



High-bandwidth Digital Content Protection

W H I T E P A P E R

February 2000

CONTENTS

Introduction	3
• What is the Digital Visual Interface?.....	4
• What is High-bandwidth Digital Content Protection?	4
• Why not use Macrovision™ or DTCP developed for IEEE-1394?.....	5
The Digital Visual Interface (DVI)	5
High-bandwidth Digital Content Protection (HDCP) technology.....	7
• Authentication and key exchange.....	8
• Content encryption.....	8
• Device renewability	9
Implementation of HDCP	9
Conclusions	11

INTRODUCTION

The consumer industry is poised to embrace high-definition digital video, and the motion picture industry is eager to supply the content. However, not all the elements are in place.

Two key enablers required to view high-definition digital video are the hardware to supply and view it and the digital interface to connect the host to the display.

The hardware to view high-definition video is becoming readily available today. High-definition televisions can now be purchased at your local electronics store, and computer monitors are of sufficient size and resolution to resolve high-definition images. DVD players and digital VHS players too, are improving the video content from standard television formats, such as NTSC and PAL, to 480 line progressive video and beyond. The transition to digital content is also well on its way, with video stored in digital form on DVD discs and computer hard drives, and digital broadcasting developing rapidly as well.

With the development and rapid adoption of the **Digital Visual Interface** (DVI), a digital standard is now available that provides a high-bandwidth, low-cost digital interface between a graphic source and a display device. This eliminates the need for decompression circuitry at the display thereby simplifying design and reducing cost.

With the hardware available and digital link in place, where is the high-definition video to take advantage of it? The missing element has been **content protection**: the ability to prevent unauthorized copying of digital content.

Movie studios have not released high-definition digital video because of the fear of illegal copies of digitally perfect content. The Motion Picture Association (MPA) has been active in defining the need for high-definition content protection:

“What we are trying to create is an environment where content owners have the technological option to prevent copying and redistribution of high value content, and consumers have the option of viewing high value content in the widest possible variety of times, places and formats.”¹

High-bandwidth Digital Content Protection (HDCP) has been developed to meet this need.

This white paper describes the basics of HDCP and its application to the DVI interface.

What is the Digital Visual Interface?

The Digital Display Working Group (DDWG) was formed in 1998 to address the need for a single, universal digital interface standard between a host and a display. The group's initial members included Silicon Image, Intel, Compaq, Fujitsu, Hewlett-Packard, IBM, NEC, and the DVI specification was based on Silicon Image's PanelLink[®] technology.

The DVI 1.0 specification was released in April 1999. The primary focus of the DVI interface has been on providing the digital connection between a PC and a display device. By the end of 1999, DVI had gained wide industry acceptance, with 150 DVI products shown at the Intel Developer Forum in August 1999². By December 1999, PC makers were told they can "safely choose DVI now,"³ and over 6 million DVI-compliant PanelLink transmitters and receivers were supplied to the PC and display industry by end of 1999.

The primary advantages of the DVI interface is that it provides a low-cost, industry standard, high-speed digital link between a video source and a display. The DVI interface supports PC resolutions beyond 1600x1200 lines, and all HDTV resolutions **without compression** including 720 and 1080 lines progressive, and 1080 lines interlaced.

What is High-bandwidth Digital Content Protection?

HDCP is a system for protecting DVI outputs from being copied. It provides a secure digital link between a video source (PC, DVD, etc) and a display device (television, monitor, projector, etc).

Three key elements of the HDCP system:

- **Authentication** to verify that a display device is licensed to receive protected content
- **Encryption** of the transmitted video to prevent 'eavesdropping' of the protected content
- **Renewability** to enable the revocation of compromised devices

HDCP provides a low-cost solution for secure transmission of high-definition video, without compromising quality, and is transparent to honest consumers – unless unauthorized copying is attempted.

HDCP was developed by Intel, with contributions by Silicon Image. The HDCP 1.0 specification was released February 2000 at the Intel Developer Forum.

Why not use Macrovision™ or DTCP developed for IEEE-1394?

The Macrovision™ Analog Protection System adds a rapidly modulated signal in the vertical blanking signal of analog video, and is widely used to prevent unauthorized copying of prerecorded videocassettes. It does not apply to digital video.

