Techniques in Art of Electronic Espionage in the ESM

*Dr. Ch. Raja

** Associate Professor, Department of Electronics and Communications Engineering, MGIT, Hyderabad.*

Abstract **-** So far we have seen various signal acquisition and processing and EOB preparation techniques in the light of Electronic Support Measures (ESM). In this paper, we shall briefly review some of the hardware support used in the case of present day electronic espionage. Moreover, we shall indicate then and there various problems faced in using exclusively digital equipment for ESM purposes and suggest a feasible and reliable method of using both analog and digital equipment for overcoming such problems.

Keywords *- EOB, ESM NCW, SDR.*

I. DIGITAL RADAR RECEIVERS

Using exclusively digital equipment especially in aircrafts may cause problems like instability and sudden failures. Alternatively, one can use the latest state of the art analog processing and digital conversion technology available in the market to provide high-dynamic range, wide-bandwidth front-ends and digitizers for receivers with 14 bit resolution and 80 MHz sampling rate. Figure 4.1 shows a digital receiver meant for ELINT operation.

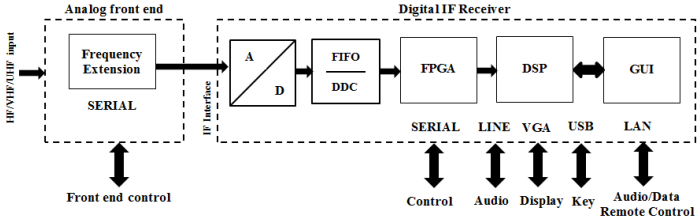

Figure 1: A digital receiver meant for ELINT operations

All digital signal paths are generally designed for 16 bit sample handling. The front-end of the receiver transforms the interested frequency sub-band to the IF with maximum bandwidth, which is equal with real-time instantaneous bandwidth of the receiver. This full-band signal can be used for fast scanning, parallel processing algorithm for finding signal components in the spectrum. But it is possible to use limiting the frequency range in the digital domain too to achieve higher frequency resolution or more accurate bandwidth estimation.

One can use a PC backbone to monitor and control the ELINT operation with the help of the digital receiver. Figure 2 shows a PC based backbone which could be used with a digital receiver. This technique more or less comes under what is known as '**Software Defined Radio' (SDR)**. Such an ELINT receiver with a PC backbone would lead to a reliable network centric warfare (NCW) system. The search intercept receiver could be further enhanced with record and replays of raw data, support libraries with predefined scanning tasks for random and systematic frequency list and provide statistical database of the results.

The results of the task are presented in the form of result log records for further processing by external command and control posts. Each log record contains the basic parameters of the emission. Basically the main parameter of the record is the carrier frequency of the signal. The record contains a sub record of signal timing which shows the signal activity by recording the time of signal emission using the GPS synchronized time stamp.

The result log can be used for further higher-level analysis. The search intercept receiver should also be able to process the angle of arrival (AOA) for all of the incoming signal components in the spectrum to provide bearing spectrum.

The signal processing could be carried out using appropriate high speed algorithms and signal parameters could be estimated.

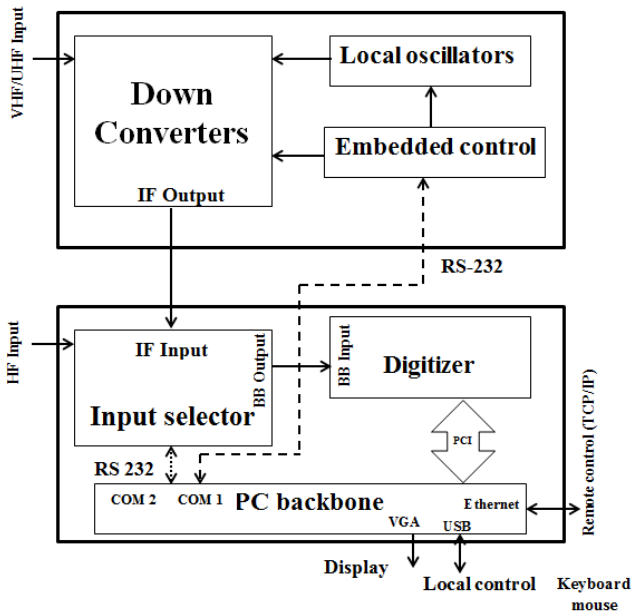

Figure 2: PC based backbone

II. DIGITAL DIRECTION FINDING SYSTEM

Direction finding system is utilized in radar, in sonar in order to find the Direction Of Arrival (DOA) of signal of interest for the purpose of positioning the emitters. Conventional direction finding system employs multi-antenna elements or by single

switched antenna followed by digital or analogue receivers and a digital signal processing block. Figure 3 shows a multi antenna direction finding system.

