DIGITAL COMPRESSION—INTEROPERABILITY ISSUES FOR THE CABLE INDUSTRY

TV/COM International
16516 Via Esprillo
San Diego, CA 92127

Graham S. Stubbs
Consultant

Tony Wechselberger
Executive Vice President

Abstract

Standardization to achieve interoperability of digital video compression technology will require more than finalizing ISO MPEG-2 and resolving concerns about security. Interoperability goals encompass the seamless transmission of digital programming across equipment, market, and national boundaries, and include availability of equipment from multiple vendors to work on the same programs. The layered structure of digital video compression lends itself to consideration of standardization issues at the levels of compression encoding, multiplex assembly, conditional access and encryption, and processing for transmission.

This paper discusses the urgent need for the cable industry to take charge of the process of assuming that its long-term interoperability requirements will be met.

INTRODUCTION

The considerable progress in the development and adoption of ISO MPEG-2 working draft standards does not yet assure the cable industry that long term benefits of interoperability will be met. At a time when the industry is planning for, and in some cases implementing facilities to compress, multiplex, and distribute cable programming, these issues deserve urgent close attention. Interoperability and standardization are not just a matter of encryption standards—the issues are broader.

Compression Standards

Present plans for a 1994-5 roll-out call for a hybrid of MPEG and non-MPEG compression to be implemented for U.S. national distribution to cable subscribers. This approach, while appearing expedient, should receive close scrutiny regarding the long term implications for interoperability with other media, and with other consumer equipment. In addition, virtually the rest of the world is imposing MPEG-2 Main Profile Main Level edicts on systems and equipment to be used in similar applications. The alternative of a full MPEG-2 compliant approach is still achievable if the industry acts promptly.

Transport Stream Standardization

Although present U.S. cable plans do call for use of the MPEG-2 Transport Stream syntax, enough variations and designer-specific freedom is permitted within MPEG-2 that multi-vendor interoperability is by no means assured. Here the cable industry has an opportunity to narrow the options for variations within the MPEG-2 structure, such that an openly specified syntax can be used by all vendors with assurance of interoperability of equipment to which a clear (non-encrypted) MPEG-2 Transport Stream is delivered.

Encryption

To achieve broad agreement on an entire security methodology would be very difficult and possibly undesirable from the point of view of vulnerability to piracy. Nevertheless, it should be possible to develop an agreement on scrambling (i.e. the algorithm used to encrypt the transport stream packets), and yet leave the methods for key delivery (i.e. conditional access) open to continuing development, and allow employment of various proprietary methodologies, including experimentation with a variety of approaches for the use of smart cards.

In Europe, the Digital Video Broadcast Group (DVB) has already started to successfully tackle some of these issues with an objective of achieving broad interoperability. In Canada, also, there appears to be a determination to achieve a similar objective through the work of ABSOC (Advanced Broadcasting Systems of Canada).

The U.S. cable industry cannot afford to ignore the opportunity to determine its own digital future. This paper identifies the principal remaining interoperability issues in the digital arena, and suggests that industry take control of the process of assuring standardization to meet the industry's long-term needs.

INTEROPERABILITY GOALS

The context for discussing interoperability of digital compression systems cannot be as a single industry or a single country.

There will develop a *global* market for programming that is prepared and stored in digitally compressed form. Compressed programs distributed by satellite within one country will find markets in other countries within the satellite footprint. The technologies encompassed by digital video compression are global in nature, not the proprietary fiefdom of a single vendor.

Thus the principal objectives in interoperability relate to:

- Seamless exchange of programming services between media, whether Digital Storage Media (DSM) such as a file server, or transmission media such as satellite, cable, telephony, or others.
- Compatible operation of equipment that is provided by multiple vendors.

A standards-based "Open Architecture" is desired for North America. Open architectures ensure lowest cost seamless transitioning between media, and ultimately, consumer equipment. Cooperation between vendors will only occur through market forces that dictate interoperability for true multiple vendor savings and full realization of the benefits of an open architecture.

