Advanced technologies deliver high-performance DSP-based surveillance systems that can be implemented efficiently.

**Building Digital Video Surveillance Systems: Beyond MPEG-4**

Over the last three years, the digital video surveillance market has shown an unprecedented boom. A search on the term “digital video surveillance” yielded 993,000 results on Google. The reasons for this surge range from the responses to 9/11 to the rise of IP infrastructure and the availability of high-performance, low-cost video processors.

A wide range of products have appeared on the market, but they can be roughly divided into two types: DVRs and IP nodes.

DVRs replace the classic videotape recorders and are placed in the control center of the surveillance system. Multiple analog video inputs are connected to the DVR (typical numbers range from 4 to 32 inputs). The DVR converts the analog signal into digital, then compresses the video using MPEG or MPEG-like algorithms to reduce the data bandwidth and to store the video on hard disks. Though not restricted to working with analog cameras, DVRs are highly popular in legacy analog systems.

IP nodes are used when building an IP-based surveillance system. Instead of running analog video cables throughout the protected facility, you can use the Ethernet infrastructure, which can be either wired (“wireline”) or wireless (although the latter is more susceptible to outside interference). The IP node consists of one or more cameras whose output is digitized, compressed, and sent over the network to a server, which records the data on a hard disk.

---

**Figure 1:** The TMS320DM642 digital media processor is highly suited for building an IP node, offering audio and video, Ethernet, and generic I/O in one device.
An infinite number of variations of the two devices exist, the IP camera being a notable one. This device incorporates a digital camera and some form of video compression and IP stack and produces either 10/100 Ethernet or WiFi outputs. Low-cost IP cameras are becoming increasingly popular in low-end home security systems.

System components can cost $850 per camera up to $1,000 per channel. What, then, are the qualities that differentiate high- and low-end surveillance systems? The answer is, high-performance systems use advanced technologies, such as video stabilization, video motion detection, and encryption and watermarking.

Consider the basic solution shown in Figure 1. The system is based on Texas Instruments’ TMS320-DM64x™ digital media processor, which runs at up to 720 MHz and has dedicated video and audio ports, as well as an Ethernet MAC.

**VIDEO QUALITY**

The first parameter that differentiates systems is the video quality. Although analog cameras record full-frame-rate video (30 frames per second in the United States, 25 in Europe), the resolution is typically low. VHS tapes can record only about 240 lines of video, with the image “stretched” to full-screen resolution.

Digital video systems typically use one of two resolutions: CIF (Common Intermediate Format), which corresponds to VHS quality, and full D-1 (720x480) which is the top quality achievable on a DVD. The latter is about four times greater than the former. As a result, encoding a full D-1 channel requires four times the processing power, bandwidth, and storage space, translating into a proportionally higher cost per channel.

Although CIF resolution is more than enough for most indoor surveillance applications, higher resolution is needed in outdoor security covering large areas or in casinos, where slight of hand is a major issue and systems must pick up the detail on a player's card. Likewise, the number of frames per second may vary from as low as 2 frames per second in indoor surveillance to the full 30 frames per second in casino surveillance systems.

The number of frames encoded must be divided among the number of cameras in the system. The typical compression performance of MPEG-4 is 120 CIF frames for a 600-MHz DM642 processor. This performance can be used for one full-frame, full-rate channel, for example, or four half-resolution (two CIF) encoders at 15 frames per second.

To complicate matters, many times a surveillance node is required to process two compression rates on a single stream, one high-performance stream for video monitoring (real-time viewing) and another, small-size, low-fps stream for recording.

The video bit rate is a major concern for any application. A full uncompressed video stream requires more than 100 Mb/s to store or stream. You can reduce the transmission rate to about 2 to 4 Mb/s without a major loss of quality by using an MPEG-4 codec. The new H.264 codec promises to reduce the stream an additional 33 percent.

Video encoding latency can also be a major issue. Many times, a controller will want to track a subject remotely by controlling the camera's motion (PTZ axis command). That's impossible if the latency of the encoding and transmission is too high, since the target will be long gone. Low-latency encoding is typically achieved by avoiding using the B frame feature in MPEG encoders. This feature results in less effective compression, but it provides good latency. Again, using one stream for monitoring and another stream for recording can overcome this problem, although it requires extra DSP resources.