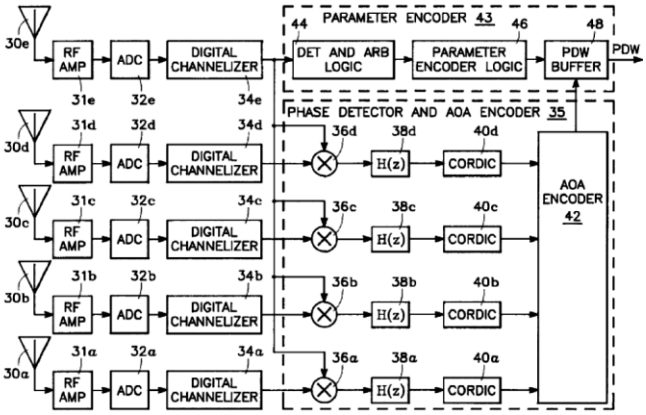

Figure 3: Multi antenna direction finding system

We propose in this thesis, a robust single channel direction finding system devoted to radar or sonar. The proposed solution is based on a switched antenna associated to a special all digital receiver architecture that allows us to digitalize directly RF signals with low sampling frequency. The proposed system takes advantages of single antenna element instead of multiple antenna ones, of all digital receivers in terms of digital signal processing and of low-cost of implementation. The novel architecture could be modeled and simulated for the test of its performance through the DOA estimate of signal of interest by employing a super-resolution algorithm.

III. A CORRELATIVE-VECTOR DF SYSTEM

Figure 4: Watkins Johnson direction finding system

The WJ-8986A shown in figure 4.4 is a low-cost compact Direction Finding (DF) system. With the help of advanced digital signal processing techniques with a state-of-the-art hardware, WJ has brought out a DF system with superior performance. The synthesizer provides a fast tuning rate. The parallel A/D Converters digitize signals. This combination ensures high probability of intercept and accurate lines of bearing (LOBs) even for short duration signals. Advanced DSP techniques used along with parallel computation capabilities considerably reduce the time needed for LOB calculations. In addition, graphical data-processing options provide a powerful tool in applications such as resolving co-channel signals and DF of low power signals

All these features allow the WJ-8986A to perform three major communications intercept system functions:

1. High-quality DF
2. Signal acquisition and monitoring
3. RF/IF PAN display using high-resolution spectral FFTs

Features of WJ 8986A

DF, acquisition, display & monitoring capability
High-accuracy antenna versatility
3- to 5-channel simultaneous signal processing
High-processing gain/DF sensitivity
50-MHz/second scan rate (with DF)
Effectiveness against frequency agile and PTT-type signals
DFs on 10-microsecond pulses (mono pulse type design)
Graphical front-panel displays
Single rack-mountable unit with EL display
Full remote control via IEEE-488 interface
PC/AT-based design
HEIGHT 8.75in (22.23cm) DEPTH 20in (50.80cm)
WIDTH 19in (48.26cm) WEIGHT 66lbs (29.86kg)

With all of its performance, the WJ-8986A is a practical, easy-to-use system. The system consists of an 8.75-inches high rack mountable chassis. The front panel of the DF contains a lighted keypad and EL display, as well as jacks for optional key- board and headset. The DF antenna and accompanying cables are the only additional hardware. Options install internally in a modular fashion. Typical system power is less than 250 watts, making it ideal for vehicular and airborne applications.

Operator interface is via the front-panel keypad of the processor or an IEEE-488.2 remote control. An optional keyboard can also perform all DF operations. System output is by a multiple grey-scale, high resolution display located on the front panel. This display provides the operator with system configuration, LOB results, and various graphical displays such as angle of arrival (AOA) versus signal strength and AOA versus frequency. An optional external CRT adds enhanced color graphics.