The majority of the world's consumer electronics companies have already committed to MPEG video and audio. North American cable operators, satellite program distributors, and program providers must also press for strict adherence to the standards developed under the

International Organization for Standardization (ISO) MPEG-2.

The cable industry must be allowed to realize the benefits of a truly seamless implementation of digital technology to ensure that digital video, audio, and data can be moved using the same protocols from program provider to satellite uplink, through cable systems to set-top boxes in the homes of cable subscribers. The industry cannot afford to have road blocks in the system such as proprietary, non-standard products mixed in with standard MPEG-2 elements. The industry can not at all really afford a later "upgrade to MPEG-2."

In some instances, conversion of protocol or signal format may be inevitable (for example, when converting between different modulation methods which are optimum for satellite and cable transmission). Standards choices should maintain protocol integrity, and should be consistent with minimizing the cost of such transformations.

Equipment provided by multiple vendors must be capable of operating with digitally compressed programming. **Multiple vendor cooperation should not, however, be equated with multiple licenses of a single vendor's proprietary system.** All vendors must agree to work within the MPEG-2 framework, and must further work to an open definition of all parameters necessary to achieve guaranteed interoperability. There is no place for proprietary compression /decompression technology or for compromise products which fail to deliver the full potential of MPEG-2. The proprietary approach ensures single vendor control over technological applications, stalls the development of a healthy, level, competitive playing field, and may bring only the limited resources of a single vendor to bear on problems as they develop, rather than the complementary resources of an entire industry.

LAYERS IN DIGITAL VIDEO COMPRESSION

In order to discuss interoperability and standardization issues in any detail, it is worthwhile to review the **layer concept** of the digital video compression system. Figure 1 illustrates the layer concept, starting with an inner core of program compression encoding and building through successive layers of transport transmission.

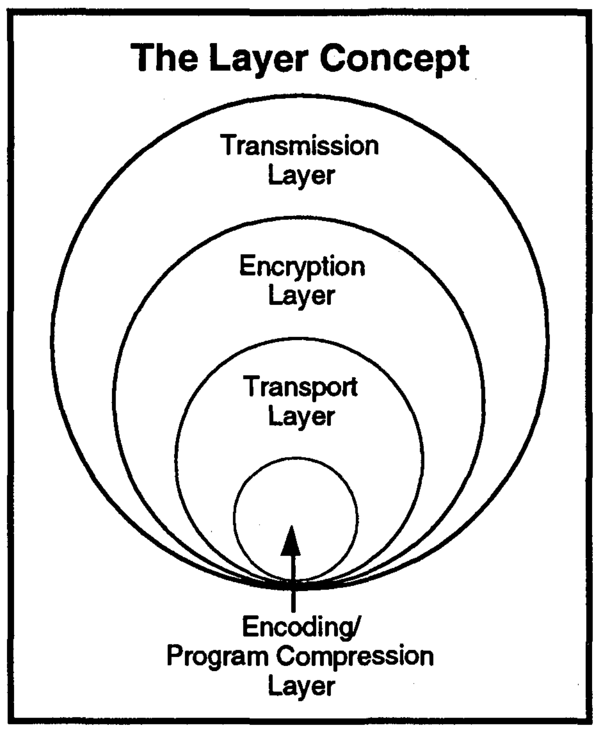

Figure 1

The **program compression encoding layer** comprises the following:

- Video compression coding, which may include intrapicture redundancy reduction and intraframe redundancy reduction/ prediction. Various coding rates achieve differing degrees of picture quality.
- Audio compression coding, based on psycho-acoustic masking. (Both Musicam and Dolby are of this type.) Various coding rates are used to achieve specific sound quality, and the number of audio channels may vary as a function of the number of languages desired and/or type(s) of audio such as mono, stereo, or surround.
- At the compression encoding layer, packetized elementary streams are formed corresponding to video, audio, and other data.
- Stream identities are created corresponding to the program source.
- Presentation time stamps are added to assure synchronized delivery of video and audio components of a given program.