DTCP (Digital Transmission Content Protection) has been developed for the IEEE 1394 digital interface. However, 1394 has a limited bandwidth of 100-400 megabits per second, not sufficient for uncompressed high-definition video (but sufficient for MPEG2 compressed video). Also, the implementation of DTCP adds the additional cost of implementing 1394 with MPEG2 encoders and decoders.

HDCP and DVI is the only industry accepted, low-cost, digitally protected link with a bandwidth of up to 5 gigabits per second.

THE DIGITAL VISUAL INTERFACE

The Digital Display Working Group (DDWG) released the DVI 1.0 specification of DVI in April 1999. The full specification is available at www.ddwg.org

The specification defines a digital interface between a host and a display device. The interface is primarily focused on providing a connection between a computer and a monitor, but also provides a display technology independent solution for the transmission of any digital content.

The Digital Visual Interface uses the PanelLink transition minimized differential signaling protocol developed by Silicon Image. The transition minimization is achieved by implementing an advanced encoding algorithm that converts 8 bits of data into a 10-bit transition minimized, DC-balanced character. PanelLink technology is optimized for reduced EMI (electromagnetic interference) across copper cables, and is DC-balanced for data transmission over fiber optic cables. In addition, robust clock recovery at the receiver achieves high skew tolerance for driving longer cable lengths as well as shorter low-cost cables. The input stream contains pixel and control data.

The link architecture is shown in Figure 1.

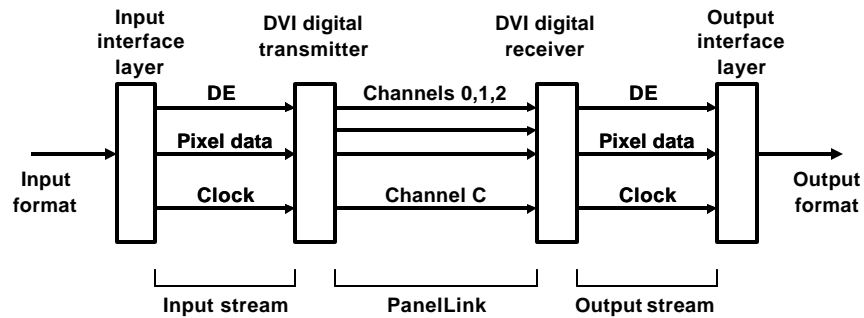


Figure 1. Panellink architecture

The link consists of three channels, and each channel supports a bandwidth of up to 1.65 gigabits per second. For the transmission of digital video, Panellink uses the three channels for the red, green, and blue data, and an additional channel C is used for the interface clock. This is sufficient bandwidth to support:

- SXGA (1,280 by 1,024 pixels) images at an 85-Hz refresh rate for a CRT
- UXGA (1,600 by 1,200 pixels) images at an 60-Hz refresh rate for a LCD
- HDTV resolutions of 720p and 1080i for high-definition televisions and projectors

To support higher resolutions, such as 2048 by 1536 pixels for high-end PC workstation monitors, two links can be integrated into a single DVI connector interface to support a bandwidth of 330 mega pixels per second, and above. This dual link configuration consists of 6 channels, and a shared clock. The amount of bandwidth required for a specific display at a given resolution is

technology dependent, as it depends on blanking overhead required. The available link bandwidth is shown along with the resolutions supported for LCD and CRT displays in Figure 2.