LOBs are calculated using a correlation algorithm on signals obtained from mono pulse antenna arrays. This technique easily adapts to a wide variety of DF antennas. Dipole antenna arrays primarily provide DF coverage in the VHF/UHF ranges. Other compatible antenna configurations include:

- Crossed-loop antennas for HF ground waves
- Large baseline arrays for HF sky waves
- Annular slot or ferrite loops for covert applications

In general, the WJ-8986A uses arbitrary antenna arrays for DF applications. The WJ-8986A uses graphics data-processing software to enhance its operation. Standard software includes a basic simplified display, plus the displays.

Configuration Flexibility

A variety of options allow system configurations for customer-specific applications, including HF and airborne DF. The standard system consists of:

1) WJ-8986A Correlative-vector DF Processor
   - 2 to 512 MHz DF unit
   - 3 channels
   - Front-panel keypad/IEEE-488 bus
   - EL front-panel display
2) WJ-9886-X 20 to 512 MHz DF Antennas

IV. DIGITAL TUNERS AND WIDEBAND RECEIVERS

Digital Tuner:

(STR-3000 frequency receiver front-end tuner)

Figure 5: STR-3000 digital tuner

Figure 5 shows a 4 channel receiver tuner 20-3000MHz

System Features

Wide frequency coverage 20-3000 MHz
IF bandwidth up to 26 MHz
Tuning step 1MHz
Fast frequency tuning capability
Low phase noise local oscillator
High dynamic range
Multi-drop RS-232 interface

Description of the System

The Sagax SRT-3000 VHF/UHF tuner is a modular building block, which can be used for high-performance surveillance, monitoring receiver applications. The tuner can be used as a stand-alone wide-band front-end for a digital IF software-defined receiver.

The Sagax SRT-3000 VHF/UHF tuner is a modular building block, which can be used for high-performance surveillance, monitoring receiver.

The incoming frequency band down-converted to a standard 70MHz IF output. 21.4MHz or 140MHz IF output frequencies are available as an option. The actual frequency and gain can be controlled trough the multi-drop RS-232 interface with some simple published command. (API) The tuner is housed as 1U height standard 19" unit with external 115/230 VAC power supply**.**

Typical applications

Spectrum monitoring and management systems
Signal intelligence and surveillance systems
Wideband intercepting and monitoring receiver systems

Functional block diagram

The VHF/UHF tuner is based on a well proved high-side first IF architecture used by top grade receivers and measurements devices to provide excellent spectral quality. The triple conversion architecture ensures the usage of lower IF frequencies too. The bandwidth of the modern digital tuners enables to use the standard 21.4MHz/70MHz/140MHz IF frequencies. The choice of used IF frequency depends on the applications. When wide instantaneous bandwidth is required in scanning receiver the 140MHz is available to use the maximum bandwidth, which is available. When narrow bandwidth monitoring reception is required the lower 21.4MHz can be used to implement the bandwidth limitation before the digital filtering to increase the dynamic range. Figure 4.6 shows the block diagram of Sagax SRT-3000 VHF/UHF tuner.

The input (RF) and output (IF) attenuation can be used to dynamically change the amplification in order to move the available instantaneous dynamic range in the desired region. The front-end contains a wide-band pre-filtering for wide-band fast-scanning application or sub-octave, tuned pre-selector for narrow-band monitoring applications.

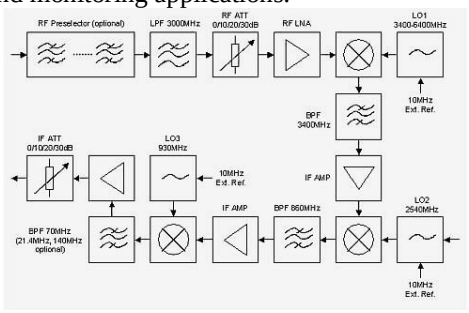

Figure 6: Block diagram of SRT-3000 tuner

All the synthesized local oscillator could be locked to an external 10MHz reference frequency to provide a phase synchronous receiving system. The locking time of the high-speed phased locked loops offer as low as 100us frequency step tuning speed for fast scanning applications. The control of the front-end is implemented as multi-drop asynchronous serial interface, but twisted pair Ethernet based IP connection also could be provided.

