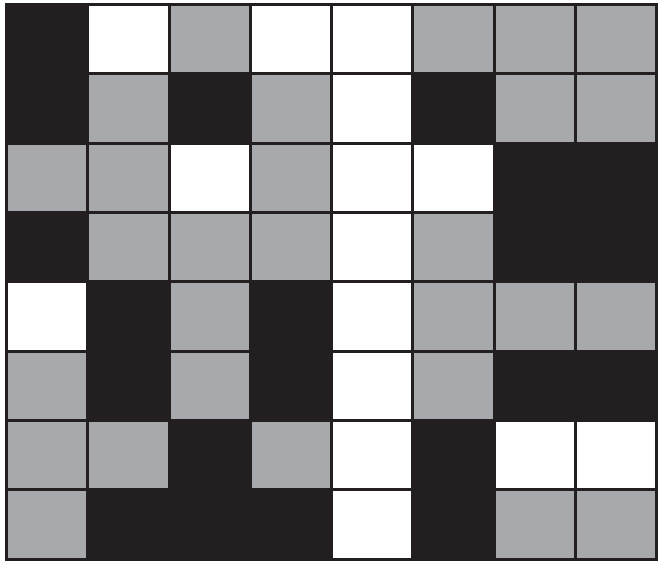
$$s_j = log_\alpha(A\alpha^{2j} + B\alpha^j + C)$$