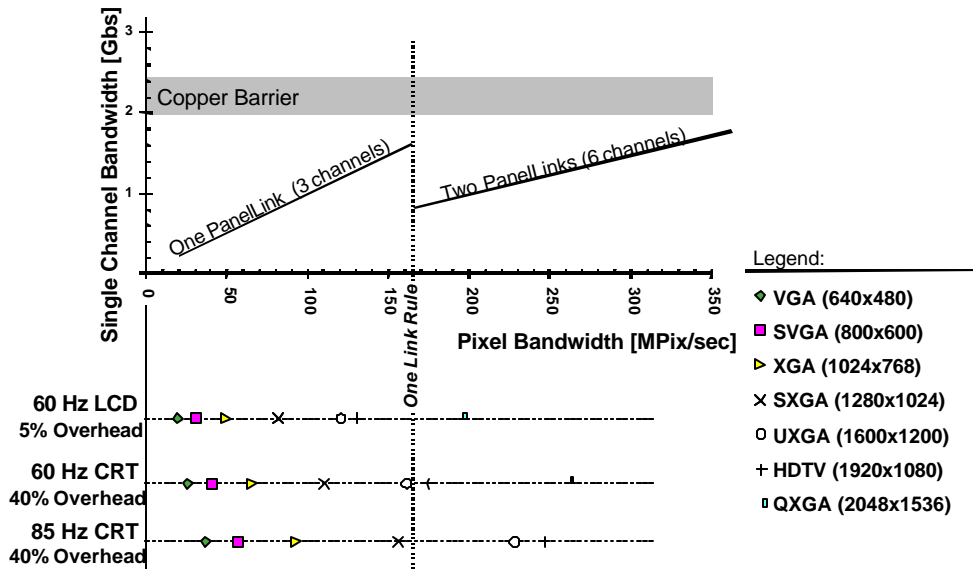


Figure 2. Available link bandwidth

The copper barrier in Figure 2. is a limitation of the copper physical layer to support high frequencies.

HDCP TECHNOLOGY

HDCP was developed by Intel, with contributions by Silicon Image, to provide a protected DVI link between a host and a display device, and thus prevent DVI outputs from being copied. Key requirements of HDCP are to:

- **Establish a secure channel:** verify that the display device is licensed to receive protected content
- **Encrypt at the host side, and decrypt at the display device:** to prevent 'eavesdropping' of the protected content
- **Have a means of identifying unauthorized or compromised devices**

Technically, this translates into a series of specific requirements:

- Authentication and key exchange
- Content encryption
- Device renewability

Authentication and Key Exchange (AKE)

Authentication is a cryptographic process for verifying that the display device is authorized (or licensed) to receive protected content. Both the authorized host and the display device have knowledge of a set of secret keys supplied to the manufacturer by the license administrator of HDCP. The secret keys consist of an array of forty 56-bit secret device keys and a corresponding 40-bit binary Key Selection Vector (KSV).

The host (device A) initiates authentication by sending an initiation message containing its Key Selection Vector, A_{KSV} , and a 64-bit value A_n . The display device responds by sending a response message containing its Key Selection Vector, B_{KSV} . The host confirms that the received KSV has not been revoked.

At this point, the two devices can calculate a shared value, which, **if both devices have a valid set of keys**, will be equal. This shared value will be used in the encryption and decryption of the protected content. Authentication has now been established.

Re-authentication continues at a rate of approximately once every two seconds to confirm the continued security of the link. If, at any time, equality of the shared value is lost, for example by disconnecting the display device and/or connecting an illegal recording device, the host will consider the DVI link to be unauthenticated, and end the transmission of protected content.

Content encryption

Content is encrypted at the source device to prevent usable, unauthorized copies of the transmitted content from being made. Encryption is the application of an algorithm, called a cipher, that transforms the content. To recover the content, the display device decrypts the content by knowledge of the correct decryption key.

The HDCP cipher is a hybrid block/stream cipher. The block cipher operates during the authentication protocol. For content encryption and decryption, HDCP uses a stream cipher where encryption is accomplished by combining a data stream, generated by the HDCP cipher, with the transmitted content, through a bitwise exclusive-OR operation. In this way the content is protected pixel-by-pixel. Encrypted content viewed on a display device without decryption is seen as random noise, with no discernable content.

Device renewability

The HDCP system is 'renewable'. If the security of the display device has been compromised, and the secret device keys exposed, the licensing administrator places the key selection vector that matches the compromised device key on a revocation list.

The key revocation list is carried by System Renewability Messages (SRM). The host manages the SRMs, and must update them when presented with a valid, newer SRM than currently held in memory. SRMs can be presented to the host in prerecorded or broadcasted content, or received from another compliant device with a newer SRM.