V. DIGITAL WIDE-BAND SEARCH AND INTERCEPT RECEIVER

(SRS-3000 PROTUS wide band receiver)

Figure.7 shows a search and intercept receiver system.

Features:

Compact design with graphical user interface
Up to 40MHz wide instantaneous real-time bandwidth
Down to 1ms time resolution
Down to 1 kHz frequency resolution
Quasy real-time frequency spectrum by complex FFT algorithms
Excellent instantaneous dynamic range
High adjacent-channel suppression
Excellent precision and sensitivity
High probability due to wide bandwidth and high-speed scanning
Flexible compatibility for system integration
Raw data recording (option)

Signal pre-classifier (option)
Wide-band DF processing (option)

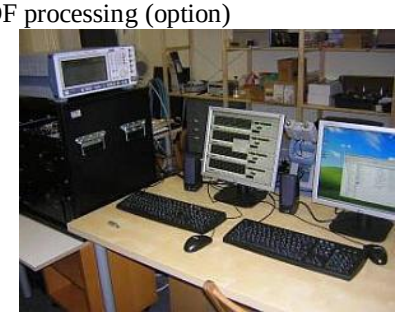

Figure 7: SRS-3000 wide band receiver

Description of the System

The receiver consists of the usual components of digital fast-scanning search intercept receiver:
RF front-end,
HF/IF digitizer,
Digital filtering and
Digital signal processor.

The SRS-3000 is a frequency-agile, lightweight HF, VHF and UHF receiver designed for limited space and high-mobility application for see, ground and air environment. Its compact size, broad tuning range and high-level remote control functionality make it ideal for multitude of system application, including commercial frequency management and military SIGINT COMINT EW missions. The receiver couples high scan speed, high frequency and time resolution, high dynamic range, and excellent selectivity to provide superior performance over many much other receivers. It achieves an outstanding in-band input third-order intercept point of +6 dB, while maintaining a typical noise figure of less than 10 dB. The equipment can be used for high-speed spectrum management, search and intercept missions as a standalone receiver or as a building block of high-grade multifunctional integrated SIGINT COMINT EW systems.

Digital Processing Of Intercepted Radar Signals

ELINT receivers like ALQ218 of Northrop Grumman has built-in facility to process received radar signal and the measured pulse parameters and other details could be directly visualized on the screen or obtained as a hard copy using a printer.

Whatever operations described in chapter 3 could be carried out using such digital receivers and real time radar signal parameter estimation could be achieved with a high degree of reliability during mission flights provided the flight is absolutely free from terrain and weather anomalies. On the other hand, during turbulent weather conditions, digital receivers have been found to be unreliable as per experience gained by Electronic Warfare Officers. In such a case, we propose here to use both analog and digital equipment under mission critical situations so that the mission objective is more or less met with to a great degree of acceptance limits.

4.3.1 Emitter Identification And Intelligence Reports

As detailed elsewhere, emitter identification could be carried out and radar intelligence maps obtained using appropriate image visualization and processing software.We make use of Logical Image Processing System version 3.0software for visualizing and processing digital maps in a PC.

Logical Image Processing System (LIPS) version 3.0

Logical Image Processing System version 3.0 is a collection of a number of image processing tools developed using Visual C++, and it works in Windows environment. The algorithms pertaining to most of the routines in this package have been developed in a novel logico-mathematical framework called **Cellular Logic Array Processing** (CLAP). This nontraditional paradigm advocates pattern-directed **Search And Replace** (SAR) techniques, and so, it guarantees speed and precision [29]. The various menus provided in the software are (i) Home, (ii) File, (iii) Edit, (iv) View, (v) 2D-Images, (vi) 3D-Images, (vii) Grid, (viii) Pattern, (ix) Auxiliary, (x) Tools and (xi) Window. The opening window of the software is shown in figure 8.

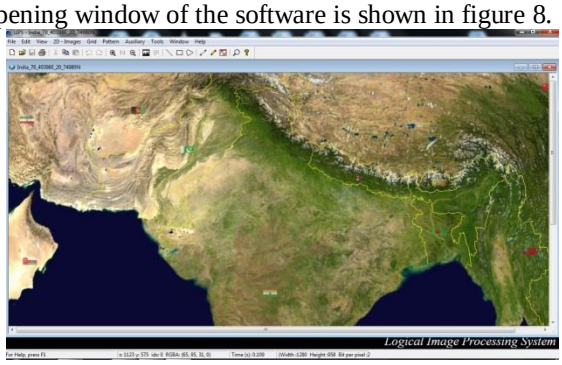

Figure 8: Opening Graphics User Interface of LIPS version 3.0

LIPS version 3.0 is a powerful tool for displaying high resolution images and processing them for obtaining any desired result. In what follows, we present the details of plotting flight paths and obtaining terrain details of selected flight paths and intercepted signal paths.

