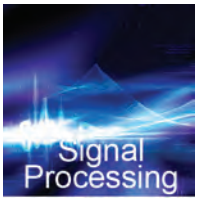
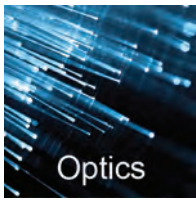




National Security Agency

2014 TECHNOLOGY CATALOG

TTP

TECHNOLOGY TRANSFER PROGRAM

2014 Technology Catalog

V2.0
July 2014

NSA Technology Transfer Program

National Security Agency
9800 Savage Road, Suite 6848
Fort Meade, MD 20755-6848

tech_transfer@nsa.gov
866-680-4539

www.nsa.gov/research/tech_transfer

This publication is available in PDF format on the NSA Technology Transfer Program website at www.nsa.gov/research/tech_transfer

WELCOME

The National Security Agency's Technology Transfer Program (TTP) was established to openly share federally funded technologies with industry, academia, and other federal agencies. Since 1990, the NSA TTP has provided outside entities access to NSA invented technologies and collaborative research and development opportunities.

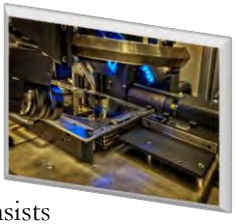
The patents in this catalog are the NSA invented technologies that are available to be shared with U.S. government agencies, industry partners, and academia.

TABLE OF CONTENTS

TABLE OF CONTENTS, CONTINUED

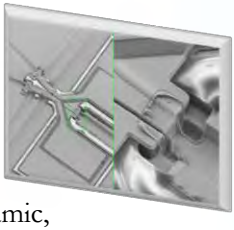
Overview

What is Technology Transfer



In the context of federal laboratories, technology transfer is the sharing of information, intellectual property (IP), expertise, and technology between the laboratories and non-federal entities (i.e., private industry, state and local governments, universities, and non-profit organizations). It consists of transfers at various levels within the technology lifecycle, ranging from conception to the actual selling of products or services in the marketplace.

Goals of the NSA's TTP Program



The NSA recognizes the value of its investments in R&D activities and the potential impact of these activities for enhancing the U.S. economy. More importantly, the NSA appreciates that leveraging its R&D with others can have a significant impact on its ability to meet the dynamic, time-sensitive requirements of its mission. This recognition is why the Agency actively participates, supports, and encourages technology transfer through its Technology Transfer Program.

Goals of the NSA TTP include:

- Encouraging commercialization of the NSA technologies
- Strengthening the U.S. industrial base
- Accelerating development of emerging technologies through cooperative research and development activities

- Developing dual-use technologies for application by the government and the commercial marketplace
- Recognizing and reward the accomplishments of the agency's scientists and inventors
- Accepting commercial-off-the-shelf (COTS) technology for government use to reduce the cost of items purchased by the federal government

"... the Agency actively participates, supports, and encourages technology transfer ..."

Doing Business with the TTP

Parties interested in partnering with the NSA's Technology Transfer Program should contact the program office for additional details. Please note that all companies interested in licensing NSA technology must be U.S.-based or have a wholly owned U.S.-based subsidiary. The following is a brief description of the requirements and process.

Licensing Process

Each license is negotiated individually and license terms may differ based on readiness of the technology, additional development requirements, exclusivity of license, estimated market size, and other factors.

Patent Bundles

Patented technologies presented in this catalog may be shown as being bundled with a group of similar properties. Please note that all technologies are available for license individually and patent bundles are presented for convenience only. Patent bundles for license purposes are solely at the discretion of the licensee.

Typical Agreement Provisions

Although each agreement is individually negotiated, most have the following provisions:

- Exclusive, partially exclusive, or non-exclusive license
- License duration, reporting period, fees, and royalty payments
- Letter of Application and a Business Plan for commercialization and marketing the technology
- Federal Register notice posted by the NSA identifying invention, licensee, and type of license (exclusive and partially exclusive licenses only)
- Public availability of invention within a reasonable period of time
- Government retention of irrevocable, royalty free, worldwide government purpose rights to the invention

8 STEPS TO LICENSING TECHNOLOGY

1 **IDENTIFICATION**
Prospective licensee identifies a specific technology.

2 **DISCLOSURE**
Prospective licensee contacts the Technology Transfer Program and completes Letter of Intent, Non-Disclosure Agreement, and Company Validation Form.

3 **ASSIGNMENT**
TTP Director assigns agreement to a transfer agent (TA) who facilitates dialogue between licensee and inventor(s) / technologist(s).

4 **SUBMIT**
Licensee decides to pursue agreement and submit Letter of Application (LOA) and Business Plan.

5 **EVALUATION**
Letter of Application and Business Plan are evaluated for technical, business, marketing, and economic understanding of intended product.

6 **AGREEMENT**
The TA, in cooperation with the Office of General Counsel (OGC), drafts agreement.

7 **NEGOTIATIONS**
Negotiations are conducted between licensee and the transfer agent.

8 **LICENSING**
After negotiations are complete, agreement is signed by both parties and executed.

AVAILABLE TECHNOLOGIES

The NSA has an extensive portfolio of patented technologies across multiple technology areas.

TECHNOLOGY READINESS

Technologies presented in this catalog are at various readiness levels. Some technologies are only theoretical basic research where others may be demonstrable, fully developed products. Please contact the Technology Transfer Program for more details on the readiness level of a particular technology.

ACOUSTICS

The NSA is a leader in acoustic research. These advanced acoustic technologies are a cornerstone of the NSA's mission to produce foreign signals intelligence. With the enormous increase in voice and acoustic data, the demand for faster, more accurate voice and acoustic signal analysis and filtering has never been greater. To meet this growing demand for voice signal intelligence, the NSA continually conducts research in acoustics signal analysis, phonetics, audio signal identification, and audio transcription.

Within the acoustics technology area, the NSA has several technologies available for license. These technologies include: methods for identification, extraction, and analysis of voice and voice signals; foreign language voice recognition; duplicate voice identification; and methods of measuring voice enhancement.

Real-Time Simultaneous Identification of Multiple Voices

Patent: 8,442,825

The invention provides multiple speaker identification by identifying voices in a manner that uniquely mimics the essence of ear-to-brain interconnection combined with observed human voice identification learning and recognition processes. The object is real-time or faster voice identification needing only relatively simple computing resources. Specifically, this invention looks for prosody matches (spectral patterns over time periods) that were trained by software in an Artificial Neural Network (ANN) description.

VALUE

Excludes non-speech sounds within audio
Real-time processing

Measuring Degree of Enhancement to a Voice Signal

Patent: 7,818,168

This technology is a method of measuring the degree of enhancement made to a voice signal. Typically, voice signals are statistically non-stationary and the more noise, or other corruption, introduced into a signal, the more stationary its distribution of values become. In this invention, the degree of reduction in stationarity is indicative of the degree of enhancement made to the signal. The method of determining the degree of enhancement begins with receiving and digitizing the signal. A user then identifies a number of formant regions and computes the stationarity for each formant. The voice signal is enhanced and formant regions in the enhanced signal are identified. The stationarity for the formants in the enhanced signal is found. Finally, a comparison is made between the stationarities of the original and enhanced signals.

VALUE

Quantifies voice enhancement
Reduces human arbitration and various listening tests

COMPARING VOICE SIGNALS

PATENT: 7,650,281

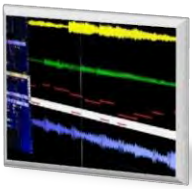
This technology tests the robustness of a given voice-matching algorithm by providing the algorithm with variants of a given digital file and testing the original against these variants including time-reversal, segmented re-arrangement, or a mixture of both time-reversal and segmented re-arrangement. In effect, this increases the corpus of ground truth, thus allowing realistic testing under controlled conditions.

VALUE

Reduces the Equal Error Rate (EER)
Larger corpus from fewer files

IDENTIFYING DIGITAL AUDIO SIGNAL FORMAT

PATENT: 7,620,469



This technology identifies the format of a digital audio signal including signals that are either self-defining or headerless. In this method, a digital audio file is received and converted from an assumed format and bit ordering to a user-definable format. The file is divided into blocks and the frequencies of occurrence are determined.

A first set of frequencies of occurrence less than and equal to most frequently occurring integer is created. Next, a second set of frequencies of occurrence greater than the most frequently occurring integer is created. Third and fourth sets of differences are created and replaced with polarity indicators. These indicators are summed and percentages calculated to determine maximum pairings. The statistics are then assigned to the converted file. This process is repeated with another format and bit ordering to identify the format with the maximum statistics.

VALUE

Identifies digital audio formats, including self-defining signals
Reduces need for human listening

Automated Detection of Duplicate Audio & Voice Recordings

Patent: 7,571,093

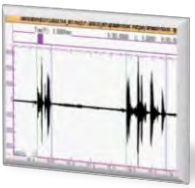
This invention detects duplicate audio and voice recordings in a collection. A recording is selected, divided into segments, and a pitch value is extracted for each segment. The total time a voice appears in the recording is estimated and pitch values that are less than or equal to a user-defined value are removed. Unique pitch values are identified and the frequency of occurrence is determined and normalized. The distribution percentiles are then calculated. This method is repeated for each recording where it is compared for total voice time, average pitch value, and distribution percentile.

VALUE

No manual transcription required
Language and content independent

Detecting Voice Activity

Patents: 7,127,392 and 6,556,967



This technology eliminates the need to manually search audio files for speech content by automatically locating speech intervals that may contain other signals such as music, noise, or empty space. It outputs the start and stop times of these intervals relative to the beginning of the file, ignoring non-speech portions of the file. This technology classifies signal segments as speech or non-speech and employs algorithms which consider characteristics derived from an audio signal's AM envelope.

VALUE

Reduces bandwidth and traffic
Improves performances of speaker recognition systems

ADVANCED MATHEMATICS

In order to remain a world leader in cryptologic methods, the NSA must continually increase its knowledge base of advanced mathematics. To fulfill its mission to secure U.S. communications and maintain the country's ability to exploit new advanced foreign communications systems, the NSA has become one of the largest research laboratories in the mathematical sciences.

NSA mathematicians continually develop new mathematical methods and several of these methods are available for license. Technologies available include computerized systems for solving non-linear Boolean equations, cryptographic methods, random number generation, geometric pattern recognition, and methods to display complex mathematics.

Collision Free Hashing for Near Match Inputs

Patents Nos: 8,363,825 and 8,355,501

This technology is a hash function that does not produce collisions for inputs that are near matches of each other, where a near match is one where the number of bit locations that differ is small and, therefore, could more easily be found than if the inputs were not near-matches.

This method allows you to define a minimum number of bit positions that differ between the first and second inputs, define the degree of the first polynomial, define the bit length of the inputs, and define the bit length of the check value.

VALUE

Does not produce collisions for near match inputs
Enables faster hashing and data retrieval

Code Generation That Minimizes Error Propagation

Patent No.: 7,676,725

When transmitting binary data, encoding schemes make the resulting waveform more immune to noise and interference. One class of transmission codes, block or line codes, are used to modulate binary symbols 0 and 1. There is a need to minimize error propagation in a line code, subject to information rate, ones density, and maximum run length. The present method is a method generates a line code so that error propagation is minimized.

This method selects the number of bits in an unencoded sequence, the number of bits in an encoded sequence, the maximum run length of an encoded sequence, and a range of ones densities of an encoded sequence. Next, an encoding map is generated that maps each unencoded sequence to an encoded sequence and generates a decoding that maps sequences. Finally, this an error-propagation score is determined and returns if a lower error-propagation score is required.

VALUE

Minimizes error propagation in block or line codes
Sets information rate, ones density, and maximum run length

CRYPTOGRAPHIC KEY EXCHANGE USING EFFICIENT ELLIPTIC CURVE

PATENTS: 7,505,585 / 7,024,559 / 6,993,136

This technology is a combination of six patented methods for generating a cryptographic key between two users. The original methods include the groundbreaking technology of identification and digital signature using efficient elliptic curve.