In the **transport layer**, bitstreams are split into equal length packets for efficient sorting:

- Each packet carries header information to identify the content (payload) and purpose of the packet.
- Additional packets carry control and other data.
- Digitized compressed streams of transport packets can be built into a multiple program multiplex.

Security and conditional access functions are added in the **encryption and authorization layer**:

- The packetized, multiplexed transport bitstream is scrambled by performing a mathematical operation (encryption) involving another piece of digital information (an encryption key) which can be changed frequently. This operation can be applied differently to each successive transport packet.
- The keys necessary for descrambling are delivered only to authorized users and thus the processes of encryption/ decryption and program authorization and conditional access are intimately related.
- The process of key delivery/key management and general box entitlement is the "conditional access" function. Different conditional access systems can be used to deliver common descrambling keys.

The **transmission layer** prepares the compressed, packetized, multiplexed, encrypted bitstream for RF transmission:

- Since transmission channels introduce noise and distortions to digital signals, forward error correction (FEC) coding is applied to facilitate detection and correction of data errors.
- Efficient (and error-free) use of channel space is critically dependent upon the choice of RF modulation method for a given transmission medium.

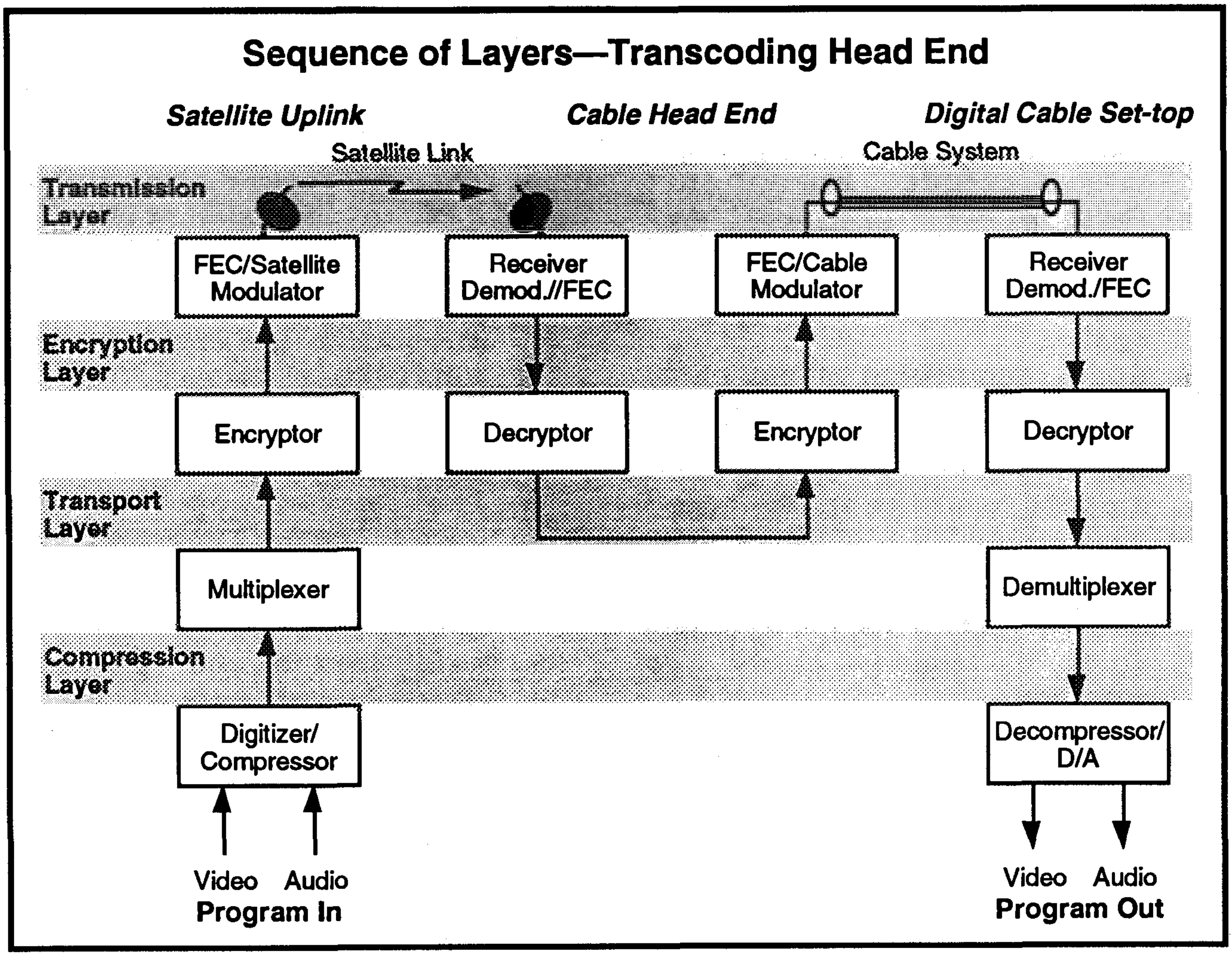

Figure 2

An illustration of the use of the layer concept in describing an end-to-end system is provided in Figure 2, which shows successive transmission through a satellite link and through a cable system. In this example, transcoding equipment at a cable head end converts from satellite modulation (e.g. QPSK) to cable modulation (QAM or VSB), and also provides for decryption and re-encryption. Note that the compression layer and transport layer as applied to the program material are unchanged.

Interoperability and standardization issues may be quite different as applied to the different layers and interfaces.

INTEROPERABILITY ISSUES

Compression Encoding