Remotely sensed imageries from satellites or surveillance aircrafts could be posted on the screen of the computer and mission flight path drawn using operators' log or directly from GPS details.

Mission flight path

Using GPS values of LatLong(latitude and longitude) one can plot flight path using this software. A sample flight path plot is shown in figure 9.

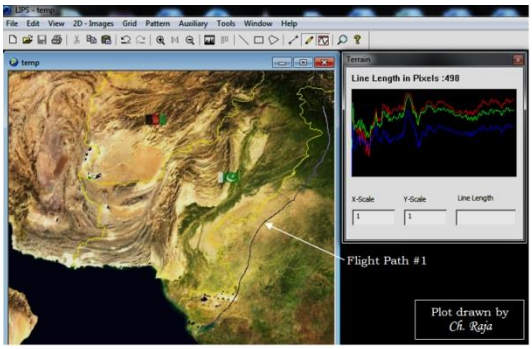

Figure 9: Sample plot of a flight path in the western sector

The digital elevation terrain model along the flight path is also shown in figure 9.

Terrain modeling of signal paths

For a particular flight path, one can obtain the terrain details of intercepted signals on board itself at various aircraft positions.

We have plotted two mission flight paths, one for the western sector and the other for the northern sector, plotted the flight paths and obtained terrain details of chosen signal paths at selected aircraft positions using the tools of LIPS version 3.0. Figures 10 to 21 show another flight path plot in the northern sector and terrain graphs as digital elevation models of selected signal paths in both the sectors. As reported by EWOs of Government of India who had actually undertaken mission flights in the western and northern sector the SNR of intercepted radar signals were found to vary with the terrain. The SNR of the receive signals were weak in hilly regions and considerably good in sea regions. It was found that the sea clutter did not hamper the signal conditions whereas the clutter due to hills introduced noise and anomalous propagation due multiple reflections of the transmitted signals. Though this point is clear in the logical sense, there is no theoretical or empirical justification for this phenomenon. In this thesis, we propose a concept of '***terrain density***' which is a measure of spatial distribution of hills and hillocks in a unit distance. The terrain density is calculated as number of peaks divided by the distance in pixels. This measure is an approximate measure since it is difficult to identify valid peaks from the digital elevation models since calculation of digital elevation itself is approximate.

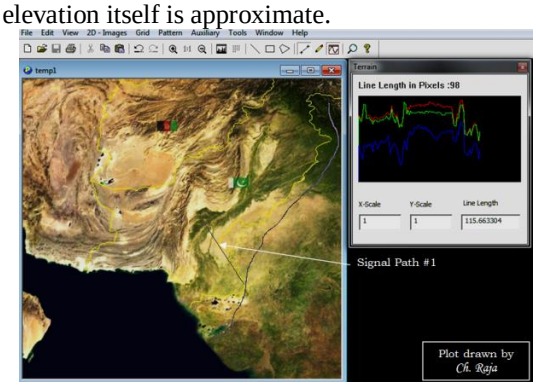

Figure 10: Digital elevation model of signal path #1 of flight path #1

No. of peaks identified = 4
Signal path length in pixels = 98
Terrain density = 4/98 = **0.040**
Average SNR of received signals = 20 dB

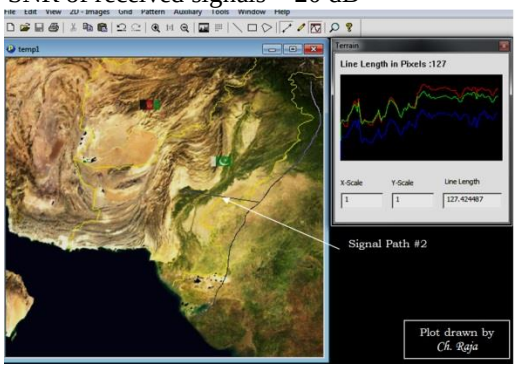

Figure 11: Digital elevation model of signal path #2 of flight path #1

No. of peaks identified = 4
Signal path length in pixels = 127
Terrain density = 4/127 = **0.031**
Average SNR of received signals = 25 dB

