
Case Study

**Intel® Core™ i7 and Intel® Core™ i5 Processors**

YCD Smart Digital Signage Solution

Embedded Computing

YCD MULTIMEDIA

"The high performance of the Intel® Core™ i7 and Intel® Core™ i5 processors, along with their new instructions for accelerating cryptography, enables our digital signage solutions to deliver media protection on-the-fly without sacrificing quality, interactivity or flexibility."

*– Dani Zeevi*
*Chief Technology Officer*
*YCD Multimedia*

# Protecting Media Content in Digital Signage

## YCD Multimedia uses powerful Intel cryptographic instructions to dramatically decrease the processor workload when decrypting media files

A prevalent security hole in many digital signage installations is, for the most part, being ignored. Generally, there is a lack of media content protection, which could lead to unlawful copying or unauthorized content playing on digital signage displays. Imagine a hacker stealing an advertisement or movie trailer, or worse, sabotaging a signage system and playing objectionable content on displays.

The surging demand for playing dynamic media content at any location, which is managed and scheduled from a central point, is increasing content vulnerability. In the past, digital signage systems were relatively closed and independent, but today, devices are connected to widely used LANs and require security to protect against malware and malfeasance. Moreover, remote displays connected via the public Internet are particularly susceptible targets because in addition to communicating over an unprotected network, someone can physically tamper with the device.

| | |
|---|---|
| Challenges | ▪ **Prevent illegal copies:** Content providers require protection against unauthorized copying, duplication or dissemination of media.<br>▪ **Prohibit unapproved playback:** Ensure a digital signage display will only play content that has been properly approved and distributed. |
| Solutions | ▪ **Implement AES security standards:** All played content is encrypted, thus avoiding wrongdoing.<br>▪ **Utilize special AES instructions:** Intel® AES-NI dramatically reduces the processor resources required to perform encryption and decryption. |
| Impact | ▪ **Customer satisfaction:** End users, as well as content providers, appreciate the value of improving media content security.<br>▪ **Lower operating expense:** Intel AES-NI uses an engine on the processor; therefore, there is no need for an additional security processor or add-in card. In addition, the engine frees up CPU resources for playback, which enables higher resolution and more video layers or zones. |

However, the cost associated with real-time decryption of data – stored locally or streamed from a server – has been an impediment to sufficiently protecting media content. When performing cryptography in software, nearly all of the CPU's processing power is typically needed. On the other hand, integrating hardware solutions, like special-purpose security processors, can needlessly add a lot of cost for customers that don't want the functionality. YCD Multimedia, serving some of the world's most recognized brands, found that by using Intel® Advanced Encryption Standards-New Instructions[1] (Intel® AES-NI), they could decrypt files almost sixteen times faster[2,3] than previous software implementations. Now, the company's software-based solution requires less than 10 percent of the processor's computing capacity to decrypt media, compared to previously consuming all of the processor.

## Enhanced Security

Deploying a strong security model, YCD implements end-to-end protection starting with its YCD|Platform* central distribution system that encrypts audio and video content before sending it to YCD|Player* stations, which then decrypt the content in real time during playback. The players also check that any stored content was properly encrypted by the YCD|Platform before playing it. Both platforms and players use Intel AES-NI security instructions to maximize performance and minimize the computing workload needed to support encryption/decryption.


**Figure 1.** Intel® Core™ i7 processor with Intel® AES-NI Engine

The software team at YCD investigated several ways to implement Intel AES-NI and measured the corresponding performance improvement compared to performing software decryption using the Crypto++ 5.6 library without Intel AES-NI. During the course of the evaluation, the team tested security functions from Intel® Integrated Performance Primitives (Intel® IPP) cryptography library, which included purpose-built software that employed Intel AES-NI.

The Intel IPPs were tested under two scenarios that varied the number of software threads executing decryption routines. Intel® Core™ i7 and Intel® Core™ i5 processors incorporate Intel® Hyper-Threading Technology (Intel® HT Technology),[4] which enables each physical processor core to run two software threads simultaneously. Thus, dual-core Intel Core i7 and Intel Core i5 processors have up to four threads available at one time.