Additional patented innovations build on the prior art by adding a binary expansion in joint sparse form and a method of generating and verifying a cryptographic digital signature using coefficient splitting. Further innovation includes a method of generating a cryptographic key using coefficient splitting on two different classes of elliptic curves which can be implemented in both a non-authenticated key exchange method and an authenticated key exchange method.

VALUE

Uses fewer steps for cryptographic key exchange
Coefficient splitting minimizes number of elliptic curve operations

METHOD & SYSTEM FOR NON-LINEAR STATE-BASED SATISFIABILITY

PATENT NOS.: 7,380,224 AND 6,912,700

This invention is a method of solving a system of generalized non-linear Boolean equations. Proving that a solution exists is called Satisfiability and if no solution exists called Unsatisfiability. This method does not require the translation of the system of equations into Conjunctive Normal Form (CNF) such as CNF SAT solvers or solve for all inputs such as Binary Decision Diagrams (BDDs).

This technology consists of a computerized method for solving non-linear Boolean equations that consist of partially solving the non-linear Boolean equation and stringing a pre-computed search inference relating to the equation in a state machine. Next, the user accesses a search inference from the state machine to develop a heuristic for solving the non-linear Boolean equation. Finally, it can be determined if the Boolean equation is satisfiable using at least one heuristic.

VALUE

Computerized determination of Boolean equation satisfiability
Equation translation into Conjunctive Normal Form not required

Cryptographic Identification and Digital Signature using Elliptic Curve

Patent No.: 7,062,043 / 7,024,559 / 6,898,284

The patents presented here highlight enhanced uses of ECC for cryptographic identification, cryptographic key generation and exchange, and digital signatures, and describe how to improve the efficiency of this approach by reducing resource requirements for each operation as well as by reducing the number of required operations.

VALUE

Requires fewer operations than other forms of ECC.
Increases system efficiency and performance.

Testing a Randomizer

Patent No.: 6,798,883

Devices that produce a random number are often referred to as randomizers and most rely on one or more sources of random data (e.g., timing of random events as compared to a threshold, random natural processes, etc.). The sources of random data are usually connected to a scrambling device that mixes the random data in some complex fashion to achieve a degree of uniformity in the distribution of the output of the randomizer.

This invention tests the sufficiency of an output of a randomizer, that is based on at least one source of random data, by determining the probability that an output of the randomizer will reoccur and by determining the minimum number of guesses one would expect to have to make to correctly determine an output of the randomizer.

VALUE

Tests the sufficiency of an output of a randomizer
Provides device mix probabilistic data to form random data

Passing a Cryptographic Key and Allowing Third-Party Access to the Key

Patent No.: 6,724,893

This invention is a method of passing a cryptographic key between users so an authorized third party (i.e. law enforcement) can access the key. This method is called *key escrow*.

With this method, a key recovery access field is embedded into the key pass method. The access field is embedded into a parameter "z." The access field allows an authorized third party to recover the key with the help of an escrow agent. Alternate methods adds steps that would allow the second user to determine if the first user is complying with escrow aspects of the method.

VALUE

Authorized third-party able to access key
Exchange key in certified, bandwidth efficient manner

Cryptographic Method Using Modified Fractional Fourier Transform Kernel

Patent No.: 6,718,038

With this technology a signal is received and an encryption key is established, where the key includes at least four user-definable variables including angle or rotation, a time exponent, a phase, and a sampling rate. At least one component of a modified fractional Fourier transform kernel is selected, where each component is defined by one of the encryption keys; and the signal is multiplied by at least one component of a modified fractional Fourier transform kernel selected. For decryption, a signal to be decrypted is received; at least one decryption key is established, where each decryption key corresponds with, and is identical to, an encryption key used to encrypt the signal.

VALUE

Use to encrypt a message header to act as electronic signature
Not limited to cotangent and cosecant functions as prior art

Multi-Dimensionally Accentuating a Deviation in Information and Identifying its Cause

Patent No.: 6,470,297

Information theory has grown to include not only preserving the integrity of a message transmitted over a communication network but also the communication network itself. Multiple devices and methods exist for preserving the integrity of a communication network through the detection of intrusion or misuse. However, no prior art discloses a method of multi-dimensionally accentuating a deviation in a transmitted message and identifying the cause.

This invention is a method of multi-dimensionally accentuating any deviation in information and identifying the cause by reducing the amount of information presented to a user and describing the information with an entropy-based function, a temperature-based function, an energy-based function, or any combination.

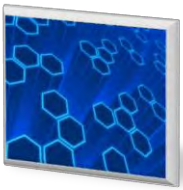
VALUE

Information may be of any type that can be arranged in a sequence
Reduces amount of information to a manageable level

"Technology transfer provides an avenue for cycling the benefits of federally funded R&D back into the U.S. economy."

LATTICE QUANTIZATION

PATENT NOS.: 6,404,820 / 6,085,340 AND 6,084,534



A quantizer is a device for converting numerical data into a finite number of possible outputs. Quantizers are used in the design of signals for use over noisy channels. This technology is a method of efficient storage and reconstruction of the codewords of the Extended Hamming Code and is typically used for pulse or digital communications.

This method is a combination of three patented technologies of lattice quantization. The first and third inventions are methods of lattice quantization that minimizes the storage requirement and the computational complexity of an eight dimensional lattice quantizer. The second is a method of lattice quantizing 24 real-number-long data points so that storage requirements are minimized.

VALUE

Minimizes the computational complexity
Minimal storage requirements

DISPLAYING 3D NETWORKS IN 2D WITHOUT FALSE CROSSINGS

PATENT NO.: 6,043,825

Graphic representations can help make networks more understandable by helping visualize the structure and, generally, network configurations are depicted as wire diagrams or graphs. That is, the processing nodes are represented as graph vertices, while arcs connecting the vertices represent the actual physical wires connecting the nodes.

The present invention is an efficient method for transforming and displaying the dynamic performance of three dimensional interconnection networks in a two dimensional graphical display by eliminating the false crossings that normally occur in such transformations. In addition, this invention allows dynamic selection of any node of the network to be the node of reference positioned at the center of the graphical display.

VALUE

Graphically represent 3-D networks without false crossings
Dynamically select any node as node of reference

COMMUNICATIONS

The NSA is charged with keeping the federal government and military communications systems secure. As a result, the agency is an aggressive developer of communications equipment and products used for wireless and wired transmission systems. These technologies include encryption systems, speech transmission methods, communication intercept devices, synchronization methods, and error correction techniques.

Communications technologies available for license include methods of transmitter geolocation, station synchronization methods, error correction, filters, equipment simulation methods, and novel speech transmission techniques.

LOCATING A TRANSMITTER

PATENT NO.: 8,068,850

This technology geolocates transmitters by replacing the circuitry used in Time Delay of Arrival (TDOA) calculations with a communication link back to a central station. In this method, a portion of a received signal is transmitted to a control station. A calibration signal is received at multiple receiving stations and a communications link is established between the receiving station and a central control station. Geolocation is performed by subtracting the communications link time delay from the time of arrival of each received signal or by calculating the communications link time difference of arrival for each pair of receiving stations and subtracting the result from the TDOA calculated from the received signal.

VALUE

Geolocates uncooperative transmitters at a central station
Requires no TDOA circuitry at each receiving station

PROXY/INTERMEDIARY DETECTION

PATENT NO.: 7,466,654

This technology uses latency differences to detect intermediary devices. A sensor is placed on the user's computer to record communication packets to and from a communication device. The packet times are recorded and analyzed to extract the minimum network layer latency and the minimum application layer latency. As the latency begins to get larger than the network layer latency, it indicates the application is not being operated from the advertised network connection, but from elsewhere.

VALUE

Provides vicinity information
Active location sensors not required

Wideband Retroreflector

Patent No.: 7,383,026

This novel technology is a single wideband retroreflector that eliminates the need for a local oscillator and a local transmitter. In addition, this technology, does not suffer the limitations on switching speed of non-linear junctions that limit instantaneous bandwidth common in prior art designs. This invention transfers data by the illumination of the retroreflector with a continuous wave of RF energy, where the retroreflector both modulates the incoming signal and retransmits it using the incoming signal energy.

In the present invention, an externally produced continuous wave radio wave transmission within the microwave-millimeter wave frequency band is modulated with a wideband signal with a minimum operating instantaneous bandwidth of 5 KHz to 500 MHz and retransmitted as a modulated waveform by the antenna.

VALUE

Eliminates need for a local oscillator and transmitter
Modulates incoming signal and retransmits using incoming energy

Impedance Matching RF Open Wire Transmission Lines

Patent No.: 7,283,015

This technology is an innovative device for impedance matching along open wire lines. Prior methods have issues such as added operational noise, limited adjustability, and are difficult to manufacture. This invention is comprised of a dielectric material with a ground plane affixed to one surface and a microstrip line conductor disposed on the opposite surface, and a movable dielectric plate. The bottom surface of the movable dielectric plate has a higher dielectric constant than the dielectric material, and the top surface possesses a conductive coating. The bottom surface of the movable dielectric plate engages a portion of the microstrip line conductor, and is movable transversely to the conductor to increase or decrease impedance and linearly change the phase. As a result, this device matches impedance during transmission in a manner that significantly reduces noise.

VALUE

Customizable device shapes provide application flexibility
Reduces current issues with UHF/microwave impedance matching

Time Sychronization Without Broadcasting a Sychronization Signal

Patent No.: 7,227,858

This CICADA protocol is a synchronization method that uses the environment as a means of ensuring that nodes within the network are working in the same time domain. This method of synchronization dynamically sets the node's timer to awaken an individual 'sleeping' node at a frequency determined by an environmental sensor variable. The environmental variable, along with empirical data, will determine the interval at which sleep intervals will be modified until a synchronization point is reached.

VALUE

Conserves energy between intervals of time
Reduces detectability and susceptibility to denial of service attacks

Correcting Errors in Formatted Modem Transmissions

Patent No.: 5,533,033

This invention is a device for and method of correcting bit errors in a formatted modem transmission that does not employ an exhaustive-search scheme. This technology is highly efficient because a much smaller number of possible errors are considered.

This method identifies those error patterns that are most likely to occur and searches for only these errors. This method identifies the formatting scheme used by the transmitting modem, checks the received data for errors, generates possible error patterns and associated correction patterns for the receiving modem, identifies the type and location of each error, and replaces each error with its associated correction pattern.

VALUE

Identifies error patterns most likely to occur
Highly efficient, smaller number of possible errors considered

COMPUTER TECHNOLOGY

The NSA has been at the forefront of computer technology for over 60 years. As one of the first developers and users of supercomputing technology, NSA personnel have participated in or tested virtually every computer advancement since the 1950s. In order to keep the NSA at the forefront of computing, agency researchers and computer scientists continue to develop advanced computing platforms, novel computing techniques, and advanced coding tools.

Computing technologies available for license include both advanced software techniques such as methods of protecting computer stacks as well as novel hardware input/output devices.

Converting Computer Program with Loops to One without Loops

Patent No.: 7,788,659

This invention was released to the NASA Software Release Authority and was developed as part of the Java Plug-in Framework (JPF) Project.

This method eliminates loops from a computer program. This method receives the program, graphs its function and control, identifies its entry point, and identifies groups of loops connected to its entry point. If there are no such loop groups the process stops. Otherwise, a group of loops is selected and the group's entry point is identified. If the selected group includes no group of loops having a different entry point then the group is replaced with a recursive or non-recursive function. Each connection entering and exiting the selected group is reconfigured to preserve their functionality.

VALUE

Preserves order of execution of the computer program
Available as open source application under JPF

Protecting a Computer Stack

Patent No.: 7,581,089

This novel invention is a method of protecting information stored on a computer stack in an easily accessible but un-modifiable location protecting the unmatched calls/returns from being overwritten.

