

Researchers Develop Low-Cost Holographic Display

A team of MIT scientists has developed a prototype for a small, inexpensive, holographic video system that works with consumer computer hardware such as PCs or gaming consoles, thereby enabling users to view images in three dimensions.

The Mark III display could enhance participation in video games and virtual worlds, which currently are displayed mainly in two dimensions. The technology could also let doctors better view medical images such as those produced by magnetic resonance imaging. It could also help designers of complex objects such as cars.

To create a holographic video, the Mark III's software produces a 3D model of objects within a scene, explained V. Michael Bove Jr., principal research scientist and director of the MIT Media Lab's Consumer Electronics Laboratory. The software then calculates how the device must process laser beams to create a 3D hologram that looks like the model from all viewing angles. Holograms result from a diffraction pattern that occurs when light waves interfere with one another after passing through a modulator.

Based on the software calculations, the Mark III sends an electronic signal into its modulator, which then encodes a laser beam

into various intensities and frequencies. When projected onto a foggy piece of glass, the light recreates the desired 3D scene as a hologram.

The graphics processor in a user's PC, gaming console, or other device produces the signal necessary to show a series of holographic images to viewers in video form.

The Mark III is the third generation of holographic video displays that MIT has developed since the early 1990s. The Mark I and II required specialized hardware to produce video signals, offered low-resolution images, were as big as a dinner table, and were tricky to work with, Bove said.

The new system processes 3D images via a standard graphics processor rather than specialized hardware.

Also, a new high-bandwidth, acousto-optic modulator which works with sound waves, replaces a stack of acousto-optic modulators. It is thus smaller and less expensive.

The Mark III currently offers only monochromatic images, and its viewing volume is equivalent to an 80-mm cube, too small for practical applications such as PCs. Multiple modulators, one for each primary color, or one very fast modulator could provide color images, according to Bove.

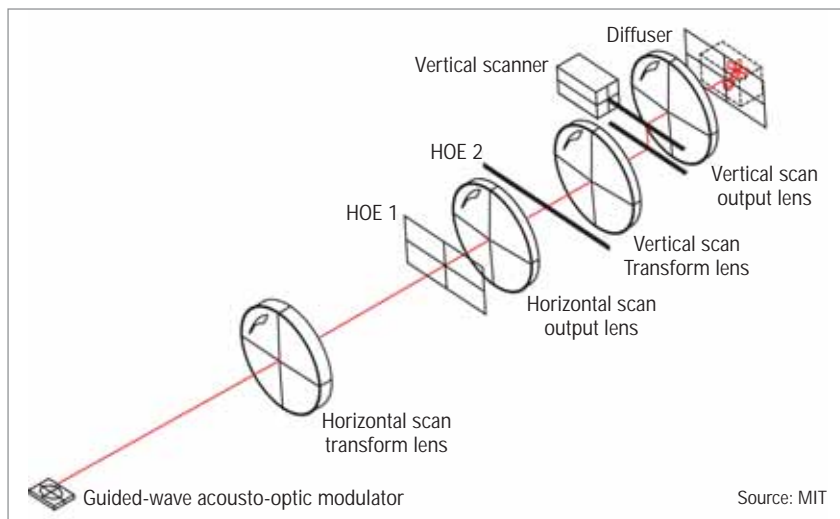
The researchers are working on a fourth-generation holographic display that shows larger, full-color images. However, Bove noted, "We won't start building it until we've learned some lessons from the Mark III."

His team is working with their corporate research sponsors to evaluate the technology's commercial potential.

A monochromatic display like the Mark III might be suitable for applications such as radiography, rather than consumer games, said analyst Jennifer Colegrove with iSuppli, an electronics-market research firm.

On the other hand, she said, a full-color version could capture a significant part of the 3D display market, which is expected to grow significantly. ■

—George Lawton
(glawton@lawton.com)



In the Mark III holographic display, a guided-wave device diffracts and modulates a laser beam to produce an image signal. The signal passes through stationary lenses and holographic optical elements (HOEs) to a moving vertical scanning mirror, which produces a raster that yields a holographic image when viewed through a diffuser.

New System Tests Spammers' Patience

A Canadian company has developed a product that delays e-mail communications and thereby causes spammers to stop trying to send junk mail to users.

MailChannels' Traffic Control uses this approach to take advantage of spammers' desire to quickly send as many messages as possible, maximizing the chance that some recipients will open them.