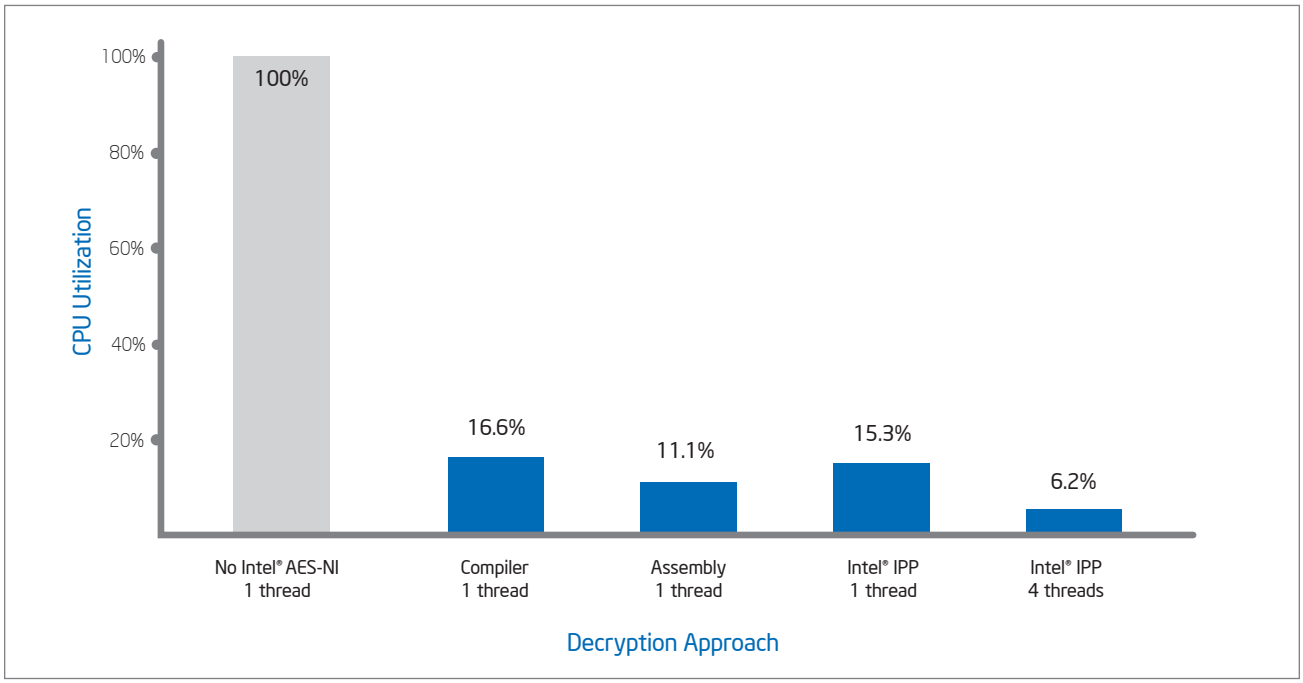



Figure 2. Relative time to decrypt a 1 Gigabyte file

**Implementation Methods Evaluated by YCD**

- **Compiler intrinsic:** A compiler embeds Intel AES-NI calls, when appropriate.
- **Optimized assembly code:** YCD developers wrote the security functions in assembly language, including Intel AES-NI calls. This single-threaded code processes four 128-bit blocks in parallel, taking advantage of the pipelining in the processor.
- **Intel IPP using one thread:** Intel IPP functions use Intel AES-NI and run on one thread.
- **Intel IPP using four threads:** Intel IPP functions use Intel AES-NI and run on four threads at the same time.

## Performance Benchmark Results

YCD measured the time required to decrypt one gigabyte of data for each of the methods using AES in CTR mode. It is a block cipher which has comparable performance for encryption and decryption. The normalized benchmark results[5] shown in Figure 2, are for decryption only, and other functions, such as playing the media file and reading from the disk, are not captured. The testing was performed on a computer equipped with the Intel Core i7 processor running at 2.0 GHz. The results are the average of five test runs for each decryption approach, and the coefficient of variation was 1.1 percent or less.

When testing four decryption approaches, the use of Intel® AES-NI decreased CPU utilization between six and sixteen times.

The best results were achieved when using Intel IPP cryptographic functions running on four threads; this method decrypted the file in only 6.2 percent of the time required by the software implementation without Intel AES-NI. The exceptional outcome is due to the high level of parallelism, and this may be the best choice for a device primarily performing encryption or decryption. However, most digital signage players supporting a multi-zone environment (i.e., simultaneously playing multiple media files with video layering) require a significant amount of computing resources; therefore, it may not be possible to dedicate four threads to decryption. In such an environment, the optimized assembly code using Intel AES-NI and a single thread may be the best implementation choice.

## Lowering the Cost of Security

Today, many digital signage installations do not sufficiently protect content media from hackers, partly because of the relatively high cost of implementing decryption on players. Until now, equipment manufacturers could choose a hardware approach that required a specialized security processor, or a software approach that typically consumed nearly all of the CPU's processing power. Making software-based decryption a viable option, Intel AES-NI cryptography instructions can reduce the security processing workload on Intel Core i7 processors by as much as sixteen times.[1] These specialized instructions dramatically lower the cost of deploying AES cryptography, enabling digital signage solution manufacturers to offer cost-effective, robust media content protection.

### About YCD Multimedia

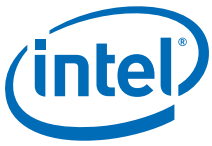
Founded in 1999, YCD Multimedia provides marketers with a set of tools for managing, distributing and targeting digital media in the retail environment. From large-format displays that promote products based on real-time inventory levels, to small shelf-level interactive displays, YCD's flexible platform can help retailers ensure a measurable impact on their business. YCD's end-to-end offering combines strategy, professional services and technology to increase profits, optimize product mix and enhance the customer experience.

To learn more about digital signage solutions from YCD Multimedia, please visit www.ycdmultimedia.com

To learn more about Intel in digital signage, please visit www.intel.com/go/digitalsignage

For more information about Intel AES-NI, visit software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni

Solution provided by:





[1]Intel® AES-NI requires a computer system with an AES-NI enabled processor, as well as non-Intel software to execute the instructions in the correct sequence. AES-NI is available on Intel® Core™ i5-600 Desktop Processor Series, Intel® Core™ i7-600 Mobile Processor Series, and Intel® Core™ i5-500 Mobile Processor Series. For availability, consult your reseller or system manufacturer. For more information, see http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni.

[2]Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products.

[3]For more information go to http://www.intel.com/performance

[4]Hyper-Threading Technology requires a computer system with a processor supporting Hyper-Threading Technology and an HT Technology enabled chipset, BIOS and operating system. Performance will vary depending on the specific hardware and software you use. See www.intel.com/info/hyperthreading/ for more information including details on which processors support HT Technology.

[5]Test Configuration: Processor: Intel® Core™ i7 L620 processor, System Memory: 2 GB, Operating System (OS): Microsoft Windows* Embedded Standard 7. The OS was started in safe mode using a command prompt to minimize any unnecessary OS overhead.



Printed in USA 0311/TB/OCG/XX/PDF Please Recycle 324879-001US