In this method, two stacks are created. The first is a normal stack and the second, or shadow stack, has shadow frames. These frames contain the return address upon a subroutine call, the address on the first stack where the return address is stored, and a user-definable state variable which is used to identify a shadow frame as a return address. Before returning from a subroutine, the two return addresses are compared, and if they do not match, the second stack is searched down, and then up, for a matching return address. If there is a match, the shadow is re-synchronized with the first stack by comparing the stored values of the first stack pointer with the first stack pointer and adjusting the shadow stack pointer.

VALUE

Stores protected information in a non-spoofable, efficient way
Protects unmatched calls / returns from being overwritten

INFORMATION PROCESSING

As the amount of speech, video, data, print, and multimedia continues to increase exponentially every year, the NSA is aggressively leading research efforts in methods to collect and process this massive amount of information. Today, NSA scientists continue to develop new methods for transporting, storing, retrieving, and analyzing information critical to national security.

Technologies available for license include methods to efficiently store, retrieve, and modify data in any language format, methods to extract text from graphics, data modeling techniques, optical character recognition, and authentication methods.

LINEAR INTERPOLATIVE CODING

PATENT NO.: 8,539,307

This invention is a device for and method of detecting and correcting errors in both a future and a past data value by computing both backward and forward coefficients. The types of errors detected and corrected include garbled data, missing data, and added data. In a garbled datum, the datum is present but its value is incorrect (e.g., transmission error due to noise in the transmission channel). A missing datum is supposed to be present but is not (e.g., synchronization error between the transmitter and the receiver). An added datum is not supposed to be present but is (e.g., perceived synchronization error between the transmitter and the receiver). This technology includes a control unit, coefficient computation unit, error computation unit, and an error detection and correction unit.

VALUE

Improves the detection and correction of errors
Detects and corrects errors in both future and past data

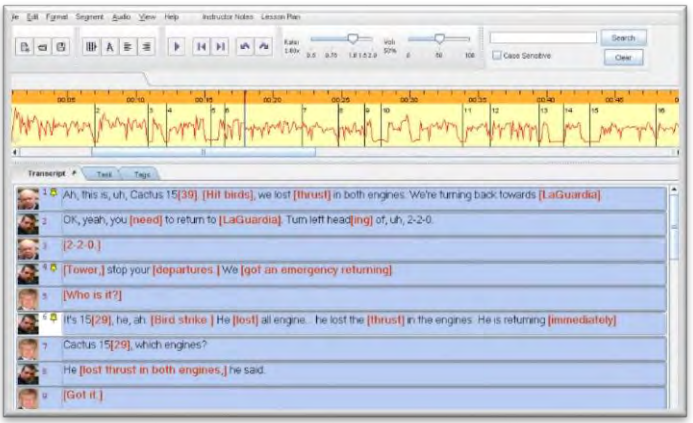
Multimedia Instructional Design System / Digital Transcription System (ScribeZone™)

Patent No.: 8,380,485

ScribeZone™ is a multimedia language processing system that has enhanced capabilities to improve the efficiency and speed of transcription and translation of audio, video, and graphic materials. This technology is also a development and delivery system for media-based instruction specifically designed for, but not limited to, language instruction. ScribeZone™ facilitates audio and graphic contextual analysis training, transcription, and translation, as well as comprehensive language skills enhancement. ScribeZone™ supports any foreign language input so it is ideal for teaching foreign language and can also be used for teaching English as a Second Language (ESL).

VALUE

Side-by-side language translation
Optimize quality control through collaboration



Assessing Language Translation and Interpretation

Patent No.: 8,185,373

This patented method establishes a standard for translation metrics, offering analysis and feedback for grading and improving translation activities. The method first consists of the receipt of a communication (source) along with identification of the source's content and format. The source material is evaluated and assigned a user-definable level of difficulty along with the translation type necessary. Next, the source translation is assessed with user-definable ratings of accuracy, interpretation of intended message, and formatting. These ratings provide the results to determine a user-definable assessment of the language translation and interpretation of the source material.

VALUE

Increased performance and reduced subjectivity
Macrotextual focus

Identifying Connected Data in Relational Databases

Patent No.: 8,001,137

This invention is a method of querying a relational database using a computer language such as Structured Query Language (SQL) to automatically determine a user-definable derived relation. This method receives data components and initializes tables with data identifiers and connection information. A transition table is initialized and each entry is replaced with a user-definable relationship of its identifier, corresponding connected data component identifier, and transition table identifier. The tables are updated and, depending on identifier transitions, the replacement step is repeated. Finally, the received data components are identified as connected based on equalities in the table entries.

VALUE

Faster relationship determination
Less prone to errors than manually determining derived relations

Identifying Topic of Text Using Nouns

Patent No.: 7,805,291

Prior methods of topic identification were based on keywords. A disadvantage of this method is that any variation in the spelling of a keyword without any significant change in meaning may cause the performance of the method to degrade.

In this method, the nouns in the text are identified and the form is determined. Combinations are created of the singular form (number is user-definable) and the frequency of occurrence of the singular form is determined. A frequency score is assigned and each combination is assigned a score that is equal to the sum of the scores of its constituent singular nouns. The top scoring singular nouns and combinations of singular nouns are selected as the topic of the text.

VALUE

No keyword performance degradation
Improved performance over dictionary variants of keywords

Database Searching and Identifying Text (ALADDIN)

Patent Nos.: 7,797,152 / 7,761,286 and 7,539,611

This technology incorporates two functions: a Tagger and a Matcher. The Tagger searches for transliterated terms (such as names) within large data sets using lexical, contextual, and morphological information. The Matcher is then applied to determine which candidate terms are known within the database and therefore of likely increased interest to the reader. The Matcher is a foreign language term-matching tool that provides results based on how the term, with variant spellings, matches entries from various dataset term lists. This knowledge-based system for term matching maintains contributions from expert linguists and an extensive collection of transliterated data.

VALUE

Linguistic expertise for the non-expert
Adaptable algorithms

SORTING TEXT AND STRING SEARCHING

PATENT NO.: 7,734,671

Prior methods of searching for a regular expression were scanning techniques. For example, reading the input text one character at a time and checking for matches. However, as data volume increases, these scanning search strategies take longer, and index-backed searching algorithms become of greater importance.

The present invention provides a method of string searching that is more efficient for large volumes of data using the Ferragina and Manzini (FM) index, a string-searching index based on the Burrows-Wheeler transformation.

With this method, an FM-index is created on received text, and a number of rows are marked. The locations of the rows are stored in data buckets as well as the last column of the FM-index, which is stored as a wavelet tree. Data blocks containing the data buckets are created, containing the number of times each character appears in the data block before each data bucket. A header block is created comprising an array of the number of times each character appears in the last column of the FM-index before each data blocks, the location of the end of the data blocks and the location of the end of the data, and appended to the data block. The header and data blocks are stored. The search process loads data buckets into memory as needed to find the required text.

VALUE

Increased efficiency for large volumes of data
More space efficient than prior art suffix tries

Modeling Single-Class Data from Multi-Class Data

Patent No.: 7,454,337

Data can include different classes within one category (speech, images, text). In speech applications, multi-class data includes speaker of interest data, speech from both genders, or multiple language speech. Prior methods modeled data from one particular class or data of a particular class contaminated with data from other classes.

The extensible technology presented here isolates a variety of entities (text, image, voice) from multi-class data. Purification of the statistical model for a data class, calibrated from data representing the identified class and at least one other class, allows enhanced identification and detection capabilities while simultaneously reducing memory and processing requirements.

VALUE

Eliminates costly memory swapping
Removes nonessential artifacts

Morphological Text Processing

Patent No.: 7,409,334

This method of morphological text processing provides all inflected forms, or any subsetthereof, of an input word or group of words of a highly inflected language. In this method, text is received, a language is selected, and a textual unit is selected. Next, the textual unit's stem and suffix is identified and a rules database is searched for the suffix. If a base suffix is found in the rules database, it is combined with the stem to form a lemma and a lexicon database is searched for the lemma. If found, a model number from the lexicon database is retrieved and cross-referenced with the rules database to obtain all inflected suffixes for the selected textual unit. Finally, the inflected suffixes are combined with the stem to form inflected forms and a subset of inflected-forms. Information associated with the lemma and inflected suffixes is output.

VALUE

Morphological text processing
Provides all inflected forms or subset for input word or word group

Automated Separation of Hand-Written and Machine-Printed Images

Patent No.: 7,072,514

This language agnostic technology automatically characterizes documents as hand-written, machine-printed, or unknown. Utilizing this method, document images are quickly scored and sorted. To assign meta-data to an image, this technology identifies and evaluates connected components within a given document, followed by comparison of suspected characters, and grouping of suspected matches by category. The result is the capability to more accurately search and sort large document collections.

VALUE

Discriminates between hand-written and machine-printed images
Language and font agnostic

Summarizing Text by Sentence Extraction

Patent No.: 6,990,634

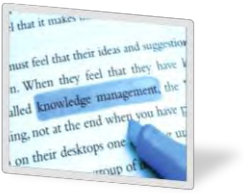
This method uses a simplified, internal algorithm to extract only those sentences from text that convey the essential meaning. The number of sentences is limited to only provide enough information for a user to determine whether or not to read the text in its entirety, or to act as a substitute for the text. With this method, each sentence in a given text is identified along with each term in the sentence. A matrix is generated with each column representing a sentence and each row representing a term. Each entry in the matrix is then replaced by a product of the matrix entry and a user-definable function that decays exponentially, so that several determinations of Euclidean length can be made in order to assign a relative value to each component of the text.

VALUE

Text summaries save time and effort
Provides concise summary of full text

Self-Referential Text Summarization (KODA)

Patent No.: 6,904,564



This technology solves the problem of extracting key sentences or phrases from a document for the purpose of summarizing the document, allowing rapid and accurate decisions about whether the document is relevant, without having to open and scan the entire document line-by-line and without the use of outside exemplary texts, dictionaries, or encyclopedias. KODA evaluates each text segment and scores its relevance to the remainder of the text. KODA also quickly and effectively processes overwhelmingly large textual data sets, reducing each document to a few representative passages. The depth of detail is user-definable.

VALUE

Fast and accurate text summarizing
Saves time and effort

Printing Portion of Document with Accountability and Error Detection

Patent No.: 6,657,740

This invention is a method for printing a portion of a document with an emphasis on accountability through the incorporation of automatic error detection. By working through a sequence of determinations, conversions, checks, and comparisons, this method guarantees that the content of a print file is precisely what is physically printed on to the actual page. For example, if a single byte is found to be out of order from its original intended format, this technology is able to detect the discrepancy and prevent the printing operation.

VALUE

Assures 100% accurate representation of original file
Zero error tolerance

DATA RELATIONSHIP AND VISUALIZATION TOOL (RENOIR)

PATENT NO.: 6,515,666

RENOIR is a Java-based data visualization tool having strong analysis capabilities for manipulating and visualizing transactional or relationship type information.

RENOIR accepts data sets of any size in most common formats that contain relationships within the data and, within seconds, automatically generates a graph, displaying the relationships as nodes and links.

The application offers numerous data layout, clustering, and annotation features that produce a knowledge-rich diagram that enables data mining and understanding of the activity (e.g., relationships) in the raw data. It provides basic and advanced link analysis functions, including temporal analysis, social network discovery, data normalization, hierarchical clustering, and integration with other tools. A few example analyses include:

- Temporal analysis — view, animate, and mark data
- Content analysis — discover patterns in unformatted text using n-gram analysis
- Network analysis — discover paths through networks
- Cyber analysis — detect denial of service attacks

RENOIR is also able to capture user-defined process flows into a single step, and can operate on stored data and real-time data feeds.

A complete set of user manuals, training guides, system integration/coding examples, and quick reference cards are all part of this polished, fully supported, platform-independent program written in Java.

