Communications Research Centre Canada
An Agency of Industry Canada

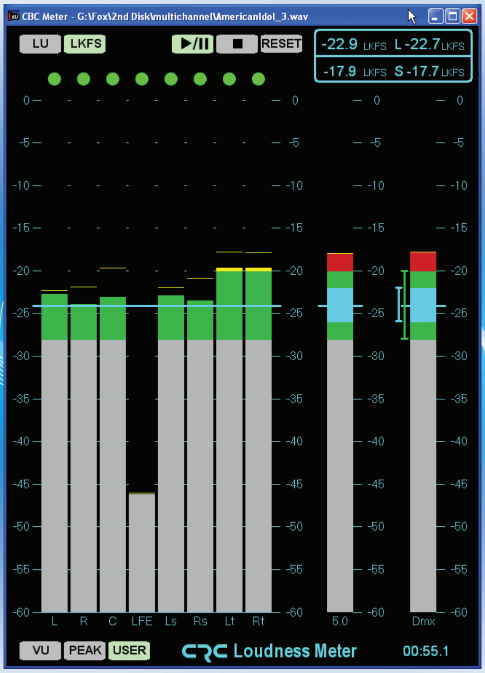
Centre de recherches sur les communications Canada
Un organisme d'Industrie Canada

Eye on Technology

ISSN 1717-7294

Issue No. 10 - Spring 2009 | www.crc.gc.ca

In This Issue...



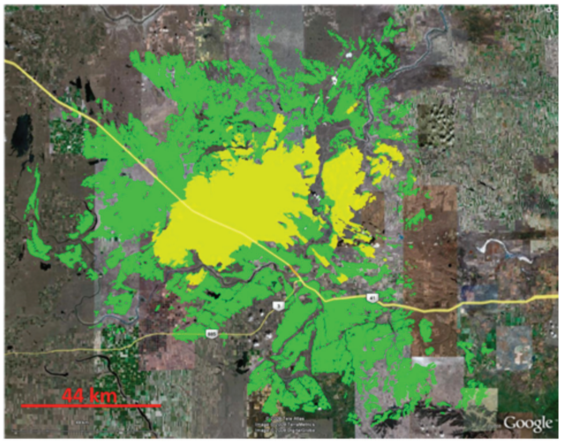
This display, of the new ITU-R loudness meter developed at CRC, is the result of CRC's collaboration with CBC/Radio-Canada. CRC is assisting Canada's national public broadcaster in the integration of the new loudness meter into its operations.

CRC Loudness Meter Chosen as International Standard

The detective creeps forward, gun drawn, barely a shadow against the dilapidated wall. Above him the clouds break, sending down a shaft of moonlight. He flattens himself against the wall knowing, just as you do, that if he's seen, if he's caught, the outcome will be death. The music, quiet and intense, builds slowly in the background. Suddenly, in the darkness, a twig snaps behind him. He whirls around … and the program cuts to a commercial that sends you shooting from the couch. You, and a million other viewers worldwide, dive for the remote to turn the volume down.

Canada

You can subscribe free of charge to this newsletter by e-mailing eye-on-technology@crc.gc.ca with the word "SUBSCRIBE" in the subject line.



This diagram highlights the improved coverage resulting from the aerostat. The yellow area indicates the predicted coverage of a base station located approximately 30 meters above ground level using a sophisticated RF planning tool. The green area illustrates the coverage improvement achieved by raising the base station to 180 meters above ground level using an aerostat. The improvement is significant, with up to 50 kilometers more range in some directions.

