



VS-1200 Frequency Domain Scrambler



Shown: VS-1200

Midian's VS-1200 series is a Digital Signal Processor (DSP) based Frequency Domain voice scrambler offering a high level of voice privacy. This technology is comparable in security to rolling code scrambling, yet does not require synchronization.

The DSP converts the analog signal into quantized digital data. It then converts the "Time Domain" signal into the "Frequency Domain". This results in an audio "frequency spectrum", which is then partitioned into bins that are encrypted by the non-linear key generator. The digitized data is converted back to the analog realm using a digital to analog converter.

The above technique and the lack of synchronization result in excellent audio quality, high security and enables the VS-1200 to be used in virtually any type of radio system. These systems include HF SSB, Conventional two-way, Trunking, and Voting.



Shown: VS-1200-VX1

The VS-1200 series has the following features:

- Total code combinations: $\sim 6.2 \times 10^{23}$
- Actual code combinations: ~ 4 billion
- Number of selectable keys: 3
- 4 user-programmable levels of security including voice inversion
- Multi-Format ANI including Motorola's MDC-1200, Kenwood's FleetSync, Harris' G-Star (aka GE-Star), DTMF and 5-Tone
- Automatic detection of scramble
- Programmable audio levels
- Dimensions: 1.59" L x 0.83" W x 0.21" H
- Plug in modules are available for Icom, Kenwood, Motorola and Vertex.
- Requires Midian's KL-4 Programmer

Below are some common applications for voice scramblers:

Military: Maintain tactical level classified information and the secrecy of planned tactical operations (TVS-2 and VS-1200).

Police: Keep criminals & news media from listening in on police communications. Criminals that eavesdrop may use the knowledge of police communications to avoid detection by police & plot activities. Protect sensitive information from being used by the news media or crime scenes from being interfered with prior to a police arrival.

Ambulance: Secure communications maintain the integrity of patients' information (HIPAA) from being intercepted when transmitted over the air.

Fleets: Taxi, towing and fishing competitors often use information intercepted over the air to take business from one another.

Industry: Some extreme activists eavesdrop on chemical and mining companies' communications. These activities can cause unnecessary harassment and litigation and may cost the companies financially.

Utilities: In an effort to protect a country's infrastructure, utilities are encrypting communications to prevent outsiders from learning information that could expose weaknesses in construction, operations, etc. that could make the site a more susceptible target.