DATA RELATIONSHIP AND VISUALIZATION TOOL, CONTINUED

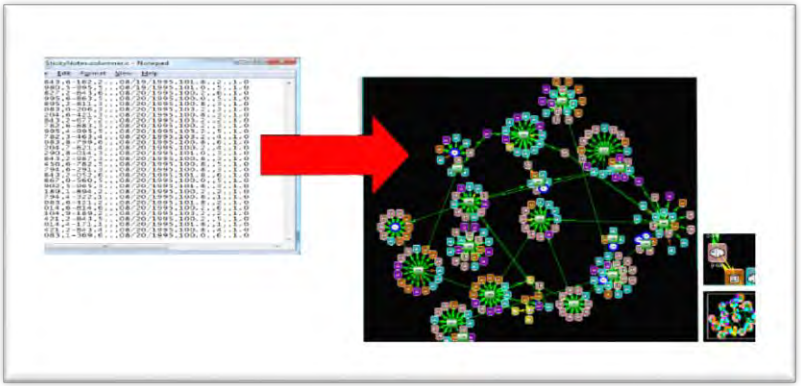
RENOIR takes large data sets that would otherwise be difficult for users to conceptualize and turns them into easily readable graphs. This powerful visualization tool works on any data set that contains associations and allows data from a variety of sources to be shared. RENOIR's unique patented data layout, community clustering algorithms, and well-developed graphical user interface (GUI) allows users to manipulate, analyze, and customize the tool. RENOIR is ideal for business intelligence applications and can be tailored to meet the needs of specific industries.

Potential markets include:

- Bioinformatics
- Law enforcement
- Energy management
- Telecommunications
- Data mining
- Finance
- Statistical analysis
- Search engines
- Marketing
- Business performance management

VALUE

Java-based tool captures user-defined process flows into a single step
Visualization works on any data set containing relationships



Finding Large Numbers of Keywords in Continuous Text Streams

Patent No: 6,311,183

In Selective Dissemination of Information (SDI) systems, text samples are run against static subscriber profiles. A sample that satisfies a profile is then selected and routed to the appropriate subscriber. In these systems, selection is often done by matching keywords specified in the profiles.

The technology presented here is a method of full-text scanning for matches in a large dictionary of keywords. The method is applicable to large dictionaries (hundreds of thousands of entries) and to arbitrary byte sequences for both patterns and sample streams. The approach employs Boyer-Moore-Horspool skipping, extended to pattern collections and diagrams, followed by an n-gram hash test, which also identifies a subset of feasible keywords for conventional pattern matching at each location of a putative match.

VALUE

Locates all matches of a keyword dictionary in a sample stream
Rapidly locates keywords without examining every sample stream byte

Full-Text, Large-Dictionary String Matching using N-Gram Hashing

Patent No.: 6,169,969

This invention is a method of large dictionary string matching that overcomes limitations of the prior art by locating keywords in continuous byte streams without the need for delimiters. This method factors each keyword into n-grams which are catalogued into hash tables. The input sample is then examined by hashing each n-gram and checking for matches. The primary test utilized in this method is an FPGA-based hardware solution in which a second software test is applied. Primary alarms generated by the hardware are then screened by a secondary tester to remove remaining false alarms.

VALUE

Improves prior art by locating keywords in continuous byte streams
Accommodates large dictionaries of keywords

IDENTIFYING DATA TYPE AND LOCATION IN A FILE

PATENT NO.: 5,991,714

The present invention is a method of identifying the types, and locations, of data contained within an electronic file, or document, of unknown data type. This method may be used to identify languages, the type of word-processors used to create the data, type of executable code included in a file, or compression schemes used to compress the data. A file may contain one or more data type of interest.

This invention is a method of counting unique n-grams and determining the weight. In an Exemplary file, the top weighted n-grams for each data type are selected and thresholds are set to determine data types. Next, data from a file with unknown data types is selected and every n-gram is listed. Weights are assigned and summed. Each sum is then compared to the threshold for that data type.

VALUE

Identifies language, data type, and compression in electronic file
Identifies type of word processor used and executable code

AUTOMATICALLY GENERATING TOPIC DESCRIPTION FOR TEXT

PATENT NO.: 5,937,422

This technology is a method of automatically generating a search query from a user generated natural language input. This technique uses a relational database automatically built from various online dictionaries with each word having several definitions and the words in the definition representing the relative importance of that word. The weight of each word propagates through the tree providing a measure of significance of each word to every other word. The words with the largest cumulative links are selected as possible topics.

VALUE

Estimates importance of every word in the dictionary
Text may be derived from any source

SEARCHING AN ON-LINE DICTIONARY USING SYLLABLES

PATENT NO.: 5,832,478

This invention is a method of improving the effectiveness of on-line dictionary searches by specifying the known syllables and their locations in the word sought, specifying the total number of syllables in the word sought, and putting a wildcard marker in the locations of the unknown syllables or unknown characters of a partially known syllable. The present invention is not limited to any language or any language representation.

With this method, a user first selects a language representation (e.g. Pinyin) for a query and performs the query. Next, the query is parsed to determine if and how many segmented syllables were used in the query. If no segmented syllables were used, a character string search for the headword that matches the query is conducted. If the query contains segmented syllables, a syllable search for headwords that contain the same syllables in the same locations is conducted. This method then returns one or more headwords in the language of the query and their corresponding definitions in the language of the user. Various wildcard symbols may be used for unknown syllables and for characters within a syllable, which may include tones.

VALUE

Improves effectiveness of wildcard searches of on-line dictionaries
Applicable to any language

Language-Independent Method of Generating Index Terms

Patent No.: 5,752,051

Automatic indexing systems typically return large volumes of documents from queries, either from full-text indexing or subject searching. This lends itself to using lists of automatically-generated index terms. The invention presented here generates index terms from sample text relative to a background corpus. In this method, background text is filtered to remove undesired symbols and n-grams are counted to produce background n-gram counts. Sample text is also filtered and n-grams are counted to produce sample n-gram counts. The background and sample n-gram counts are compared to produce n-gram scores and each symbol of the filtered sample text is assigned a symbol score derived from the n-gram scores. A symbol threshold is determined and words and phrases are extracted as index terms when the filtered sample text contains symbols whose scores exceed the symbol score threshold.

VALUE

Filters text to remove undesired symbols
Index terms drawn from text without language-specific processes

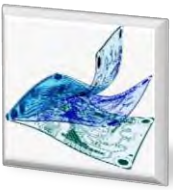
MICROELECTRONICS

As demands for faster electronic circuits have challenged industry scientists and designers, researchers at the NSA and its associated Laboratory for Physical Sciences have been pioneers in microelectronic device manufacturing and semi-conductor materials. Groundbreaking research has resulted in manufacturing techniques for advanced photonic logic devices, radio frequency absorbing printed circuit board technologies, flexible organic circuit manufacturing, integrated circuit laser devices, and many other technologies.

Technologies available for license include wafer fabrication methods, specialty electronic circuits, methods to view magnetic patterns on magnetic media, and novel circuit board technologies.

Fabricating a Flexible Organic Integrated Circuit

Patent Nos.: 7,452,746 / 6,013,534 and 6,017,822



This invention is a method of fabricating flexible organic integrated circuits (ICs) such as flexible substrates used for large area displays, identification tags, electronic paper, etc. In addition, this technology is useful for fabricating flexible ICs which have irregular shapes such as outer perimeters of varied slopes and angles as well as high temperature flexible ICs.

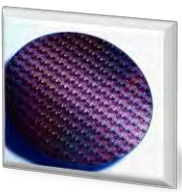
With this technology, a rigid substrate, such as a silicon wafer, has alternating layers of thin film conductors and dielectrics attached to form a High Density Interconnect (HDI). Organic transistors are then fabricated and connected to the HDI. Next, the rigid substrate and the flexible substrate are bonded to a handle wafer. The rigid substrate is removed and the organic IC is released from the support to yield a flexible IC, or it may be left on the support for shipping or for further processing.

VALUE

Fabricating flexible ICs with irregular shapes
Fabricating high temperature flexible ICs

Fabricating and Integrating Decoupling Capacitors

Patent No.: 7,297,613



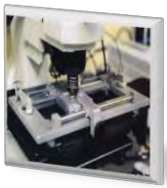
This technology provides a method of fabrication and integration for high quality decoupling capacitors with high capacitance values, low parasitic losses, good yield, and long-term reliability. This method enables high-yielding capacitors and other passive elements to be placed very close to the processor or other integrated circuit design and provides improved signal integrity.

VALUE

Reduced signal loss and footprint
Reduced cost and increased yields for RF systems

Fixture for High-Resolution Imaging of Magnetic Media

Patent No.: 7,239,332



This invention is a device to view different areas of a magnetic pattern recorded on magnetic media and to spatially relate one view with another. It also provides a method to view a magnetic garnet film after the magnetic pattern is transposed onto the magnetic garnet film.

This technology uses air pressure in a bladder to push the magnetic media firmly against the garnet. This avoids problems with non-uniform contact and provides a means of obtaining good garnet image quality over a field of view equal to the garnet dimension. Operationally, the garnet imager is more efficient to use than a magnetic particle fluid, since no advance preparation of the solution is required, no drying time is required, and there is no contamination of the material under investigation.

VALUE

Applies uniform contact between media and garnet
No advance preparation of fluids

Reverse Engineering Integrated Circuits

Patent No. 7,183,123

Integrated circuit (IC) analysis imaging techniques are used during failure analysis and typical methods include collection and analysis of emitted radiation, electron microscopy, or conventional optical imaging. Backside imaging allows enhanced viewing of the interconnects, which reside at the lowest level of the chip. Interconnects are a frequent source of failure in an integrated circuit and clear inspection greatly reduces the number of defective parts.

This invention allows a clear image of the components of an IC to be obtained without adding elements to the backside of the processed IC and also allows analysis by multiple conventional imaging techniques.

VALUE

Upper layers of metal do not need to be removed
Layers can be imaged without staining

Surface Preparation and Imaging for Integrated Circuits

Patent No: 7,019,530

The difficulty in performing failure analysis or reverse engineering on an integrated circuit (IC) is obtaining a clear view of the components of the circuit. To achieve this, most modern systems attempt to obtain a clear image of the top side of the IC through light emission or a combination of optically obtained images and emitted images. This invention provides a semiconductor analysis technique that allows a clear image of the components of an IC to be obtained from the top side of an IC device after backside processing and that allows analysis by multiple conventional imaging techniques.

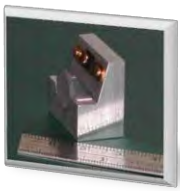
With this method, a substrate is selected and an opening is cut to fit the IC to be analyzed. An adhesive film is applied to the top surface of the first substrate. An IC is inserted into the opening and attached to the bottom side of the adhesive film. Next, the first substrate and IC are bonded to a second substrate. The bottom side of the first substrate and the IC are thinned until the substrate wafer is removed. A handle wafer is attached to the bottom of the first substrate. The second substrate is then removed and thinned and an analytical imaging technique is performed on the IC from the top side of the first substrate. The first substrate and IC are processed to a user-definable level.

VALUE

Supports clearer, multiple top-side imaging techniques
Provides more accurate failure and operational analysis

Forward Scattered Electron Image (FSEI) Sample Holder

Patent Nos.: 7,005,652 and 6,777,678



This technology is a combination of two patents. The FSEI sample holder is a method that brings Transmission Electron Microscope (TEM) quality to the less expensive Scanning Electron Microscope (SEM) by providing information about the sample that is both surface sensitive and very high resolution. This new technology enables more high-resolution imaging on a general category of samples and eliminates the need for additional hardware at a tremendous cost savings.

This technology uses an angled sample holder and a two-stage reflector to obtain a perspective view of the sample. A perspective view allows details along the edge to be imaged. Furthermore, the high tilt angle causes as many as 50% of the high energy electrons to be forward scattered off the surface of the sample. These electrons carry high resolution and surface sensitive information.

VALUE

Produces image resolution at the 1.0 nanometer range
Requires no additional detector hardware

Timer Circuit Utilizing Thermal Effect

Patent No.: 6,498,770

This technology is a timer circuit that utilizes the thermal runaway effect. The timer circuit includes a switch, resistor, transistor and protective device. When current flows through the first terminal of the transistor, current begins to flow through the second terminal. This current heats the transistor and increases its gain and leakage current. The increased gain causes a higher current to flow through the second terminal which heats the transistor further. This cycle eventually activates the protective device, which both acts as the time indicator and disconnects the power to the transistor to protect the transistor from damage.