In order to assure interoperability, MPEG-2 Main Profile Main Level compression compliance is essential. The timing of MPEG-2 is no longer an issue. Cable and satellite delivery systems will, during 1994, have access to 100% MPEG-2 compliant systems. The ISO MPEG committees have now frozen all essential parameters of the world standard necessary for compression encoding, and chip vendors are nearing release of MPEG-2 compliant silicon components. The benefits of agreement on digital standards are now available and are being adopted throughout the world. Full compliance with MPEG-2 Main Level Main Profile requirements means that advantage can be taken of the maximum capacity and quality assured by MPEG-2 without the need for costly upgrades later. This is essential for cable's leading role in the national communications structure, and to compete as a global player. There is no longer any room or rationale for half measures or proprietary compression solutions.

Transport Multiplexing

Compliance with MPEG-2 is not sufficient on its own to assure seamless exchange of programs between media and interoperability of equipment supplied by different vendors. MPEG-2 can be thought of as a toolbox of rules from which selections can be made for specific purposes—particularly in the transport multiplex area. Vendor cooperation and standardization of certain of these parameters—for example, those specifying sources and destinations of programs, time synchronization of program contents, and the "hooks" for attaching encryption—are necessary to assure seamless operation.

An openly specified and complete syntax, within the MPEG-2 specification, is necessary for vendors to build equipment designed to reprocess and/or receive digitally compressed programs. The transport stream defined in the MPEG-2 standard provides coding syntax which is necessary and sufficient to synchronize the decoding and presentation of video information while ensuring that coded data buffers in the decoders do not overflow or underflow. The information is coded in the syntax using time stamps concerning the decoding and presentation of coded audio and visual data, and time stamps concerning the delivery of the data stream itself. However, the MPEG-2 rules allow the use of a number of user-selectable bits and fields. It is in this area of user-selectable data that vendor coordination is necessary—on an open, non-proprietary basis—in order to guarantee interoperability.

Encryption and Conditional Access

Encryption, security, and conditional access are not specified directly by MPEG-2, other than allowing data space with the transport for security-related and conditional access data. To achieve broad agreement on a single, overall security methodology would be both difficult, and potentially disastrous, in terms of vulnerability to piracy. Nevertheless, certain aspects of the security are candidates for standardization, including the method used to scramble the digital bitstream, and the "hooks" for retrieval of control data.