IMPLEMENTATION OF HDCP

Figure 3. shows the application of HDCP to a DVI link:

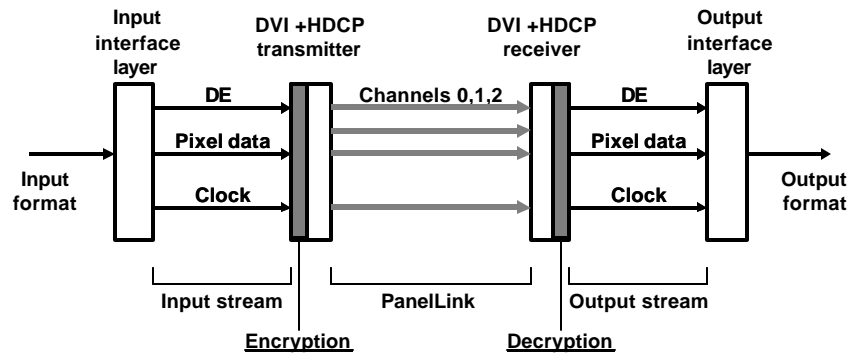


Figure 3. Application of HDCP to a DVI link

Data encryption is applied at the input of the DVI transmitter, and decryption is applied at the output of the DVI receiver. The available bandwidth of the DVI link is not compromised by the implementation of HDCP.

Figure 4. shows the components typically required for the application of HDCP to a DVI link between a PC and its display device:

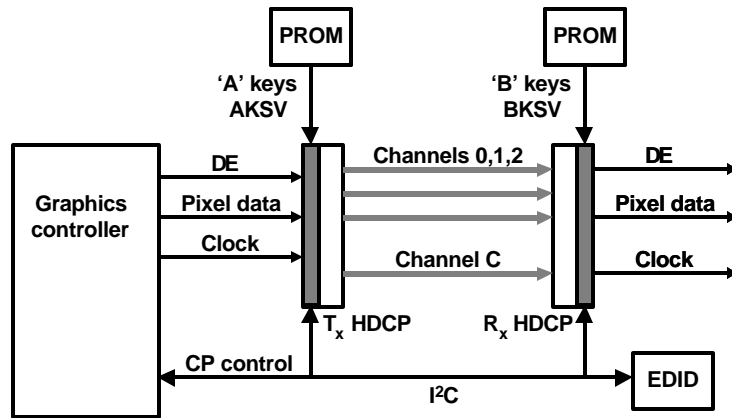


Figure 4. Application of HDCP to DVI link between a PC and its display device

The secret keys and Key Selection Vectors (KSVs) are held in the PROMs of the PC graphics card and the display device. The values that must be exchanged between the PC and the display device are communicated over the existing I²C serial bus of the DVI interface. The HDCP ciphers are implemented in the DVI digital transmitters and receivers, and add approximately 10,000 gates to each device.

For the display device, implementation of HDCP requires replacing the existing DVI receiver with a HDCP enabled receiver, and adding a small PROM for key storage. For the host system, the DVI transmitter is replaced by an HDCP enabled transmitter, a small PROM is added, and HDCP software drivers are required to support the HDCP functions.

All implementations of HDCP must be tamper-resistant and satisfy the robustness and compliance rules described in the technology license.

The first demonstration of HDCP technology was performed by Silicon Image at the Intel Developer Forum in February 2000.

CONCLUSIONS

With the release of the HDCP 1.0 specification in February 2000, the stage is set for the release of high-definition digital video to the consumer. HDCP enables a robust, protected link between a host and a display device, while taking full advantage of the industry standard, high-speed, DVI interface. Implementation of HDCP is transparent to the honest consumer, and, as no video compression is required, provides the highest quality, all-digital solution at the lowest cost.

References

1. Jack Valenti, President and CEO of the MPAA. October 28, 1999 MPAA press release
2. David Fair, Intel. Stanford Resources Flat Information Display conference, Monterey, December 1999
3. David Mentley, Stanford Resources. Stanford Resources Flat Information Display conference, Monterey, December 1999

For questions and additional information please e-mail: HDCP@siimage.com.

Silicon Image, Inc.

1060 E. Arques

Sunnyvale, CA 94086

T 408.616.4000 F 408.830.9530

www.siimage.com

© 2000 Silicon Image, Inc. All rights reserved. Silicon Image, the Silicon Image logo, PanelLink, the PanelLink logo and PixelPrecision are trademarks or registered trademarks of Silicon Image, Inc. in the United States and other countries. Other trademarks are property of their respective holders. Product specifications are subject to change without notice. Printed in the U.S.A. 2/00 SII WP-002-A