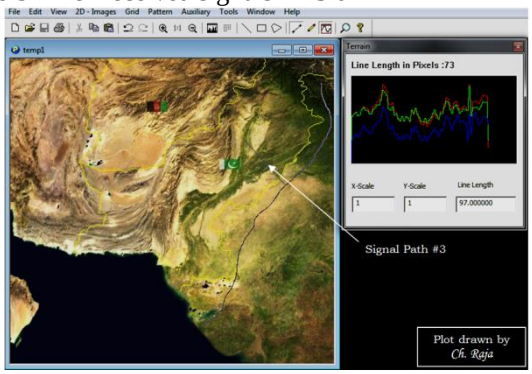

Figure 12: Digital elevation model of signal path #3 of flight path #1

No. of peaks identified = 2
Signal path length in pixels = 73
Terrain density = 2/73 = **0.027**
Average SNR of received signals = 30 dB

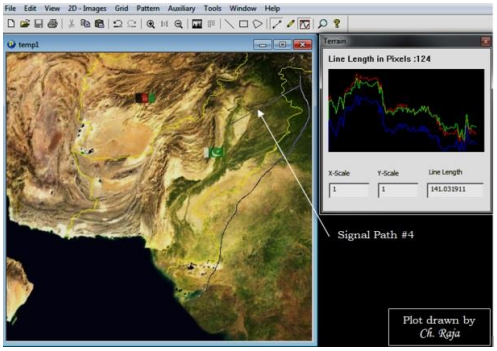

Figure 13: Digital elevation model of signal path #4 of flight path #1

No. of peaks identified = 1
Signal path length in pixels = 124
Terrain density = 1/124 = **0.008**
Average SNR of received signals = 35 dB

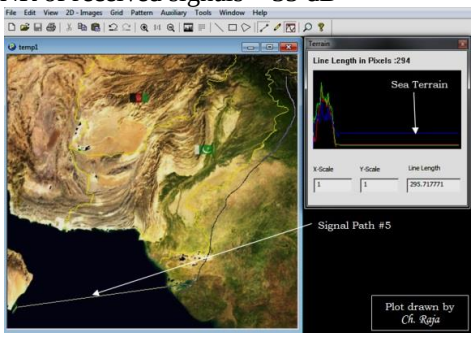

Figure 14: Digital elevation model of signal path #5 of flight path #1

No. of peaks identified = 1
Signal path length in pixels = 294
Terrain density = 1/294 = **0.003**
Average SNR of received signals = 40 dB

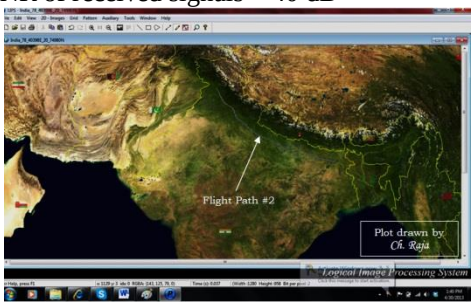

Figure 15: Sample plot of a flight path in the northern sector

Figure 16: Digital elevation model of signal path #1 of flight path #2

No. of peaks identified = 8
Signal path length in pixels = 155
Terrain density = 8/155 = **0.0516**
Average SNR of received signals = 10 dB

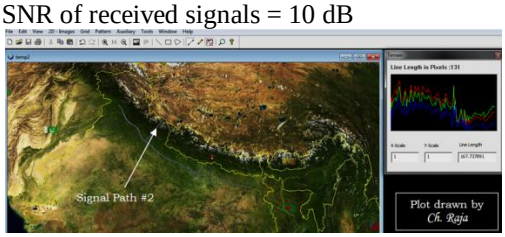

Figure 17: Digital elevation model of signal path #2 of flight path #2

No. of peaks identified = 7
Signal path length in pixels = 131
Terrain density = 7/131 = **0.053**
Average SNR of received signals = 15 dB