VALUE

Replaces digital timer circuits
Less complicated and more reliable than prior methods

Recovering a Gate-Level Netlist from a Transistor-Level

Patent No.: 6,190,433

Various tools have been created to quickly analyze an integrated circuit (IC) based on a transistor-level netlist and layout of the IC. In many instances, however, the layout of the IC is not available. There is a need for a method of recovering a gate-level netlist from a transistor-level netlist of an IC where layout information of the gates included on the integrated circuit is unknown.

This method recovers a gate-level netlist from a transistor-level netlist description of an IC where layout information for the gates contained in the IC is not known. This is accomplished by comparing a functional description of every gate function of interest to a functional description of a set of connected components selected from a transistor-level netlist. Different circuit implementations of a particular gate function may be recovered using a single functional description of the gate function in question.

VALUE

Provides high-level abstraction to describe ICs
Recovers netlist where gate layout information is unknown

TTP

"Federal technology transfer exists, in part, to provide a return on investment for tax payers."

NETWORKING

As U.S. Government data networks and systems continually come under attack from countless cyber threats the NSA, in its mission to secure our infrastructure, has to stay one step ahead of thousands of foreign adversaries. Network penetrations, denial of service attacks, data traffic interceptions, and rerouting are just a few of the challenges facing agency engineers and scientists on a daily basis. As a result, the NSA has developed some of the world's leading network security capabilities.

Networking technologies that are available for license include advanced firewall technologies, multiple level minimum logic networks, traffic monitoring as well as inter-network data transport, secure file transfer, and network address location methods.

MESH NETWORK ROUTING (PULSE)

PATENT NO.: 8,443,105

This invention provides a method to characterize the physical layer capabilities of the device in one simple measure to dynamically decide the best route based only on the potential health of the next hop neighbor. Once a pressure value for each router node is determined, traffic is sent to the neighboring node with the lowest pressure value. With PULSE, routing decisions are distributed to individual nodes on a next-hop basis eliminating the need to determine the full path through the network. This method drastically reduces the number of messages needed to route packets and the amount of information maintained by each node.

VALUE

Significant throughput improvement
Ability to make best routing decision

MAKING ELEMENT APPEAR IN SHORTEST NETWORK PATH BY MINIMAL DECREMENTS AND INCREMENTS

PATENT NO.: 8,233,397

In telecommunication networks, it is often desirable to change the link weights to engender path changes in a certain desired fashion. For example, a high-capacity link might suddenly become available over which the traffic between the given source-destination pair of an important customer might need to be rerouted to alleviate congestion on the current route.

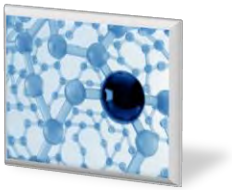
This invention is a device for and a method to identify the minimum set of links in a network and the minimal decrements and increments to the link weights so a node or link that does not appear in the shortest path of the unmodified network appears in the shortest path of the modified network.

VALUE

Minimizes weight changes (decrements and increments)
Reduces implementation time of network link weight changes

Reliably Communicating via Computer Network

Patent No.: 7,743,122



Network communications continue to experience interruptions in data delivery due to the lack of availability or bandwidth in a channel. This invention increases the reliability of network communications by adaptively constraining the routing of communications within a network.

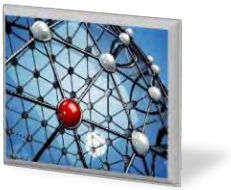
This technology identifies the hub and leaf nodes in a network. By communicating between the hub and leaf nodes, and between hub nodes, a leaf node can be re-designated as a hub node if the leaf node identifies a region of the network not known by a hub node. In addition, a hub node can be re-designated as a leaf node if the hub node becomes redundant. All re-designations are based on node statistics consisting of number of neighboring nodes, amount of node uptime, number of neighboring nodes plus amount of node uptime, and node processor speed.

VALUE

Adaptively constrains routing of communications within a network
Able to re-designate leaf nodes as hub nodes as needed

Establishing & Updating Master Node in Computer Network

Patent No: 7,738,504



In cluster type networks, a master node typically controls decision making and tasks non-master nodes. A master node may malfunction, or a node may be added to a network that is more suited to be the master node than the designated master node.

This technology establishes and updates a master node in a computer network by scoring each node based on its physical attributes. The highest scoring node is designated as the master node. The master node sends messages, including its score, to non-master nodes requesting each non-master node score. If a non-master node has a higher score, it requests the master node relinquish its master node status.

VALUE

Does not require global administrator
Uses scoring to determine master node instead of field comparison

Firewall for Processing a Connectionless Network Packet

Patent Nos: 7,073,196 and 6,141,755

Some networks combine IP and ATM by transmitting IP packets over ATM channel commonly referred to as IP over ATM. The IP packet is divided into segments and then made part of an ATM data segment. Combining the capabilities of an ATM firewall with those of an IP firewall does not, necessarily, yield a more efficient or more secure firewall for an IP over ATM network.

This invention is a secure, efficient firewall that applies a security posture to connectionless IP data packets transmitted over a connection-oriented ATM network. This invention allows a connectionless packet access to a network, where the connectionless packet is compared only once, if at all, to a database containing access rules. Each allowance or denial is recorded, and a system administrator is alerted if denial or threshold limits are exceeded.

VALUE

Packets only require first time comparison to acceptance rules database
Provides maximally efficient firewall

Multiple Level Minimum Logic Network

Patent Nos.: 7,068,671 and 5,996,020

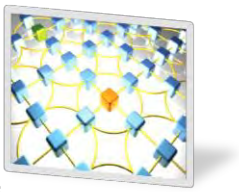
This technology is a multiple level, minimum logic network interconnect structure with high bandwidth and low latency. This structure utilizes a data flow technique based on timing and positioning of messages communicating through the interconnect structure. Switching control is distributed throughout multiple nodes so that a supervisory controller providing a global control function and complex logic structures are avoided. The interconnect structure operates as a "deflection" or "hot potato" system in which processing and storage overhead at each node is minimized. Elimination of a global controller and buffering at the nodes greatly reduces the amount of control and logic structures in the interconnect structure, simplifying overall control and network interconnect components and improving speed performance of message communication.

VALUE

Eliminates global controller and buffering at the nodes
Simplifies overall control and network interconnect components

Acknowledging Receipt of Data Packets

Patent No.: 6,957,374



This invention is a method of reassembling, acknowledging, and transmitting data packets by accounting for the received packets in groups rather than individually. The groups may be comprised of received data packets or gaps in the received data packets. Both groupings provide a more efficient way of processing data packets.

An acknowledgement message is returned to the sender which lists the gaps in the stored data packets. Efficiency is increased by identifying each gap by identification number rather than enumerating each individual missing packet. These steps are repeated for each additional data packet received. This method also drastically reduces the work required at the receiver to reconstruct these vectors, replacing matrix multiplies by mere substitutions. It can efficiently recreate the rest of the extended hamming code to reference all of the required lattice points.

VALUE

Higher transmission efficiency
Enables faster message reassembly

Geolocating Logical Network Addresses

Patent No.: 6,947,978

This technology provides a method for determining the physical location of network hardware using a logical network address on a nonlinear electronically switched network evolving in real-time without reliance on time-distance correlations.

Unlike more familiar geolocation methods such as direction finding or triangulation, this method uses the latency of communications to and from an Address to be Located (ATBL) to determine its location. This method creates a network latency topology map which is mapped by measuring the round-trip latency between one or more network stations of known location and many network endpoints, which can themselves be network stations, of known location.

VALUE

Geolocation can't be spoofed by user/operator at ATBL
Does not require software loaded onto endpoints at ATBL

FILTER SYSTEM FOR INFORMATION NETWORK TRAFFIC

PATENT NO.: 6,385,205

Various hardware-only and hardware and software combination devices are known for directing packets throughout a network system. A number of these devices are designed to optimize the performance of the network by evaluating packets and either determining a specific destination, or providing a filter, to only pass designated packets. The technology presented here is a hardware-only filter for controlling data packet traffic. The filter consist of a grid system with columns and rows and a grid populating device that inserts binary numbers that are the comparison between an incoming packet and the column and row headers of the grid.

With this technology, a converter breaks down data packets into eight-bit octets that are identified and placed in the column headers of the grid. Predetermined row header information is placed in the row headers. Next the row and column headers are compared to produce positive and negative binary numbers in the event of a match and a non-match, respectively. These numbers are placed in the grid squares by the grid populating device as controlled by the offset positioning means. Next, determine if any column is all ones. If so, the data packet is released from the memory device where it was temporarily stored. If no column is all ones, the data packet is cleared from memory.

VALUE

Selects desirable packets from traffic with hardware-only device
More efficient than software packet handling

OPTICS

In order to satisfy the demand of increasingly fast encryption, switching, and data processing systems, optical switching and transmission methods continue to evolve. The NSA has been at the forefront of many of these technologies and agency scientists have developed numerous optical data transport methods and devices. These technologies have included methods of manufacturing advanced integrated circuit waveguides, photonic logic devices, optical filters, and optical signal modulation devices.

Optical technologies that are available for license include optical bandpass filters, optical switches, modulators, optical clock recovery, and beacon authentication methods.

Low-Loss Fiber Chip Alignment

Patent No.: 7,128,476

This invention is a method of aligning optical fiber to a photonic integrated chip that results in lower back reflections, lower insertion losses, easier alignment, and a more rugged package.

With this technology, a thermally formed spherical lens is attached to the end of the fiber and a via is etched along a side of a photonic chip preferably a tetrahedral, conical, or pyramid aperture. The spherical lens is then inserted into the via and the optical device is aligned with each via. Alignment of the lens and via is performed using conventional means. Next, an anti-reflection coating is applied to the end of the optical device abutting the via and spherical lens. An index matching fluid is applied to each lens. Finally, the lens is connected to the via using conventional means such as UV curable epoxy.

VALUE

Easily scalable
Inexpensive implementation

Optical Clock Recovery Device Using Non-Linear Optical Waveguides

Patent No.: 6,701,049

Transmission of data over long fiber links results in timing jitter, which is a major signal degradation problem. The timing jitter refers to a random variation of the pulses' arrival time at the receiver, and it can be on the order of a pulse width. This jitter may cause slight changes in the repetition rate of the data at the receiver. Therefore, at a node or a receiver, the timing of the data needs to be extracted and synchronized with a local clock that in turn drives the data processing devices, which perform other signal processing operations, such as demultiplexing or optical signal regeneration. This extraction of the data timing at the receiver is called clock recovery. As optical data transmission speeds approach 100 gigabits per second, a phase noise yielding less than one picosecond of clock timing jitter is required.

The invention presented here provides an all-optical timing extraction device using the non-linear characteristics of optical waveguides for counter-propagating pulses. In addition, the invention provides an all-optical timing extraction device that can resolve timing delays between pulses on the order of a few picoseconds.

VALUE

Resolves timing delays between pulses to two picoseconds
Bit-rate flexible, all-optical timing extraction device

TENSION-TUNED ACOUSTO-OPTIC BANDPASS FILTER

PATENT NO.: 6,647,159

Typically, wavelength sensitive optical switches are used for wavelength division multiplexed (WDM) signals because the wavelength separation between channels is small. In the case where a narrow, optical band of traffic carried by a specific wavelength of a multi-wavelength signal needs to be separated from the rest of the traffic, a wavelength-sensitive optical switch can be implemented at considerable cost savings.

This invention is a device that allows one or more bands of optical wavelengths to be selected for further transmission. All light within the optical bandwidth of operation is first coupled from the core mode of an optical fiber to a specific cladding mode by a chirped broadband cladding mode coupler. These cladding mode light waves then enter a narrow-band core mode coupler whereby selected optical bands of wavelengths, tuned by the tension on the optical fiber, are re-coupled back into the core of the optical fiber. The chirped broadband cladding mode coupler is isolated from the narrow-band core mode coupler by an acoustic absorber to limit the acoustic interaction between them.

