



Statutory Meetings and 9th Ministerial Strategic Seminar

5-9 December, 2011

**Security for Digital Watermarking, Finger
Printing and Wireless**

Dr. Oscar Moreno



GAUSS RESEARCH LABORATORY, INC.



GAUSS RESEARCH FOUNDATION, INC.



Digital watermarking

- Also referred to as simply watermarking, is a pattern of bits inserted into a digital image, audio or video file that identifies the file's copyright information (author, rights, etc.).
- The name comes from the faintly visible watermarks imprinted on stationery that identify the manufacturer of the stationery.

The Purpose of digital watermarks

- The purpose of digital watermarks is to provide copyright protection for intellectual property that's in digital format. Unlike printed watermarks, which are intended to be somewhat visible, digital watermarks are designed to be completely invisible, or in the case of audio clips, inaudible.

New Construction

- Such arrays are highly useful in the field of digital watermarking, and digital fingerprinting of multi-dimensional data, such as audio and video, and in other information security applications. We have filed a provisional patent application for watermarks built using our construction, and have published the work at international conferences and in journals.

Novelty

- Our arrays are the only ones that provide:
 1. Fingerprinting
 2. That are applicable for video and audio, or an integration of both.

Application

- Fingerprinting for government documents. In other words if you had our watermarks in the documents of the wikileaks scandal we would have been able to trace the source of the leak and apprehend the guilty person

Wireless Security

Our contribution is for the area of spread spectrum which started in the second world war and is been widely used by the military. It is more secure by taking the transmission sequence and spreading it, making it appear as random and therefore hard to jamm it or hack it.

-
- There are 3 kinds of direct sequence spread spectrum:
 1. FDMA that requires FCC approval and is not used for cell phones.
 2. TDMA that shares the time among users and CDMA that divides codes.
 3. CDMA is the technique patented by QUALCOMM and is made this company into a multibillion dollars company.

2. and 3. are presently still used

A new kind of CDMA

- In the present research we use the following discoveries of Tirkel-Moreno:
 1. Substitution of a balanced and high complexity sequence into a family of frequency hopp codes produce secure sequences for the applications (cryptography, wireless, watermarks).

A new kind of CDMA

2. Found frequency hopp codes with optimal cross correlation for as large number of users as needed, this was obtained for arbitrary number of dimensions also.
3. Combining 1. And 2. we obtain families of watermarks very secure for use as fingerprints for multimedia applications.
4. Also 1. And 2. can be obtained to give very secure wireless CDMA systems. This is a breakthrough in the wireless area.

Type	Length	Efficiency %	Normalized Correlation Bound	Balanced Family Size	Total Family Size	Normalized Complexity
Gold	31	100	0.29	17	33	0.32
Moreno Tirkel 2 (p=7)	42	100	0.238	0	48	0.453
Moreno Tirkel 2B (p=7)	42	85.7	0.222	48	48	>0.5
Moreno Tirkel 2R (p=7)	56	100	0.143	48	48	0.768
Gold	63	100	0.27	33	65	0.19
Moreno Tirkel 2 (p=11)	110	100	0.127	0	120	~0.255
Moreno Tirkel 2B (p=11)	110	81.8	0.156	120	120	>0.5
Gold	127	100	0.13	65	129	0.11
Moreno Tirkel 2R (p=11)	132	100	0.091	120	120	>0.5
Moreno Tirkel 2 (p=13)	156	92.3	0.097	168	168	>0.5
Moreno Tirkel 2R (p=13)	182	85.7	0.095	168	168	>0.5
Small Kasami	255	100	0.067	0	16	0.047
Large Kasami	255	100	0.129	0	4111	0.062
Moreno Tirkel 2 (p=17)	272	94.1	0.07	288	288	>0.5
Moreno Tirkel 2R (p=17)	306	88.9	0.063	288	288	>0.5
Moreno Tirkel 2 (p=19)	342	100	0.064	0	360	>0.5
Moreno Tirkel 2B (p=19)	342	89.5	0.072	360	360	>0.5
Moreno Tirkel 2R (p=19)	380	100	0.053	360	360	>0.5
Moreno Tirkel 3R (p=19)	380	100	0.105	6858	6858	>0.5*

Summary

The great complexity and the balance means that our research is ideally suited for great security which is the main research problem for present day wireless. Therefore ours might be the big breakthrough in the wireless area.