For more information contact Joe Fournier, Senior Research Engineer, Wireless Applications & Systems Research, at 613-949-0175 or *joe.fournier@crc.gc.ca.*

Steganalysis: Detecting the Invisible

Steganography, the art and science of hiding communication, has been a part of spy craft and military strategy for millennia. In the *Histories of Herodotus*, written in 440 BC, the author recounts the story of Histiaeus, who shaved the head of his most trusted slave, tattooed a message on his scalp and, once the hair had grown back, sent the man through enemy lines to deliver the message. Unlike cryptography, where the message is evident but its meaning is obscured, the goal of steganography is to hide the message entirely so only the sender and the recipient know of its existence – what the Communications Research Centre's (CRC) Dr. Ken Sala refers to as "hiding in plain sight." And, like all things in the modern world, steganography has gone digital.

"Most people don't understand that each time you visit a website the photographs from that website are downloaded to your computer," explains Sala.

That, added to the recent proliferation of cheap, accessible steganography software, means you may already have altered or "dirty" files on your computer with no knowledge that they're there, and this has some companies and government departments concerned. While most steganography software is used for legitimate purposes, the fear is that these powerful programs could be used to mask illegal activity such as the theft of trade secrets or the exchange of child pornography. Both private companies and government departments are looking for ways to ensure their computers and websites are free of corrupted files.

"When you consider that there are over 2.5 trillion images exchanged through the Internet on a daily basis," says Sala, "the potential scope of the problem becomes clear."

Most steganography software is used lawfully for securing computer files. In the age of the laptop, where a hard drive may contain secret company files as well as bank passwords and personal information, the software can be employed to hide sensitive material and thus protect it in the event that the laptop is lost or stolen. Many companies also want to secure desktop computers within the workplace, especially those of people working on classified projects.

Sala's interest is the flip side of steganography, the science of steganalysis. While the steganographer's goal is to hide the message, Sala's research focuses on ways to detect altered files. All digital steganography involves one or several carrier files – often image files – as well as the image or message the sender wishes to hide. What is important to understand, says Sala, is that the steganography software embeds the hidden image in the binary code of the carrier file. There is no "picture-within-a-picture," so no matter how hard you stare, the faint outline of the hidden image will never emerge. Rather, says Sala, digital steganography uses binary code to exploit a weakness in the human eye.

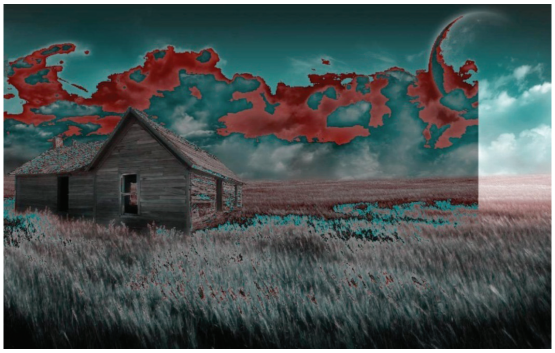
Each pixel within a digital image is made up of 24 bits of information – a string of zeros and ones that translate into the pixel's colour. But with 24 bits, a computer can generate over 16 million colours, far more than the eye can distinguish. To embed the hidden message, then, the steganography software "steals" bits from each pixel and replaces them with the binary code for the secret digital file. By stealing only the least significant bits within any pixel, the very slight alteration in hue can't be detected by the human eye. So how much information can you hide in a snapshot?

"Just think of a common digital camera," says Sala. "You have 3600 x 2400 pixels in each image, and each pixel is coded by 24 bits. I can easily steal six bits from each pixel and not noticeably alter the colours. That means I can commandeer over 50 megabits for my hidden message in only a single image. I can put the whole text of the Bible in 50 megabits."