The methods used to secure satellite and cable transmissions can be decoupled (see Figure 2 for an example of decrypting the satellite signal and re-encrypting for cable distribution). The goal of a headend-in-the-sky (HITS) can still be achieved by distributing the cable addressable control data stream as a data service via satellite.

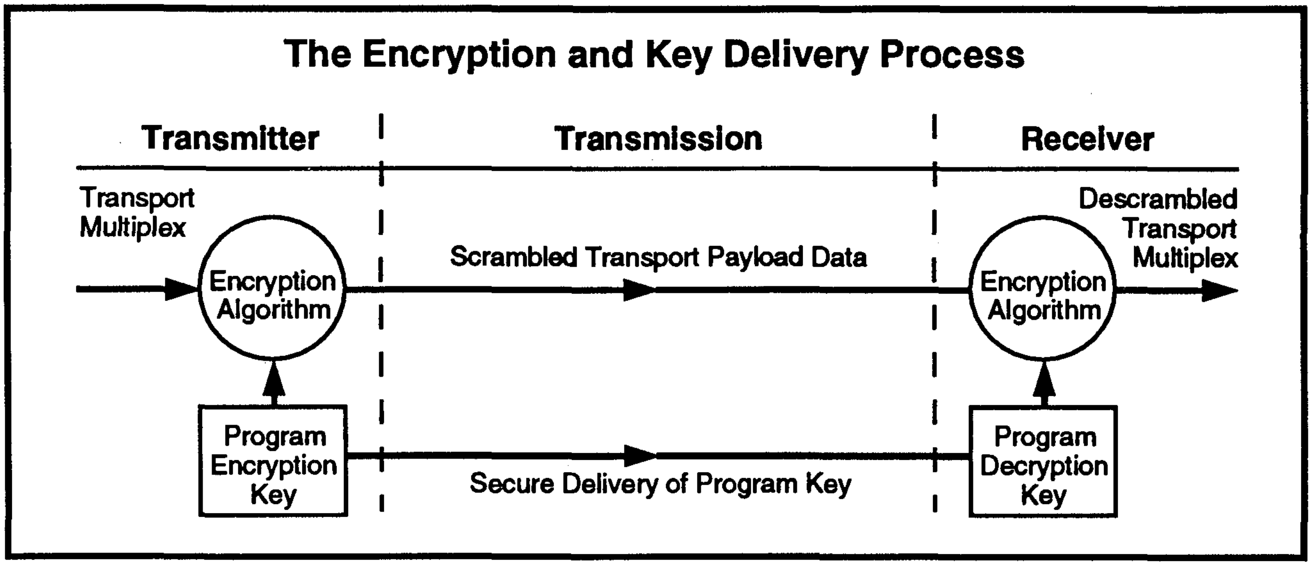

Figure 3

As can be seen from Figure 3, the process required to scramble the transport payload and the delivery of decryption keys can be considered separate. In fact, with a common scrambling method, more than one key delivery system may be employed (see Reference). Selective distribution of decryption keys is the preferred method of controlling access to programs in a digitally encrypted system. Thus key distribution can be thought of as an essential component of conditional access. Because of variances in market requirements and the potential benefit of added security, it may be desirable to allow multiple conditional access systems to coexist and operate in the same digital compression system.

The method of injecting and retrieving conditional access streams into and from the MPEG-2 transport is provided for, but not specified within MPEG-2. Two conditional access-related message types are anticipated:

- **Entitlement Management Message (EMM)**—which is subscriber specific (can also be global).
- **Entitlement Control Message (ECM)**—which is program specific.

The method for mapping EMM and ECM streams to a common program in the MPEG-2 tables must be defined, as well as agreement on the use of private data tables.