S_0	S_1	S_2	S_3	S_4	S_5	S_6	S_7
	■		■				
		■			■		
■							
						■	■

Approximately p quadratics leading to distinct arrays

COLUMN

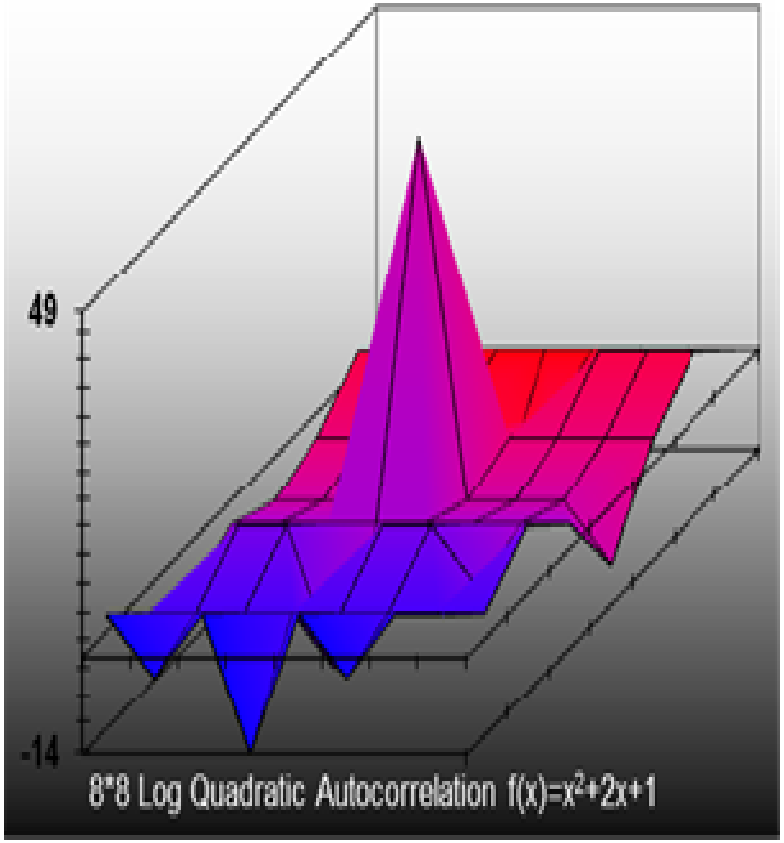
ARRAY

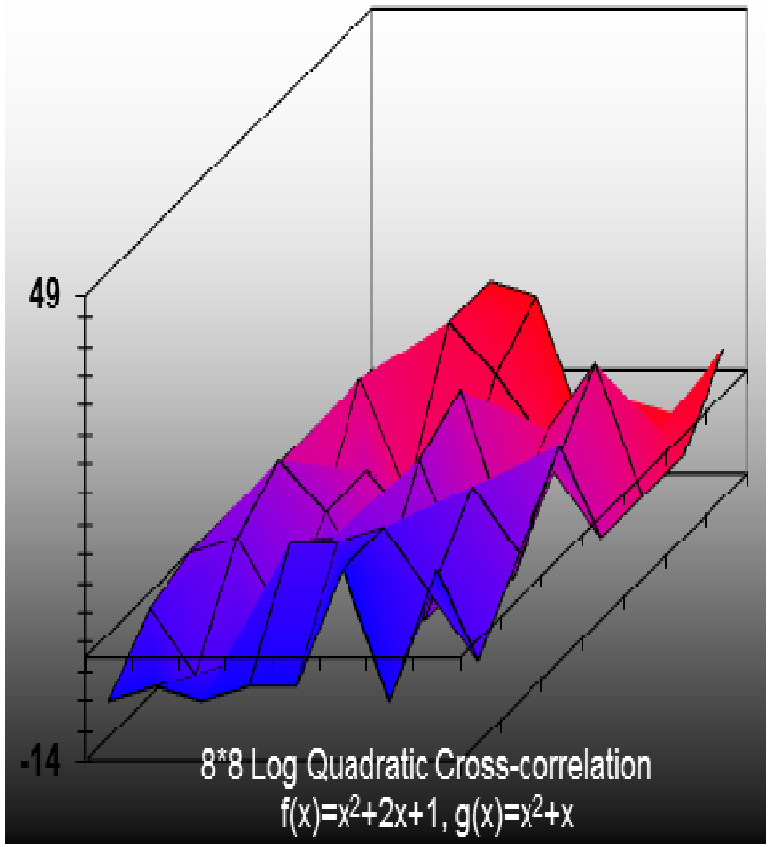