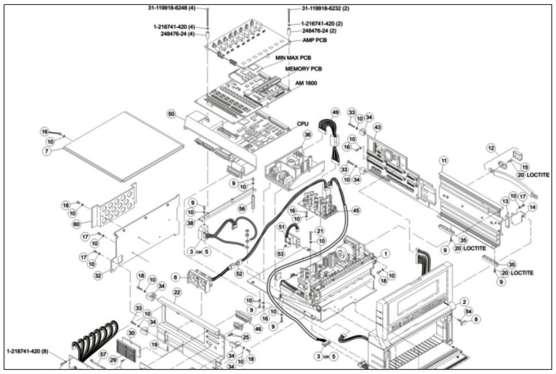
To extract the hidden image or message, the recipient then uses the software to strip away the code for the carrier file, leaving only the code for the secret message. These bits are then reassembled into an array that can be displayed as a JPEG, GIF or other file. While this simple substitution of the hidden-message code for least-significant-bits (lsb) is relatively easy to detect, says Sala, the new, more sophisticated steganography tools now allow users to encrypt their code before embedding it in the carrier file, as well as spread it out across multiple files. Each picture in the "family album" could thus contain an encrypted section of code from the hidden message or image, and this, says Sala, makes the altered files extremely difficult to detect.

Sala's research focuses on the use of neural networks to detect hidden files. Neural networks, he explains, are computer networks made up of simple "artificial neurons" that process information. Working together, these "artificial neurons" function much like a human brain, learning from past experience and coming up with novel ways to solve a problem. According to Sala, the advantage of using a neural network to search for altered files is two-fold. First neural networks can process vast amounts of information.

Original image concealing hidden image data



Original image showing the portion containing the hidden image data



Extracted file

"You can throw tens of thousands of images per second at these neural networks and they just spit out an answer: clean or suspect."

Second, they learn, so as steganographers come up with increasingly convoluted ways to hide information, the neural network will evolve and adapt. But to carry out a complex task like detecting hidden files, the neural network, says Sala, must be trained, and this involves presenting the network with as many varieties of clean and altered files as possible.

"It's like training a child. You start with the easy stuff and progress to the hard stuff, giving feedback along the way."

Sala is currently building a database of clean and dirty files, trying to develop the most nefarious ways imaginable to embed hidden messages. These files will then be used to train a neural network to detect anomalies in a file's structure that would indicate a hidden message. If he succeeds – if he is able to train a neural network to flag suspect files – he'll have, he says, the electronic equivalent of a sniffer dog. With this powerful tool, able to scan large numbers of files in a short period of time, resources can be focussed on cracking open only the suspect files.

"To do this kind of work," says Sala, "we need something fast, that can evolve and learn, but we also need something that is in-house, not in the public domain. Once a new kind of steganalysis software is on the market, the people who are using this kind of technology for illicit purposes have already figured out a way to get around it. With neural networks, that's almost impossible."

For more information contact Ken Sala, Research Scientist, Integrated Electronics, at 613-998-2823 or *info@crc.gc.ca.*

One Step Closer to the Wireless World

In October 2008 the Communications Research Centre (CRC) hosted the 4th Optimized Link State Routing Protocol Workshop (OLSR), drawing participants from Europe, North America and Asia. They came with a single purpose in mind: to discuss and test the next generation of software that will lead to a truly wireless world. The software, being developed in part by CRC, will allow computers to communicate – to form networks – in the complete absence of infrastructure.

These mobile ad hoc networks (MANETs), explains Maoyu Wang, a research engineer with CRC's Mobile Ad hoc and Sensor Network Systems group, have tremendous potential for use in situations where the infrastructure has been destroyed by natural disasters or war. But they also have a distinctly Canadian context, she points out. MANETs could be used to link people in rural communities and, in some cases, even link those communities to the Internet by "stepping stone" nodes. While several prototype MANETs are up and running in Europe, the current version of routing software (OLSRv1) places limitations on their usefulness in real-life situations, something Wang and her CRC colleagues have set out to change. At CRC's October workshop, Wang showcased the lab's OLSRv2, a new version of the routing protocol that allows for fast and accurate movement of data within a mobile ad hoc network, but without the problems and limitations inherent in the earlier version.

"When you form a network via the Internet," she explains, "you require infrastructure. You have routers and communication beacons, fixed points that direct the flow of data packets to the various addresses. In a mobile ad hoc network you have no fixed points, so each computer must act as a router as well as an end host."