VALUE

Able to select one or more channels to pass through the filter
Broadband cladding and narrow-band core mode coupler isolation

Chirped Fiber Acousto-Optic Bandpass Filter

Patent No.: 6,580,841

With Chirped Fiber Acousto-Optic Bandpass Filters, all light within the optical bandwidth is first coupled from the core mode of an optical fiber to a specific cladding mode within a chirped broadband cladding mode coupler. A selected RF frequency of a flexure wave, induced by an acoustic wave amplifier and acting on a chirped region of fiber, couples all light within the optical bandwidth from the core mode of the optical fiber to a specific cladding mode. The cladding mode lightwaves enter a narrow-band core mode where selected frequencies of flexure waves, induced by a second acoustic wave amplifier, re-couple selected bands of wavelengths back into the core mode. As a result, the device uses less power and allows individual control of multiple acoustic signal strengths and frequencies, efficient coupling of all optical traffic for selecting individual optical channels, and changes to the strength or magnitude of optical signals by varying the frequency.

VALUE

Does not require core-block and more power efficient
Multiple acoustic signals with controllable strengths and frequencies

Acousto-Optic Bandpass Filter

Patent No.: 6,556,729

The acousto-optic bandpass filter is a device where one or more wavelength bands may be selected for further transmission. In this device, all light within the optical bandwidth of operation is first coupled from the core mode of an optical fiber to a specific cladding mode by a long-period photo-induced grating. These cladding mode light waves then enter an acousto-optic interaction region where selected RF frequencies of flexure waves, induced by an acoustic wave amplifier, re-couple selected bands of wavelengths back into the core mode.

VALUE

Lower optical losses
More versatility and reduced power consumption

All-Fiber Optically-Controlled Optical Switch

Patent No.: 6,081,634

Optical switches are typically controlled by electro- or acousto-optic techniques such as surrounding the waveguides with electro- or acousto-optic material to control the coupling between the waveguides.

This invention utilizes two waveguides controlled by a third waveguide. The waveguides are in the same plane and the third may be an optic fiber or slab waveguide. The first and second waveguides are close enough to exhibit evanescent wave coupling and the propagation constant is identical. The second waveguide is positioned closer to the third optical waveguide. Switching between the first and second waveguides occurs when the propagation constant of the third is changed optically.

VALUE

Avoids switch-fiber coupling issues (i.e. incompatible modal fields)
Significantly reduces reflection losses

SECURITY

The NSA has invented some of the modern world's most ground-breaking data and device security technologies. These technological breakthroughs have included methods of encryption and decryption, physical security devices, network intrusion detection, as well as secure computing and data transfer methods.

The NSA has numerous security technologies available for commercialization including methods of generating cryptographic keys, digital signature validation, secure computing technologies using virtual machines, and wireless intrusion detection methods. Additional technologies available include physical security apparatuses such as tamper evident cargo seals and reusable tamper evident shipping packages.

Image-Based User Authentication

Patent No.: 8,655,027

This invention is a method of authenticating a computer user so that authentication cannot be compromised by either keystroke monitoring or looking over the shoulder of the user. With this method, an image is captured of the user and assigned a username. The user selects an image category, two or more patterns, facial location, and rotation value.

When a user logs into the system, the system presents a series of images. The user selects an image and system projects the image onto the face at the selected rotation. The system captures an image of the user's face with the rotated images and authenticating the user if the facial features match and the pattern images match.

VALUE

Authentication not compromised by key logging or visual surveillance
User selectable image categories and pattern images

Detecting SIM Card Removal and Reinsertion

Patent No.: 8,478,340

Methods exist for identifying when an unauthorized user attempts to use someone else's electronic device using the unauthorized user's SIM card. However, there is a need to detect misuse of a valid SIM card with an electronic device for which the SIM card was intended to be used.

This technology is a device for and method of determining if a SIM card was removed and reinserted into a device by an unauthorized person. After initially inserting a SIM card into a device, this technology monitors any SIM card removed and reinserted and an indicator on a graphical user interface reports the removal and re-insertion to the user.

VALUE

Detects misuse of a valid SIM card by unauthorized person
Alerts user of SIM card removal and reinsertion

USB and Data Port Protector

Patent Nos.: 8,449,309 and 8,414,314

Increasingly, universal serial bus (USB) ports are becoming the preferred method to maliciously extricate data or infiltrate malicious software into a computer system. As a result, the need to secure USB ports from unauthorized access is becoming a priority for system administrators and security personnel.

This technology consists of two patented devices (reusable and single use) that provide a simple method for blocking access to a USB port. The reusable USB Port Protector consists of one tabular plug and a matching shim that are inserted into the port. The lower shim is inserted first and then the upper tab is inserted. When the two are mated together, a security wire can be inserted through a hole in each preventing the two pieces from being separated. Projections on the lower shim, prevent the assembly from being removed blocking access to the port electrical connections.

VALUE

Quick, easy, two-part installation
Reusable and one-time use models

Reusable Tamper Evident Bag Closure

Patent No.: 8,196,442

This invention is a device that can maintain the chain of custody so as to provide the user with the assurance that the information being protected has not been compromised.

This tamper-evident bag closure is defined by a lid with multiple hasps and a base with knobs that attach to the bag. The bag is secured by a locking mechanism placed through an opening on the base and inserted within an insertion aperture. When the mechanism is locked, the lid slides into alignment with the base and engages the plurality of hasps with the plurality of knobs, thus securing the bag.

VALUE

Multiple bag closure options
Multiple tamper-indicating features

Reusable Tamper Indicating Tube

Patent No.: 8,177,089

The present invention is a reusable tamper indicating transport tube that can be used to securely transport large drawings and other documentation without damaging or distorting them.

The tamper-evident tube consists of an outer tube with cap, an inner tube with cap, an inner tube locking mechanism, and an outer tube locking mechanism that is affixed to the peripheral surface of the outer cap.

VALUE

Provides secondary level of service
Visually verify evidence of tampering

Tamper Evident Cargo Seal

Patent No.: 8,052,180

This technology is designed to protect cargo shipments from tampering, shrinkage, counterfeiting, and introduction of hazardous material.

This invention secures access using a hasp closure method. The free end of the cargo-seal strap is wrapped around the hasp, positioned, and inserted as a pin through the opening into the body of the serialized device. Two blanks are inserted, blocking the pin opening, and preventing the pin's release from the body.

VALUE

Requires no special mounting hardware
Provides visual tamper indication

Providing a Computer User with High-Level Priviledges

Patent No.: 7,945,947

This invention monitors all terminal sessions in an operating system, such as Microsoft's Windows®, for a special key sequence and if found, launches a command shell running with high privileges for use by the logged-on user, regardless of which user it was and without requiring subsequent authentication.

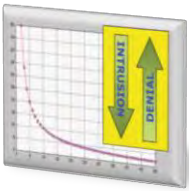
The advantage of this method is that it allows any user to launch a command shell with high privileges even though the user may only have few privileges, and does not require a login with a username and password to be entered each time.

VALUE

Allows user to launch privileged command shells
Simple command for authentication reduces user input

Assessing Security of an Information Access System

Patent No.: 7,895,659



This method objectively assesses the security of an information access system by estimating the total vulnerabilities of a system protected by multiple verification mechanisms.

With this method, verification mechanisms are selected and an error tradeoff plot showing false acceptance rate versus false rejection rate for each mechanism is estimated. Next, a corresponding false acceptance rate and false rejection rate pair from each error plot is estimated. Combining the false acceptance rates help determine intrusion protection and combining the false rejection rates helps determine denial protection. The final estimation of system vulnerability is derived from the combination of the error tradeoffs for each specific verification mechanism.

VALUE

Provides objective security measure of information access system
Eliminates the need for subjective system security judgments

Accelerated Batch Digital Signature Verification

Patent No.: 7,890,763

High speed processing of digital signatures commonly starts with group/batch processing until a failure occurs, at which point the process slows until bad signatures are segregated from the remainder of the batch.

This technology provides three new batch verification methods of identifying invalid digital signatures from a group that are faster and more efficient than existing divide-and-conquer methods.

VALUE

Up to 94% speed improvement
Tuned to work with groups and error rates of any size and percentage

Authenticated Cryptography

Patent No.: 7,827,408

Message encryption and authentication are typically performed separately. In other words, a message is encrypted using one method and then a cryptographic hash of the message is generated using a second method.

This invention is a device for and method of encrypting and authenticating a message and authenticating any additional information. The present invention provides a cryptographically stronger authentication method and is more efficient to implement, than the prior art.

VALUE

Provides combined authenticated encryption in efficient manner
Does not require random numbers, two encryption keys, or checksums

GENERATING AND DISTRIBUTING STRONG DES KEYS

PATENT NO.: 7,657,030

Data Encryption Standard (DES) is an encoding, or cryptographic algorithm which requires a cryptographic key that is 64 binary bits in length. DES uses the same key for both encryption and decryption. Such a key is commonly referred to as a symmetric key. Each 64-bit DES key consists of 56 randomly generated bits and 8 parity bits. The present invention is a method of generating strong DES cryptographic keys in a manner that does not require checking for parity or weak keys.

With this method, all possible hex values are generated. Next, all possible two-hex value combinations are generated, where one of the two-hex values has odd parity and the other even parity. Then, eliminate values E0, 01, F1, FE, 1F, 0E, 1E, and 0F. Next, arrange each remaining two-hex value combination once in a user-definable order, such that the hexadecimal values alternate even and odd parity. Then, select eight unique two-hex value combinations in a user-definable manner. Finally, use the selected eight two-hexadecimal value combinations as the DES cryptographic key.

VALUE

Does not modify key, select key based on time periods, or use double keys
Does not require a check for parity or weak keys

TAMPER PROTECTION FOR LOCKING MANHOLE COVERS

PATENT NO.: 7,607,858

Modern telecommunications equipment is increasingly utilizing underground vaults and conduits that are accessible by sealed manhole openings. Typically, the manhole opening consists of an annular frame attached to the telecommunications vault below grade.

This invention is a locking device that improves the security of certain telecommunications vault manhole cover systems. The operation of this improved security saddle differs from the prior technology in that the padlock and the tamper evident device can now be mounted below the lockbar. The lock and device can now be mounted in a way that they cannot be damaged.

VALUE

Protects padlock from damage
Protects tamper indicating products

Reusable Tamper Evident Bag

Patent No.: 7,350,689

This invention provides the user with the ability to initiate roundtrip courier services without including supplemental supplies or complex procedures. The dual-seal characteristic of this container allows items to be outbound couriered, its primary seal to be inspected and certified by its recipient, and a return trip to be initiated using its secondary seal.

Receipt tags are also provided to authenticate the bag upon inspection, which may very well constitute the entire contents of the return shipment in certain certified shipments.

VALUE

Allows seal inspection, opening, and resealing for return shipping
Provides authentication of contents during each shipment

Reusable Tamper Indicating Security Device

Patent No.: 7,201,410

This invention allows the use of labels where labels have not been an acceptable method of tamper technology by permitting labels to be used on surfaces that normally do not work well with a pressure sensitive label.

This device is a scalable unit designed to provide a disposable, smooth surface to affix tamper-indicating labels. The fixture consists of two base units with disposable blanks in each.

VALUE

Mounts to surfaces that typically will not accept a label
No need to remove adhesive residue from previous labels

SECURE VIRTUAL MACHINES (NETTOP®)

PATENT NO.: 6,922,774

Public and private executives and IT managers are acutely aware of the risks in allowing their users access to proprietary, sensitive, or otherwise classified information, and access to the Internet from the same device.

NetTop® significantly reduces these risks and recurring IT investment by allowing a user secure simultaneous access to multiple networks or environments independent of the operating system or user applications. Users seamlessly "window" across multiple environments or networks accessing the same information and applications. Each network or environment and its data is securely isolated from the other without the need for multiple workstations at the end-user's location.