$$c_i = (-1)^{[log_\alpha(\alpha^i - 1)] \bmod 2}$$

SIDELNIKOV

CORRELATION



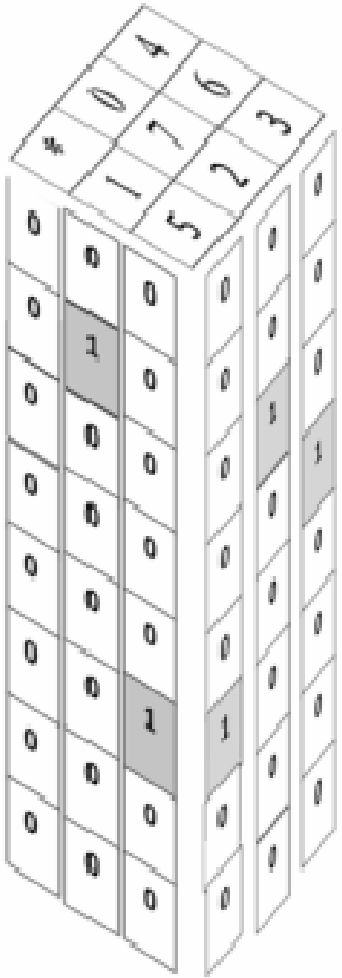


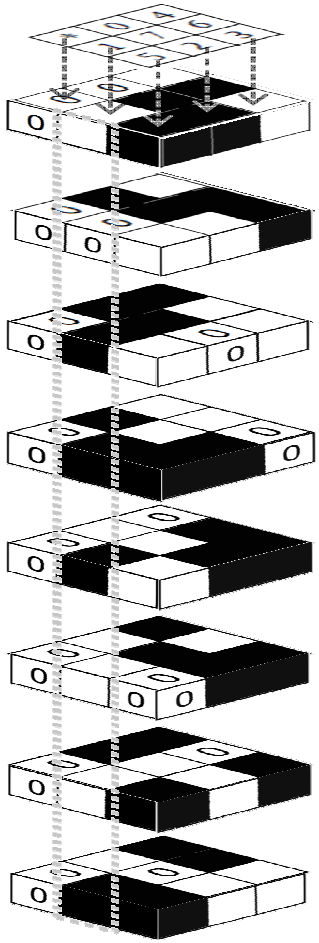
3D LOG QUADRATIC CONSTRUCTION

GF(3^2)