Figure 18: Digital elevation model of signal path #3 of flight path #2

No. of peaks identified = 6
Signal path length in pixels = 159
Terrain density = 6/159 = **0.037**
Average SNR of received signals = 30 dB

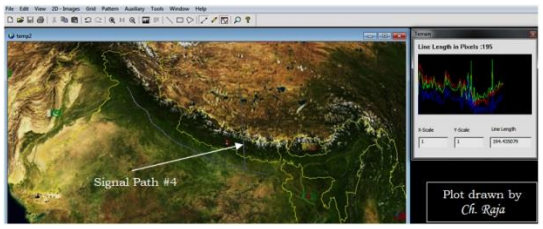

Figure 19: Digital elevation model of signal path #4 of flight path #2

No. of peaks identified = 5
Signal path length in pixels = 195
Terrain density = 5/195 = **0.025**
Average SNR of received signals = 45 dB

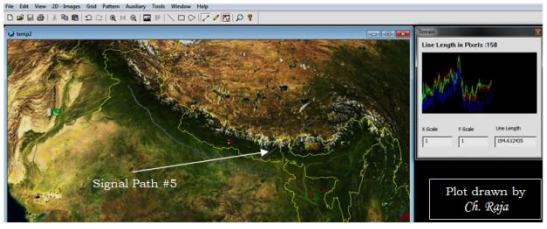

Figure 20: Digital elevation model of signal path #5 of flight path #2

No. of peaks identified = 4
Signal path length in pixels = 158
Terrain density = 4/158 = **0.025**
Average SNR of received signals = 45 dB

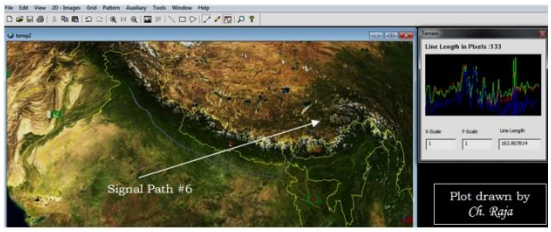

Figure 21: Digital elevation model of signal path #6 of flight path #2

No. of peaks identified = 3
Signal path length in pixels = 133
Terrain density = 3/133 = **0.022**
Average SNR of received signals = 50 dB

With reference to figures 9 to21, one may observe that there is a relationship between the terrain density and the average SNR of received radar signal. Lower the terrain density higher the value of SNR. The theoretical justification for this phenomenon is not dealt with here in this thesis because it involves a strong mathematical study of terrain and clutter modeling and anomalous and duct propagation of electromagnetic radiation. In addition to that, one has to take into consideration the terrain density of the flight path also. Such a kind of study is not in the scope of the work intended to be carried out in this paper.

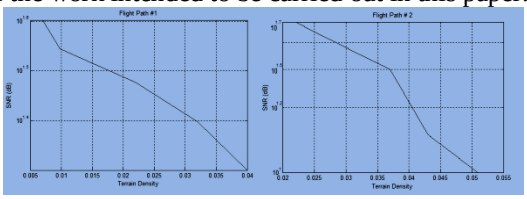

Figure 22: Plot connecting terrain densities and SNRs

Figure 22 shows a graphical representation of the relationship between terrain densities and average SNRs of received radar signals.

So far we have seen the techniques used in the art of electronic espionage in the ESM sense. Hardware and software involved in this practice is also seen. A special kind of software called Logical Image Processing has been introduced here for the purpose of drawing flights path and signal paths of chosen mission flights with real time geographical digital maps.

Author :

Ch. Raja completed B.E (ECE) from Andhra University, Vizag in 1994 and M.Tech (DSCE) from JNTU, Hyderabad in 1999. Obtained Ph.D from JNTU, Hyderabad in 2014 in the area of Radar Signal Processing (electronic warfare). Presently working as an Associate professor in Mahatma Gandhi Institute of Technology, Hyderabad. He is having 22 years of teaching experience and taught subjects like Digital Signal Processing, Electronic Devices and Circuits, Probability Theory and Stochastic Processes and Switching Theory and Logic Design etc. He is a life member of ISTE,Fellow of IETE,FIE(I) and LMSSI. He also visited the City University of Hong Kong, Hong Kong, as an Academic visitor for a period of two months in the year 2000. He has published several papers in international journals and conferences in the area of Electronic Warfare, Antennas and Image Processing.