**ADVANCED VIDEO FEATURES**

**Stabilization**

Perceived video quality is affected by other algorithms besides the video compression. Video from security cameras, especially outdoor cameras, often shake. Shaking comes from many sources. Swaying buildings, wind, cameras mounted near air vents, PTZ servos, and...
such, all generate shaky and unsteady video. This effect is amplified by high-power zoom lenses.

Removing the shaking reveals cleaner details (Figure 2), which are required for both good- and high-quality security video. Shaky video tends to compress very badly, resulting in further loss of details. Stable images result in greater compression and higher quality for remote and Internet viewing. Also, modern digital compressors use many bits to encode the moving features of a video. If the whole image shakes, everything is moving, wasting an enormous number of bits. That’s another reason why removing the shaking enables digital recorders to store more, higher-quality video.

DVR can save considerable disk space by recording only when motion is detected (or increasing the encoder bandwidth), in addition to alerting security forces. VMD algorithms typically consume 5 to 20 percent of a DM642’s power, depending on the use of stabilizations and the robustness of the VMD. Combining VMD with traditional sensors, like tripwires and volume detectors, can significantly increase detection rates and reduce false positives.

Algorithms for another form of video detection, smoke and fire detection, are being added to identify physical danger.

Several companies are now taking the intelligence of these systems to the next level by developing content analysis tools that can respond to such instructions as “Retrieve the video where a blue car appeared.” The tools analyze and tag video in real time as part of the new MPEG-7 standard.

Encryption can maintain the privacy of the people within the protected area, as well as prevent outsiders from interfering with the system data without detection.

Several companies provide video stabilization algorithms for the TMS320C6000™ DSP platform that use as little as 5 percent of the DSP’s processing power per channel.

**Video Motion Detection**

Video motion detection (VMD) is quickly becoming one of the hottest technologies in the homeland security market. With tens of millions of CCTV cameras in the world, it’s impossible to have a person view each one and detect intruders. VMD algorithms provide artificial intelligence-like performance in detecting intruders by analyzing a video stream and overcoming vibration, wind, dust, and light changes, as well as minor interference by, for example, small animals. Combining VMD with a

the order of video lines, digital surveillance systems can rely on advanced generic data encryption technology, such as the triple DES system developed by IBM or the new Advanced Encryption Services (AES) encryption, Snapshield

Watermarking preserves the authenticity of the video recorded by the system. Digital images and videos can be manipulated easily, diminishing the integrity of the content. Watermarking solutions embed a digital signal containing the secure hash value of the image in the digital image or video. The watermark is invisible to the naked eye and doesn’t alter the value of the content. Any attempt to manipulate even a single frame will be detected. A secret key is needed to access the information embedded within the watermark, adding another layer of security. The date and time of capture is stamped on each video frame; therefore any attempt to remove frames in the video stream can be detected.

Watermarking is becoming essential both for preventing outside parties from interfering with the video and for proving to the courts that recorded digital video is reliable and can be used as reputable evidence.

**CONNECTIVITY**

Aside from video monitoring and archiving, a surveillance system needs to provide much more functionality, such as connectivity. A swivel camera can be controlled (PTZ) via a serial port to allow
remote control by security personnel at the control center.

Audio can be sent to and from the DSP using the DM64x’s serial MCBSP ports, providing audio recording and two-way intercom capabilities. The GPIO pins can be used to control alarms, connect to traditional intruder detection devices (volume detectors, trip-wires, photo-optic sensors, and the like), and control doors.

When connected to the correct input hardware, the DSP can be used to process biometric information. Most notably, you can add fingerprint recognition to a security node to provide highly effective access control.

**POWER CONSUMPTION**

Using DSP technology, it's possible to create compact, highly dense solutions with a large number of streams. Unlike Pentium-based solutions, which are inherently large and consume 50+ W per full video channel, DSP-based solutions can produce small IP nodes and DVRs with dozens of high-performance channels.

Another benefit of low power consumption is the limited use of fans for cooling. As a rule, the more heat a system produces, the lower the MTBF. Fans further reduce the MTBF, since they are notoriously unreliable, and once they malfunction, the system is a short way from burning up.