*	α^0	α^4
α^1	α^7	α^6
α^5	α^2	α^3

*	0	4
1	7	6
5	2	3

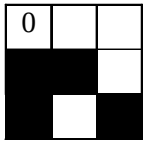


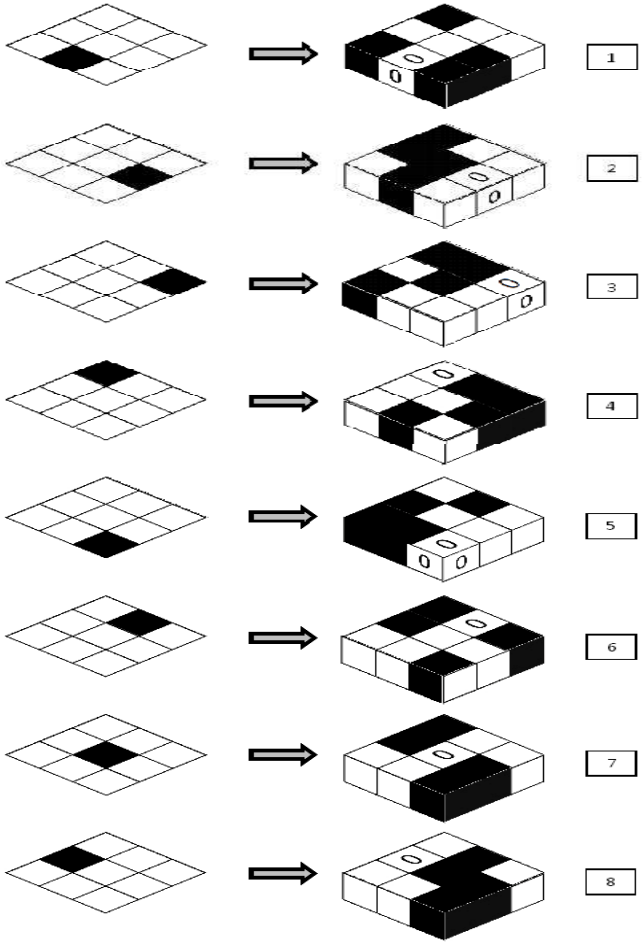


3D EXPONENTIAL QUADRATIC CONSTRUCTION

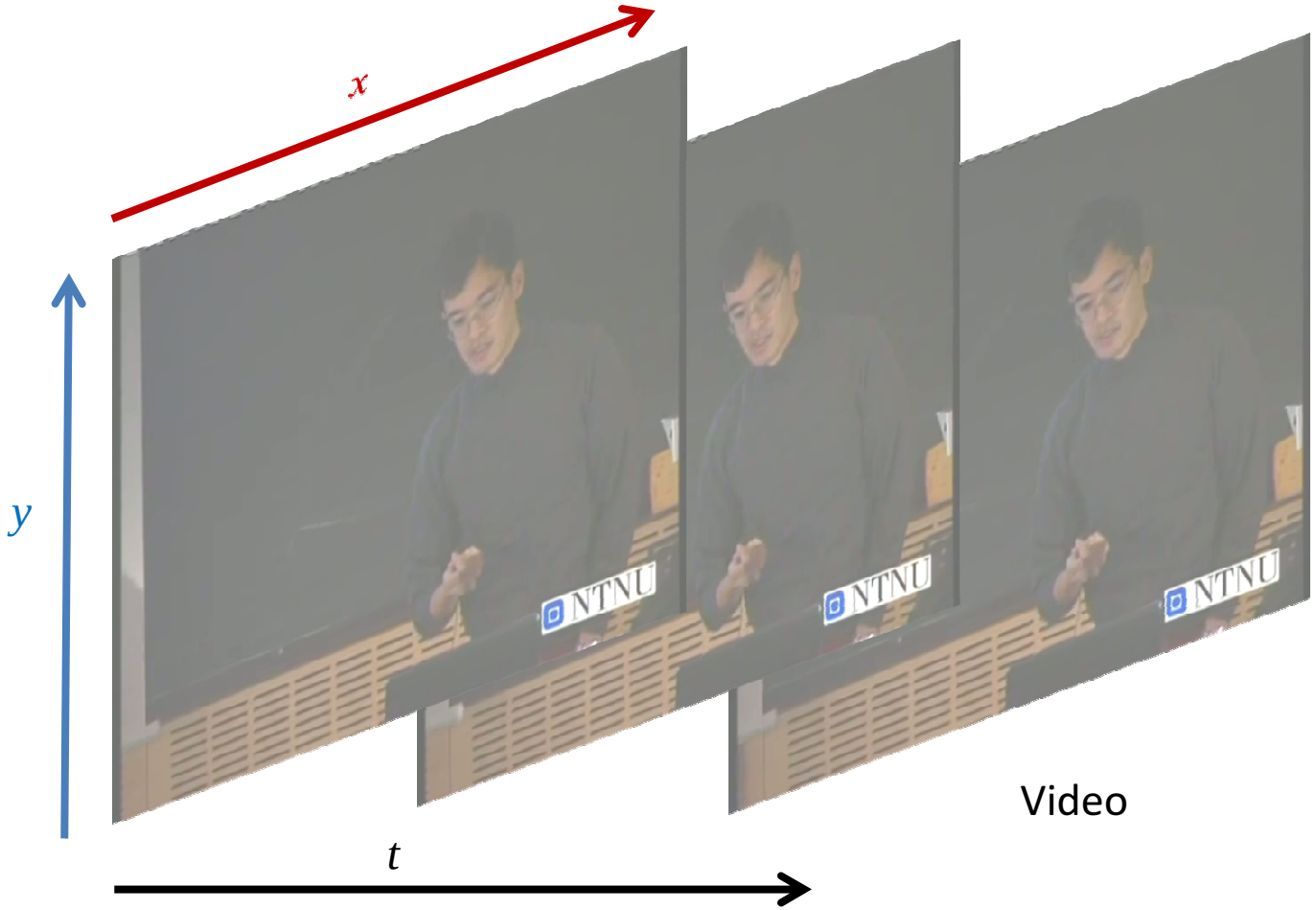
*	α^8	α^4
α^1	α^7	α^6
α^5	α^2	α^3

1	**(1,0)**
2	**(2,1)**
3	**(2,2)**
4	**(0,2)**
5	**(2,0)**
6	**(1,2)**
7	**(1,1)**
8	**(0,1)**

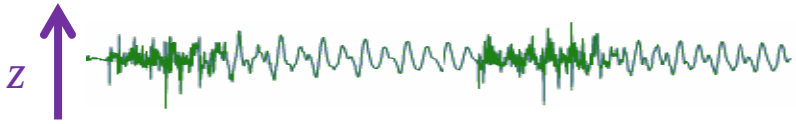




MULTI-DIMENSIONAL MULTIMEDIA



Video



Audio (up to 14 channels)