VALUE

Reduces complexity of required equipment and multiple machines
Centralized security functionality

SELF-AUTHENTICATING CRYPTOGRAPH APPARATUS

PATENT NO.: 6,912,284

Autokey encryption refers generally to a substitution cipher in which the key, following application of an initial key, is determined by preceding elements of the key or cipher. In an autokey encryptor, each key bit generated is a function of one or more prior key bits. The key in a cipher text autokey encryptor is a function of a prior sum of key and plain text bits.

This invention provides an enciphering/deciphering system incorporating a linear sequence generator and providing encipherment and authentication in a single process, comprising self-authentication capability while providing authentication without the need for a parity check code. The result is an improved autokey cipher utilizing infinite error extension while also possessing a high degree of cryptographic security.

VALUE

Reduces complexity of required equipment
Provides message authenticity with a low probability of error

SHREDDER RESIDUE DISPERSION SYSTEM

PATENT NO.: 6,820,830

Most paper destruction devices in use today operate using paired rotary cutting elements and fall into one of three categories: strip cutter, the most basic type of shredder, where the paper is cut into strips; cross cutters, where the paper is cut both in-line with the direction of insertion into the shredder and across that dimension; and disintegrators, which have sets of rotating cutting elements that simply randomly cut the paper until the shredded pieces are small enough to be able to fall through a screen below the cutting elements.

This method provides a shredder residue dispersion system where shredder residue from each document shredded is directed into multiple residue receptacles for separation of the document residue to thwart reassembly. The system increases the security of a standard shredder by dispersing the shredded paper into multiple bins on a continuous basis. This ensures that no one document will be complete in any one residue bag.

VALUE

Increases the security of a standard shredder
Ensures no one document will be directed to one residue bag

> "One driver of successful innovation is technology transfer, in which the private sector adapts federal research for use in the marketplace."

Presidential Memorandum, *Accelerating Technology Transfer and Commercialization of Federal Research in Support of High-Growth Business*

Method of Verification Using a Subset of Claimant's Fingerprint

Patent No.: 5,982,913

Fingerprint verification is different from fingerprint identification. In a verification system, the claimant claims to be a particular person and the claimant's fingerprint is compared against the fingerprint of the person the claimant claims to be.

This invention is a fingerprint verification method where a claimant claims to be a certain individual, who has previously enrolled in the system, and a portion of the claimant's fingerprint is compared against the entire fingerprint of only the enrollee the claimant claims to be. A portion of the claimant's fingerprint is divided into a number of segments and information from only a user-definable number of segments are used to determine whether or not a match exists. A Fast Fourier Transform is used to speed-up the comparison process.

VALUE

Captures portion of fingerprint and compares it to entire fingerprint
Segments fingerprint and only compares to claimed individuals

Port Protector Assembly for D-Sub Connectors

Patent No.: D662,894

This design patent is for a port protector assembly for D-sub connectors. The assembly consists of an inner cover affixed to the connector screws and an outer cover affixed to the inner cover with a security wire or other device.

VALUE

Easily installed, two-piece construction
Security wire prevents removal

SIGNAL PROCESSING

As the nation's primary signals intelligence organization, the NSA has been a leader in signal processing since the 1950s and many of the digital signal processing technologies commonly used today originated from research conducted by agency scientists. The NSA was responsible for many of the audio and video signal processing technologies as well as satellite communications methods.

Signal processing technologies available for license include transmitter location methods, range limited antenna, noise reduction techniques, amplification, frequency estimation, and signal decoding methods.

INFINITE IMPULSE RESPONSE RESONATOR DIGITAL FILTER

PATENT NO.: 8,396,912

With the need for efficiency in representing cochlear hair cells, the use of an Infinite Impulse Response (IIR) resonator digital filter is preferred over the Finite Impulse Response (FIR) filter. Unlike FIR, an IIR filter provides for computational efficiency and meaningful immediate output following a one cycle initialization (i.e. no staging delays) when given an input.

This invention is an IIR resonator digital filter that is more efficiently implemented than existing IIR filters and is suitable for biomimetic voice identification systems.

VALUE

More efficient than existing IIR resonator digital filters
Can be utilized in a biomimetic voice identifier

COHERENT DEMODULATION OF GMSK-AIS SIGNALS IN CO-CHANNEL

PATENT NO.: 8,275,077

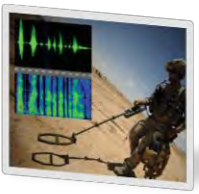
This invention improves demodulation of Gaussian Minimum Shift Keyed (GMSK) and does not require preamble codes or an equalizer. In this method, a carrier frequency of a received signal (having a carrier residual) is estimated, the signal is basebanded, the signal's carrier frequency is tracked, and the carrier residual is then removed. Next, a data burst is detected and a bank of poly-bit matched filters is generated and applied to the signal. A magnitude and phase of each filter output is determined. A maximum magnitude is determined, a baud center is located, and correlation signals are generated by applying the filters at the baud center. Finally, a carrier phase is estimated and removed, a Viterbi decoding algorithm is applied to the signal, and the transmitted data sequence is estimated.

VALUE

Reduces error rate
Enhanced signal quality

Determining a Coherence Measurement for a Digital Signal

PATENT NO.: 8,200,731



This technology uses alternative methods to exploit different signal features and does not require thresholds to obtain coherence figures-of-merit. Since a sinusoidal waveform of a single frequency is perfectly coherent, it serves as the 'gold' standard. Time dependent signals used in tracking radar systems, laser ranging, sonar processors, and imaging systems can all benefit from the methods in this patent for both enhanced detection of targets and removal of unwanted artifacts or false alarms. This technology has been demonstrated on output from various metal detector products and shown to reduce the number of false positive results.

VALUE

Intuitive user interface
Device agnostic

Geolocation

PATENT NO.: 7,893,875

The present invention improves upon the prior art with a method to process large-length, wide-band signals without losing precision and processing complex-valued signals.

This method utilizes two receivers, in motion, that receive a signal from the transmitter. The signal is digitized and the receivers convert the digitized signals to complex-valued signals. Transmitters on the receivers transmit their digitized signals, locations, and velocities at the time the signal was received at the processor. The processor then determines the difference in radial velocities of the receivers relative to the transmitter. This difference in radial velocities and delay time between signals is used to geolocate the transmitter.

VALUE

Not dependent on calculating complex ambiguity functions (CCF)
Increased precision

Determine Range and Velocity of an Object

Patent Nos.: 7,755,536 and 7,545,325

This method provides the ability to determine the position and velocity of a transmitter over a wide range of bandwidths. The second invention models the Doppler process as a time shift and change of scale of the original signal. In this process, the received signal is delayed in time and dilated. In this invention, the method of performing the resampling function is to apply a forward Fourier transform of one length to the zero-padded signal and apply an inverse Fourier transform of a different length to the results of the first transform. This pair of operations results in a resampling of the signal at a rational multiple of the original sample rate. The scale correlation is then computed as the normal correlation of the transmitted signal and the resampled signal.

VALUE

Accurate model of Doppler process
Rational signal resampling

Decoding Signals Having Binary BCH Codes

Patent Nos.: 7,734,991 and 7,694,207

This invention is a method of correcting a received communication signal by rapidly computing syndrome sequences for binary BCH codes. The present invention speeds up the syndrome sequence calculation. An efficient binary matrix multiplication converts the syndrome into the syndrome sequence of the vector, with the extension field elements represented in terms of the power basis. This conversion matrix is easily derived from field multiplication and the coefficients of the generator polynomial alone.

VALUE

Reduces error-correction time
Increases efficiency in processing

Estimating Digital Signal Frequency

Patent No.: 7,715,996

This method estimates frequency without FFT or Hilbert transforms. The invention replaces the Hilbert by the simpler differentiation operation and orthogonality is established using Gram-Schmidt.

The received signal is segmented into a user selectable number of data blocks, which may be disjointed or overlapping. Tapering may also be applied to data segments using any of the known window tapers. For each data block, the signal is differentiated, and the Gram-Schmidt process is used to obtain orthogonality between a signal and its derivative. The phase is computed using the inverse tangent or the complex logarithm. Finally, the frequency is estimated by differentiation of the unwrapped phase. This invention improves the prior art by having all operations performed in the time domain and no filtering.

VALUE

More intuitive applications
Made-to-order design

System to Remove Noise and Interference from a Signal

Patent Nos.: 7,676,046 / 7,492,814 and 7,457,756

This method is a combination of three patented technologies. First is a method of calculating a joint time-frequency domain of the signal that preserves the phase information contained in the signal. This is critical for reconstructing the waveform after noise removal. The second technology further enhances the noise and interference removal system by concentrating a Short Time Fourier Transform (STFT) and estimating a noise and interference-free signal by integration. The third technology further adds a user-definable set of peak values in the concentrated STFT. Elements that do not correspond to the peak values are eliminated from the joint time-frequency domain resulting in a clean signal.

VALUE

Preserves the phase information contained in the signal
Allows reconstruction of waveform

RANGE LIMITED ANTENNA

PATENT NOS.: 7,642,986 AND 7,292,202

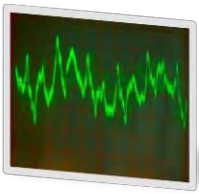
This device is a Range Limited Antenna (RLA) containing two or more antenna elements arranged in sets (A, B, etc.) and an RF signal processing network connected to paired sets of antenna elements so the antenna is sensitive (has gain) to signals within a Region of Interest (ROI) and insensitive (has attenuation) to signals outside the ROI. The elements are dipoles closely arranged to limit the signal time of arrival difference relative to the wavelength. The sets are widely separated. By examining the signal phase difference at the elements of the set A, which is related to the angle of arrival, and measuring the same signal phase difference in set B, a determination can be made of the approximate range of the signal source from the antenna array. The design allows adjustments to cut-off, radius-attenuation rate, frequency band, and sensitivity.

VALUE

Supports operating frequency range of 1MHz to 3GHz
Insensitive (has attenuation) to signals outside user selected range

ESTIMATING A HIGH FREQUENCY CARRIER SIGNAL

PATENT NO.: 7,444,128



The invention presented here is a novel method of estimating the carrier frequency of a high frequency (HF) single sideband signal from the structure of the underlying speech signal.

A signal is received, and divided into user-selectable time segments. A spectral peak vector is calculated by performing spectral estimation on the time segment divided signal. A first correlation vector is calculated on the spectral peak vector, and a second correlation vector is calculated from the spectral peak vector and the first correlation vector. The time average vector is appended with the result from the second correlation vector, and the process repeats for each time segment the received signal was broken into. The carrier is estimated using the most commonly occurring frequency in the time average vector.

VALUE

Accurate estimation and tracking of speech components
Unnecessary to process the entire time-frequency surface

Single Frequency Repeater

Patent No.: 7,346,311

This invention consists of a novel, single frequency repeater that retransmits a signal at the same frequency and higher power level. This technology also avoids problems with feedback and concurrent oscillation. The single frequency repeater is comprised of a backplane, receiving antenna, filter, amplifier, power supply, switch, and transmitting antenna. However, in this invention, the receiving antenna and the transmitting antenna are placed in each other's back lobe, with the transmitting antenna oriented in an orthogonal direction to the receiving antenna. This technology is very suitable for SCADA range extension applications, especially for large installations such as power plants and refineries. The technology can also be implemented into LAN repeaters and cellular applications.

VALUE

Control remotely
Adaptable to different locations

Estimating Signal Frequency

Patent No.: 6,577,968

This invention estimates a signal frequency using multidimensional FFT where the signal is converted to a row vector and segmented. Each segmented row vector is converted to a first matrix and each matrix entry is multiplied by a first weighting column-vector. An FFT is performed on each result. The process is repeated on a delayed version of the signal. Next, a complex conjugate is calculated for each result, a cross-spectrum matrix is formed, and a magnitude above a threshold is selected in the matrix. An angular frequency is set to either the phase of the selected magnitude, phase of the mean of the complex numbers in the row in containing the selected magnitude, or the selected magnitude. The frequency is then set to the estimated angular frequency divided by 2π and the signal delay period.