Typically, when an e-mail server receives a request to accept an incoming message, it quickly responds to the sender, explained MailChannels CEO and founder Ken Simpson. While this takes place, the Simple Mail Transfer Protocol (SMTP) keeps the connection open between the sender and receiver, thereby tying up the transmitter's resources.

Traffic Control software is usually installed in the e-mail server and receives messages before the server software. Traffic Control initially analyzes traffic to determine legitimate senders based on factors such as their reputation, protocol compliance, host characteristics, and message content. Messages from legitimate senders pass through without delay, and messages deemed to be harmful are blocked.

For suspicious messages, Traffic Control causes the e-mail server to conduct the digital handshake a few bits at a time, making the process last up to 10 minutes, depending on user configuration.

Legitimate senders' computers generally determine that there is a

problem with the connection and simply try again. "Even after eight minutes [of waiting], 60 percent of legitimate e-mail senders still try to deliver their message," Simpson noted.

Spammers, on the other hand, configure the software that sends their messages, usually from hijacked zombie computers, to stop trying when messages don't transmit quickly.

According to Simpson, 90 percent of spammers give up trying to send their message after 10 seconds of delays. Their resources are finite, and if they set their systems to keep trying to send messages in the face of delays, it reduces the volume of spam they can send, he explained.

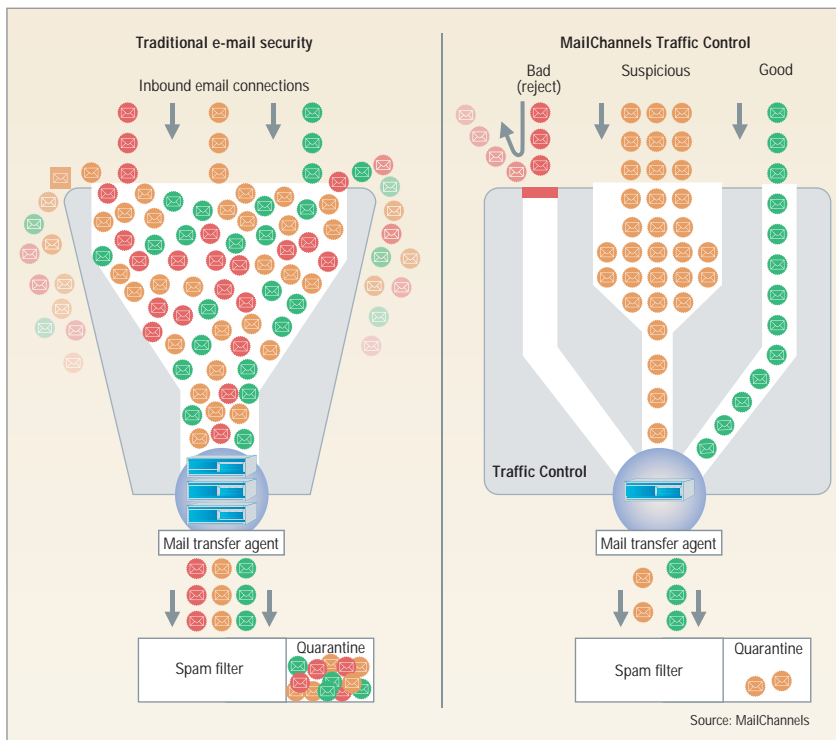
Small pauses in the communications process can quickly add up, create a traffic backlog, and slow receiving e-mail servers to a crawl. The servers generally can't process enough backed-up traffic to recover quickly, Simpson said.

In response, he noted, MailChannels has developed SMTP multiplexing, which lets thousands of incoming transmissions multiplex onto far fewer mail-server connections. This lets the user's server handle the traffic backlog in a manageable way, he explained.

Traffic Control should be effective because it segregates legitimate and suspicious traffic and then handles the latter before it gets to the mail server and causes problems, said Carl Howe, a principal with Blackfriars Communications, a market research firm.

Nonetheless, he said, no single technique will stop a large and complex problem like spam. Instead, he added, users must work with a variety of approaches. ■

—Linda Dailey Paulson
(ldpaulson@yahoo.com)



MailChannel's Traffic Control handles spam by analyzing e-mail to identify legitimate, harmful, and suspicious messages. Traffic Control admits legitimate messages and blocks harmful messages. The product causes the e-mail server to slow the digital handshake with suspicious messages, causing spammers to stop sending them.