A new technology being introduced for IP nodes is IEEE 802.3af, power over Ethernet. Devices using less than 10 W can receive their power through the IP network with no need of additional wiring. This technology can considerably reduce infrastructure costs. Needless to say, low-power devices are much easier to run off batteries, allowing the system to keep working when there’s a power-down or if someone tampers with the wiring.

There are thousands of IP nodes and DVRs on the market, as well as companies offering various tools and technologies to build such solutions. The solutions can be roughly divided into PC-based and embedded.

**WHAT’S OUT THERE?**

Hundreds of companies offer PCs equipped with video capture cards that can be used as DVRs. Some use hardware-based compression to overcome the performance limitation of the Pentium. In general, these solutions offer limited performance and reliability but offer very competitive pricing for the DVR market.

The embedded solutions are based on ASICs or DSPs performing video processing. ASIC-based solutions typically use MPEG-2 compression with limited features (using ICs developed for entertainment by such companies as Zoran and C-Cube). DSP-based solutions, like the one described here, can be developed from scratch or by using tools such as TI’s DM642 Evaluation Module (EVM); and third-party video encoders, such as UBVideo’s or Prodys’s, plus an audio codec and other useful libraries. Mango DSP takes a different approach, providing complete DSP-based programmable platforms, like the four-channel RAVEN-X IP node or the eight-channel LARK DVR.

As always, each solution has its merits, depending on performance, features, channel cost, and time to market.

Joel Rotem is the chief applications engineer at Mango DSP Inc. in San Jose. Before joining the company, he cofounded DV-Demand, which specialized in MPEG-2 and DVD technology, and has filed two patents in these fields. Prior to that, he worked at Waves Inc.
IMPORTANT NOTICE

Texas Instruments Incorporated and its subsidiaries (TI) reserve the right to make corrections, modifications, enhancements, improvements, and other changes to its products and services at any time and to discontinue any product or service without notice. Customers should obtain the latest relevant information before placing orders and should verify that such information is current and complete. All products are sold subject to TI's terms and conditions of sale supplied at the time of order acknowledgment.

TI warrants performance of its hardware products to the specifications applicable at the time of sale in accordance with TI’s standard warranty. Testing and other quality control techniques are used to the extent TI deems necessary to support this warranty. Except where mandated by government requirements, testing of all parameters of each product is not necessarily performed.

TI assumes no liability for applications assistance or customer product design. Customers are responsible for their products and applications using TI components. To minimize the risks associated with customer products and applications, customers should provide adequate design and operating safeguards.

TI does not warrant or represent that any license, either express or implied, is granted under any TI patent right, copyright, mask work right, or other TI intellectual property right relating to any combination, machine, or process in which TI products or services are used. Information published by TI regarding third-party products or services does not constitute a license from TI to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property of the third party, or a license from TI under the patents or other intellectual property of TI.

Reproduction of information in TI data books or data sheets is permissible only if reproduction is without alteration and is accompanied by all associated warranties, conditions, limitations, and notices. Reproduction of this information with alteration is an unfair and deceptive business practice. TI is not responsible or liable for such altered documentation.

Resale of TI products or services with statements different from or beyond the parameters stated by TI for that product or service voids all express and any implied warranties for the associated TI product or service and is an unfair and deceptive business practice. TI is not responsible or liable for any such statements.

Following are URLs where you can obtain information on other Texas Instruments products and application solutions:

<table>
<thead>
<tr>
<th>Products</th>
<th>Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amplifiers</td>
<td>Audio</td>
</tr>
<tr>
<td>Data Converters</td>
<td>Automotive</td>
</tr>
<tr>
<td>DSP</td>
<td>Broadband</td>
</tr>
<tr>
<td>Interface</td>
<td>Digital Control</td>
</tr>
<tr>
<td>Logic</td>
<td>Military</td>
</tr>
<tr>
<td>Power Mgmt</td>
<td>Optical Networking</td>
</tr>
<tr>
<td>Microcontrollers</td>
<td>Security</td>
</tr>
<tr>
<td></td>
<td>Telephony</td>
</tr>
<tr>
<td></td>
<td>Video &amp; Imaging</td>
</tr>
<tr>
<td></td>
<td>Wireless</td>
</tr>
</tbody>
</table>

Mailing Address: Texas Instruments
Post Office Box 655303 Dallas, Texas 75265

Copyright © 2004, Texas Instruments Incorporated