VALUE

Able to resolve multiple signals
Resolve signals separated by less than width of one transform cell

FEATURE EXTRACTION USING WAVELET AND FOURIER TRANSFORMATION

PATENT NO.: 6,385,543

Any unwanted component in a signal may be viewed as an interferer. To remove an interferer, the signal must first be expanded by methods such as Fourier transformation, Taylor series expansion, or wavelet transformation. An expanded signal is then modified to remove the interferer and the inverse of the expansion method is performed on the expanded and modified signal to obtain the original signal minus the interferer. This method removes at least one user-definable frequency from a signal in a manner that is, computationally, more efficient than prior art methods and may be applied to signals containing a number of samples that cannot be processed by prior art methods.

This invention removes a frequency from a time domain signal by reducing the samples in the signal by wavelet transformation, projecting the feature to be removed onto a wavelet basis using Fourier transformation, and subtracting the projection of the feature from the projection of the original time domain signal.

VALUE

More efficient frequency removal than prior methods
Can be applied to signals containing a number of samples

Converting Multiple Signal Types to NRZ Format with Automatic Self-Test

Patent No.: 6,246,348

Signals are transmitted in a wide range of formats, voltage levels, and speeds (e.g., digital, analog, TTL, MECL, T1, fiber optic, etc.). A signal in one format may be incompatible with a signal in another. Therefore, different procedures may be required to process different signal formats. Different procedures may require the use of different processing equipment. Such equipment may be expensive, and the operator may be required to receive extensive training in order to be able to operate the equipment.

This device converts data signals to NRZ format in one of a user-selectable signal formats, where the data signal is selected from RS232, RS422, sine wave, analog, TTL, LVDS, MECL, PECL, T1, E1, T2, E2, T1C, T3, E3, STM-1, E4, CMI, OC3, and fiber optic. This invention also converts data signals to NRZ format in one of a user-selectable output-signal formats consisting of RS422, TTL, LVDS, ECL, MECL, PECL, and DECL.

VALUE

Able to process multiple signals
Convert signals to NRZ format in user-selectable output format

Mechanisms for Transferring Technology

The NSA welcomes the opportunity to partner with industry, academia, and government agencies to support the mission of the NSA to extend its resources into private communities. In order to do this, the NSA TTP primarily facilitates the following types of agreements:

- Patent License Agreements
- Cooperative Research and Development Agreements
- Education Partnership Agreements
- Technology Transfer Sharing Agreements

PATENT LICENSE AGREEMENT (PLA)

WHAT IS A PLA

The PLA is a license granted by the NSA to a partner to commercially develop and market its domestic and foreign patents and patent applications. Using a PLA, the NSA grants its partner a non-exclusive, partially exclusive, or fully exclusive license to make, use, or sell the patented invention. In return, the partner typically pays a royalty back to the government and inventors.

HOW DOES A PLA WORK

When a patented NSA technology is identified by a licensee as having commercial potential, the licensee submits a satisfactory development and marketing plan. This plan outlines the licensee's approach to commercialization of the invention. The invention must be brought to market within a specified time period and the licensee must continue to make the benefits of the invention accessible to the public.

The PLA provides the private sector with the opportunity to commercially develop federally-funded research to promote economic growth and global competitiveness.

PATENT LICENSE AGREEMENT FEATURES

Benefits	Elements
Encourages commercialization of federally funded research in the private sector	Exclusive, partially exclusive, or non-exclusive license
Saves industry and academia the **cost and time** of conducting R&D	License duration, reporting period, fees, and royalty payments
Provides royalty income to the government and its inventors	Letter of Application and a Business Plan for commercialization and marketing the technology
Creates new industry and employment opportunities in the private sector	Federal Register notice posted by the NSA identifying invention, licensee, and type of license (exclusive and partially exclusive licenses only)
Maximizes the value of the NSA's R&D investment and resulting technologies	Public availability of invention within a reasonable period of time
Increases the awareness of market and technology trends and the needs of both industry and government	Government retention of irrevocable, royalty free, worldwide, government purpose rights to the invention

Cooperative Research and Development Agreement (CRADA)

What is a CRADA

The CRADA is a cooperative agreement between the NSA and industry, academia, non-profits, and state and local governments. These agreements leverage each party's resources in order to conduct research and development (R&D) that benefits both. Through this collaboration, each party shares the benefits and risks in obtaining valuable technology transfer goals and objectives.

How Does a CRADA Work

A CRADA allows both parties to leverage personnel, facilities, equipment, and other resources during collaborative R&D activities. The non-federal partner does not receive any funds from the NSA, but may contribute funds to the project. Under a CRADA, the government may grant the non-federal partner patent licenses for any invention developed under the agreement.

A CRADA provides the NSA and the collaborating partner the opportunity to engage in joint research and development efforts, sharing the risks and benefits.

Cooperative Research and Development Features

Benefits	Elements
Creates new products, processes, and intellectual property to meet mission and commercial goals	Legal and business framework for managing and executing the CRADA
Reduces research and development **costs and time**	Statement of Work (SOW) defining the nature and scope of the R&D to be conducted
Leverages external expertise, ideas, and resources	Estimate of resources to be used during performance
Provides a joint approach to solve specific problems by applying different cultural solutions	Financial obligations that specify what funds, if any, the partner will pay the NSA
Increases the probability of bringing **inventions to the marketplace**	Definition of any rights to patents, trademarks, or copyrights brought into or created from joint research performed under the CRADA
Increases the awareness of market and technology trends and the needs of both industry and government	Contact information for management and technical issues

EDUCATION PARTNERSHIP AGREEMENT (EPA)

WHAT IS AN EPA

The EPA is an agreement between the NSA and an educational institution to transfer or enhance technology and provide technology assistance to the institution. Under an EPA, the NSA scientists can provide training and mentoring to personnel in the science and technology fields. Also, the NSA may transfer or donate laboratory equipment to public and private schools.

HOW DOES AN EPA WORK

An EPA is normally initiated by an NSA sponsor who submits the education objectives for review. A task plan is developed in collaboration with the institution outlining the learning objectives and goals. These goals may be teaching, mentoring, training personnel, developing curriculums, or transferring equipment and technology. Once approved, both parties can begin executing the learning tasks.

An EPA allows the NSA to share its unique experience by providing training to personnel in the science and technology fields at all education levels.

EDUCATION PARTNERSHIP AGREEMENT FEATURES

Benefits	Elements
Involves students to ensure a **future resource** of scientists, mathematicians, and engineers	Intellectual Property rights to inventions created under the EPA
Provides **unique opportunities** for learning not available from other resources	Copyrights that explain the ownership of works of the partners
Provides **access to the NSA personnel** to teach courses and develop science curriculums	Protections given to proprietary information brought into an agreement and that which is developed under the agreement
Permits students and teachers to become involved in **developing useful technological applications**	Task Plan outlining the learning objectives and goals
Provides access to the NSA resources, either by loan or donation, which **relieves** institutions from some of the **financial burden of R&D investment**	List of any equipment or other property to be loaned
Improves community awareness of the NSA core values and enhances the reputation of the laboratory	

TECHNOLOGY TRANSFER SHARING AGREEMENT (TTSA)

WHAT IS A TTSA

The NSA has numerous patents, patent applications, and other intellectual property (IP) that it frequently transfers to other government agencies. The TTSA is an agreement between the NSA and another government agency that protects the NSA's rights to seek commercialization of technologies it owns and to effectively track the transfer of these technologies.

HOW DOES IT WORK

A TTSA is initiated by NSA government personnel for the recipient agency. Each TTSA includes specific language regarding non-commercialization and restricts the transfer for government use only. Contractors and other partners requiring technology in support of a contract must have their contract officer representative (COR) submit the request.

The TTSA allows the NSA to transfer technology to other government agencies while protecting its rights.

TECHNOLOGY TRANSFER SHARING AGREEMENT FEATURES

Benefits	Elements
Simplifies agreements that specify the purpose, terms, and conditions related to the technology transfer	Description of purpose
Facilitates easy transition of technology between U.S. Government agencies	Terms and conditions related to the transfer
Reduces recipient agency **R&D expenditures** by leveraging previous NSA investments	Non-commercialization language
Reduces development time of mission-specific technologies	Transfer restrictions for government only use

LEGISLATION

There are many laws that promote technology transfer and provide technology transfer mechanisms and incentives. The following are highlights of some of the federal legislation that apply to the NSA's TTP Program.

Stevenson-Wydler Technology Innovation Act of 1980

This act defines technology transfer and encourages federal laboratories to engage in cooperative research with private industry, state and local governments, academia, or nonprofit organizations. Its provisions also established and defined the basic activities of an Office of Research and Technology applications (ORTA) at each federal laboratory, and set aside a small percentage of each laboratory's budget to fund technology transfer activities.

Bayh-Dole Act of 1980

This policy permits small businesses, universities, and nonprofit organizations to obtain title to inventions developed with federal funds. This policy also allows the federal agency to retain an irrevocable license to use the invention. This policy permits federal laboratories to grant exclusive patent licenses to industry.

Federal Technologies Transfer Act of 1986

This act requires scientists and engineers to consider technology transfer an individual responsibility. It also enables federal labs to negotiate licensing arrangements for patented inventions and requires that federal inventors share in royalties from patent licenses. It establishes a charter and funding mechanism for the Federal Laboratory Consortium (FLC). The FLC is responsible for a variety of activities including providing training courses and assistance for technology transfer programs.

Executive Order 12591 of 1987

This order ensures that federal laboratories assist universities and the private sector by transferring technical knowledge. It also promotes commercialization of federally-funded inventions by requiring that laboratories grant contractors the title to patents developed with federal funds, as long as the government is given a royalty-free license for use.

15 United States Code, Section 3710A

When entering into a CRADA agreement, preference shall be given to business units located in the U.S. which agree to substantially manufacture products in the U.S.

APPENDIX A

ACRONYMS

The following is a list of acronyms used in this publication.

AMP	Analytic Metadata Producer
ANN	Artificial Neural Network
ATBL	Address-to-be-Located
BDD	Binary Decision Diagrams
CAF	Complex Ambiguity Functions
CNF	Conjunctive Normal Form
COR	Contract Officer Representative
COTS	Commercial-off-the-Shelf
CRADA	Cooperative Research and Development Agreement
DES	Data Encryption Standard
DoS	Denial of Service
EER	Equal Error Rate
EPA	Education Partnership Agreement
ESL	English as a Second Language
FFT	Fast Fourier Transform
FIR	Finite Impulse Response
FLC	Federal Laboratory Consortium
FM	Ferragina and Manzini (FM)
FPGA	Field Programmable Gate Array
FSEI	Forward Scattered Electron Image
GMSK	Gaussian Minimum Shift Keyed
GUI	Graphical User Interface
HDI	High Density Interconnect
HF	High Frequency

ACRONYMS, CONTINUED

IAM	Intellectual Asset Management
IC	Integrated Circuits (ICs)
IIR	Infinite Impulse Response
IP	Intellectual Property
JPF	Java Plug In Framework
LOA	Letter of Application
NSA	National Security Agency
OGC	Office of General Counsel Intellectual Property and Technology
OM	Opportunities Management
ORTA	Office of Research and Technology Applications
PLA	Patent License Agreement
R&D	Research and Development
RF	Radio Frequency
RLA	Range Limited Antenna
ROI	Return on Investment
SDI	Selective Dissemination of Information
SOW	Statement of Work
TA	Transfer Agent
TEM	Transmission Electron Microscope
TDOA	Time of Delay Arrival
TTP	Technology Transfer Program
TTSA	Technology Transfer Sharing Agreement
SEM	Scanning Electron Microscope
STFT	Short Time Fourier Transform
USB	Universal Serial Bus
WDM	Wavelength Division Multiplexed

APPENDIX B

PATENT INDEX

PATENT INDEX, CONTINUED

PATENT INDEX, CONTINUED

PATENT INDEX, CONTINUED

PATENT INDEX, CONTINUED

ACCESS TO INNOVATION
TTP

National Security Agency
Technology Transfer Program
9800 Savage Road, Suite 6848
Ft. Meade, MD 20755-6848
tech_transfer@nsa.gov
866-680-4539