Group Works on Open Source Interoperability

A new consortium is trying to make open source software from different vendors work together so that the products can better compete against the suites of integrated and interoperable proprietary applications that many large software companies offer.

The newly formed Open Solutions Alliance (www.opensolutionsalliance.org) plans to work toward enabling open source application interoperability, certifying quality approaches to integration, and promoting cooperation among developers.

There are few interoperability standards for open source business applications, and they aren't applicable to building a suite of interoperable programs, noted OSA board member Barry Klawans, chief tech-

nology officer at JasperSoft, an open source business-intelligence vendor.

Companies thus have had to spend considerable time and money trying to make open source applications work together, which has hindered the software's adoption.

In response, the OSA will document guidelines and best practices for building and deploying interoperable applications. The effort is designed not to push members' products but to provide a resource for companies, Klawans said. The alliance also wants to offer information on open source license-management issues, help arrange collaborative projects among vendors, and provide technical support to sellers and users.

As part of this effort, the OSA wants to ensure that its approaches

will make open source software work together smoothly even when running on proprietary platforms, in which many companies have invested heavily.

The alliance has already produced a roadmap (www.opensolutionsalliance.org/team/ProjectManagement.do?command=ProjectCenter§ion=File_Library&pid=1&folderId=-1) to show the problems it will deal with, as well as a timeline for developing standards, best practices, and prototypes of interoperable open source software.

To enable interoperability, the OSA is considering recommending both APIs and the use of common elements within applications that would enable the programs to work together.

Company Cleans up after Online Messes

A startup company has begun offering a service that tries to remove information online that could hurt clients' social reputations or even damage their chances of getting a job.

ReputationDefender (www.reputationdefender.com) tracks online information relating to customers—such as photos, blog postings, and social-networking activities—for \$10 per month. For \$29.95 per incident, the company asks Web sites and data-hosting services to remove potentially damaging materials. When unsuccessful, the company refunds its fee, said CEO Michael Fertik.

When removal isn't practical, the company can make unwelcome content show up less prominently in search engines so that it is less likely to be seen, he noted.

ReputationDefender offers three services: My Reputation for adults; My Child for parents who want to protect their children's online reputations; and My Privacy, currently in alpha testing, for removing private data—such as Social Security and driver's license numbers, home addresses, and phone numbers—from Web sites.

Using site-scraping robots and human research, ReputationDefender searches the Internet, particularly

social networking sites, for potentially harmful material.

"Fully half of our clients use our service just to search for information. They want to keep up to date on what's being said about them online," noted Fertik.

"The requests [to eliminate information] are from clients who are looking out for their professional lives, their romantic lives, and their personal reputation and sense of self."

"If someone is calling you a nasty name or publishing a photo that doesn't need to be on the Internet, we don't think you need to suffer from that kind of indignity," he said. "We also believe it is the right of individuals to know what others are saying about them and of private individuals to protect themselves from unintentional, inappropriate, or illegal intrusions into their privacy."

However, there are certain steps the company refuses to take. For example, it will not try to remove news articles or government records. And, Fertik explained, "We will not hack sites, use viruses, carry out [denial-of-service] attacks, or do anything 'black hat.' We're open and transparent with our techniques. And our approach is very civil and very polite." ■

—George Lawton

The OSA has announced that it has begun work on its first major interoperability prototype: the Common Customer View. The CCV will provide a common way for users to work with data and will also let them perform tasks such as logging on to an entire suite of applications at one time.

The CCV will also address issues such as a common look and feel for open source application interfaces and real-time synchronization among programs.

The prototype will use Talend's open source data-integration soft-

ware and expertise from Unisys and SpikeSource, an open source application-management vendor. In addition to these companies, the OSA includes vendors such as Centric CRM and Enterprise DB.

Several large open source vendors—MySQL, Novell, Linux vendor Red Hat, and SugarCRM—have not joined the OSA. “This will hurt the alliance,” said Perry Donham, director of enterprise-integration research with the Aberdeen Group, a market research firm.

Moreover, Donham noted, the OSA must compete with the

Interop Vendor Alliance (<http://interopvendoralliance.org>), to which numerous open source and proprietary software firms, as well as hardware companies, belong.

To be most useful, he said, the OSA should focus on open source applications' interoperability with proprietary applications, as well as with other open source software. ■

—Linda Dailey Paulson

Editor: Lee Garber, *Computer*,
l.garber@computer.org