Project 1 – Audio Recording

Emergency

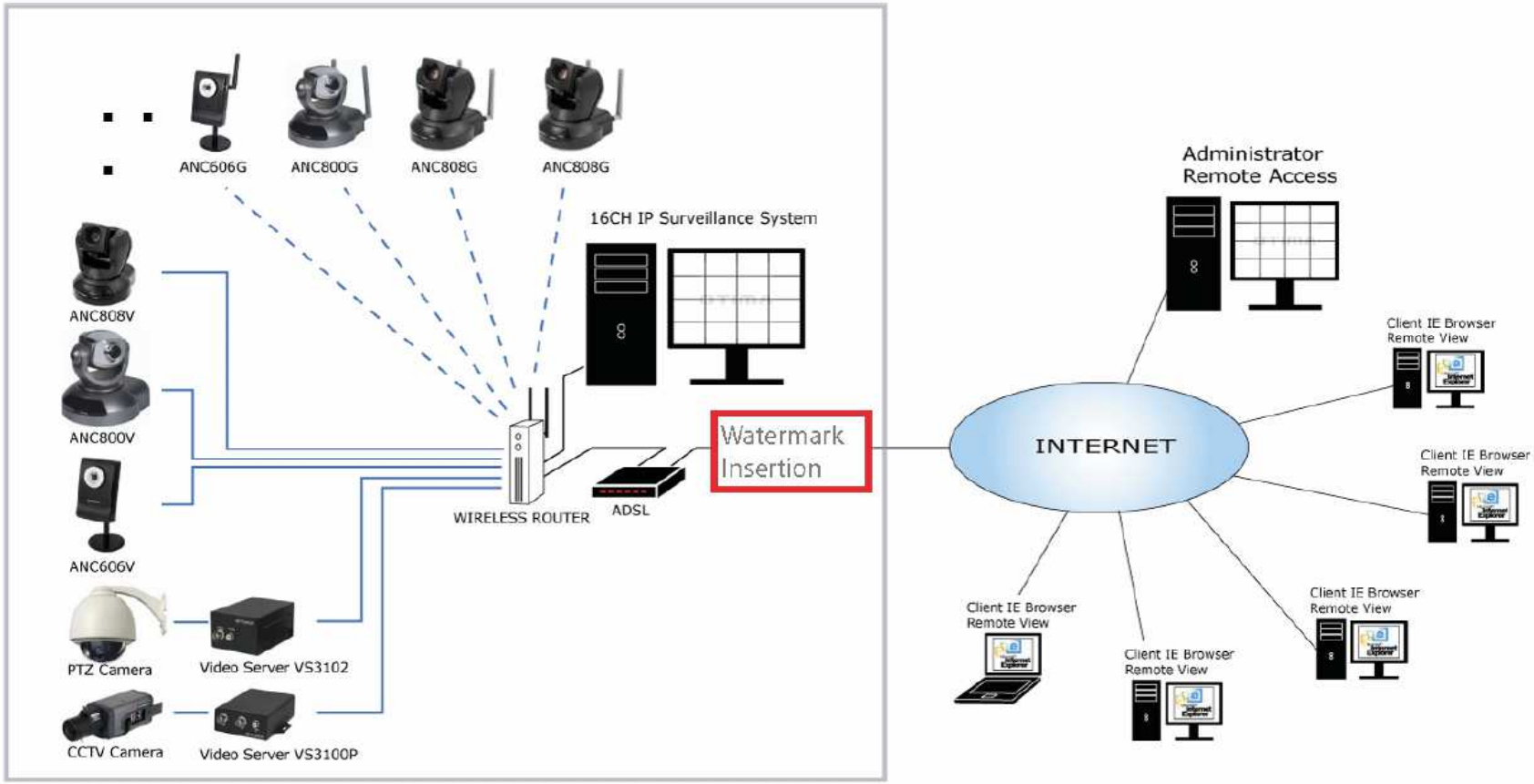
Hospital

Watermark

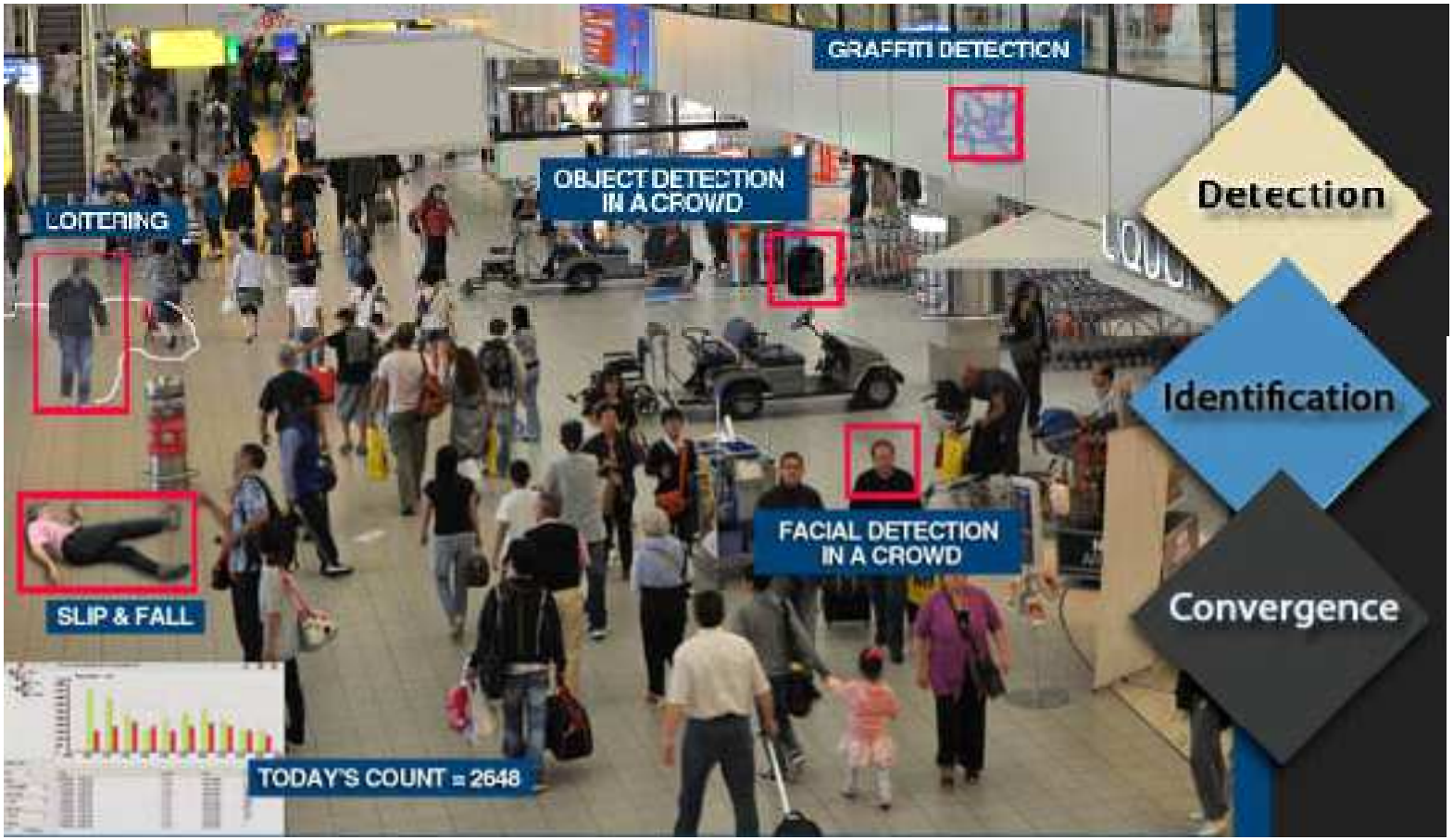
Recording Device

Emergency Call + Watermark

Project 2 - Video Surveillance

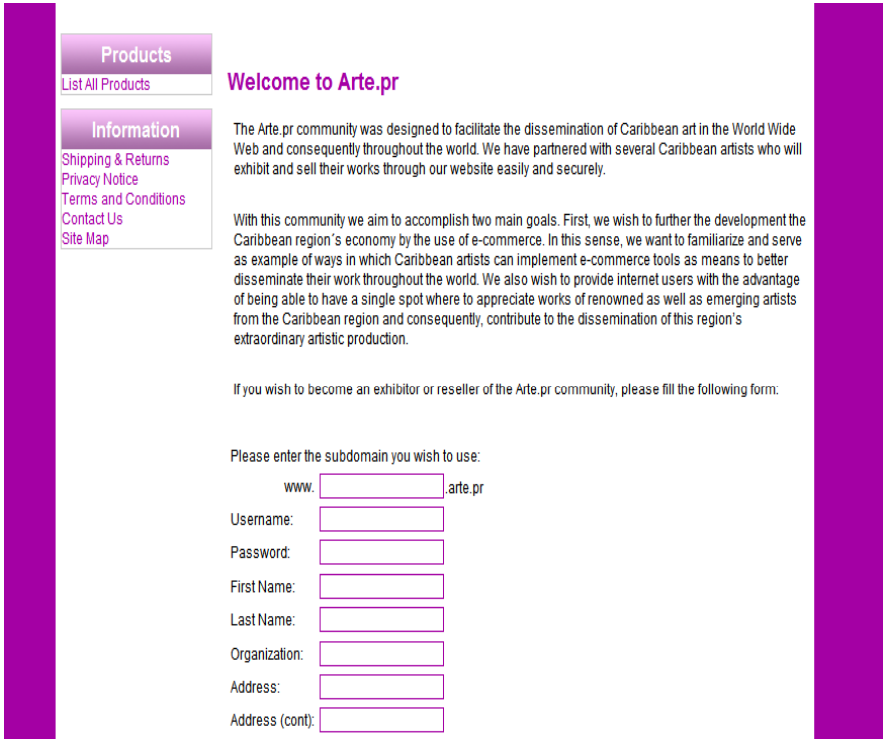


Project 2


GRAFFITI DETECTION
OBJECT DETECTION IN A CROWD
LOITERING
Detection
Identification
FACIAL DETECTION IN A CROWD
Convergence
SLIP & FALL
TODAY'S COUNT = 2648

E-Commerce Communities

- Arte.pr community was designed to facilitate the sale of Caribbean art on the internet. We have partnered with several Caribbean artists who exhibit and sell their works through our website easily and safely.



PUERTO RICO
Top Level Domain

User Communities

- We have given the task of designing a user community for the users of .PR, the purpose of the community is seeking to establish a channel with strong links between domain users of the .PR and domain administration, in order to better serve the community and achieve higher levels of excellence.

PUERTO RICO
Top Level Domain