There are advantages to agreement on bitstream scrambling and on placement of EMM and ECMs. The European Digital Video Broadcast Group (DVB) has already made considerable progress in this area—its activity is a useful model for action here.

Transmission—Satellite and Cable Modulation

Transmission of high speed digital data via satellite or cable requires more than just the selection of an appropriate RF modulation method. Optimized systems apply advanced forward error correction (FEC) coding to transmissions in order that receivers can identify and correct errors caused by noise or distractions. Agreement of the transmission segment necessarily involves discussion of FEC as well.

The satellite case should appear relatively straightforward. There is broad agreement that QPSK is the satellite modulation method of choice. However, transponder bandwidths are not all the same and TDM data rates may well vary. Fortunately technology now exists to permit a receiver to work adaptively with a very wide range of received signal bandwidths and an equally wide range of data rates (e.g. 1 - 90 Megabits per second). Still, some agreement on boundaries would be helpful.

In the case of cable modulation, the case is not quite so clear. In making a selection of a modulation method for terrestrial broadcasting of Advanced Television (HDTV), the Grand Alliance and the FCC's Advisory Committee on Advanced Television Service (ACATS) selected 8 VSB based on testing of VSB and QAM techniques. These organizations also made a selection for higher data rate ATV service on cable of 16 VSB. The 16 VSB modulation is equally applicable to multi-channel digitally compressed programming. A 6 MHz bandwidth cable channel using 16 VSB modulation could be used to transmit up to 38.5 Mbps of data (useful payload).

There is also a push for the use of 64 QAM and higher order modulation such as 256 QAM for multi-channel cable transmission. A 6 MHz bandwidth cable channel using 64 QAM modulation could be used to transmit up to 28.8 Mbps of data (useful payload); approximately 35 Mbps for 256 QAM.

It may be thought that the selection of a modulation method can be dealt with on an individual cable system basis. But what happens to the ultimate possibility of putting the digital tuner and demodulator inside the subscriber's TV receiver? To achieve that objective, agreement on modulation (and associated FEC) is still necessary.

How Necessary Is Standardization?

In order to achieve:	*Compression Encoding*	*Transport Multiplex*	*Scrambling/ Scrambling Interface*	*FEC/ Modulation*
Pre-compressed delivery of programs	Essential			
Transmission between different media (cable/satellite, etc.)	Essential	Essential	Helps	
Multiple vendor sourcing of commercial satellite/cable head end equipment	Essential	Essential	Essential	Essential
Multiple vendor sourcing of consumer equipment	Essential	Essential	Essential	Essential

PRIORITIZING STANDARDIZATION

Can standards be prioritized? The need for standards is certainly most compelling at the compression encoding and transport multiplex levels. How essential is standardization to interoperability? The previous table indicates the relationship between standardization of each of the compression layers and the various needs for program exchange and the notion of multiple vendor sourcing of equipment.

CONCLUSION

The interoperability goals of seamless program delivery and multi-vendor equipment supply are achievable for the cable industry's next generation of digitally compressed video hardware. The world's leading electronics companies—including major U.S. cable equipment vendors—have made it possible for all the world's cable operators and satellite users to "drive on the same side of the road" on the information highway. Only 100% MPEG-2 compliance coupled with agreement on specific transport, transmission, and scrambling parameters will allow this to happen. Industry-wide pressure and cooperation is required to obtain the best possible technical and economic benefits in the adoption of digital video compression.

- Universal provision for MPEG-2 Main Profile Main Level.
- Openly defined and agreed upon Transport Parameters.
- Coordination of scrambling of the digital bitstream and the associated transport hooks.
- Agreement on cable modulation with the best multi-channel and HDTV transmission capacity.

REFERENCE

"Methodologies for Multiple Conditional Access Technologies in Digital delivery Systems." Tony Wechselberger and George Parkanyi. Paper presented at Canadian Cable Television Association Convention, May 1994.

About the Authors:

Mr. Stubbs is the president of Graham Stubbs Associates, a consulting firm specializing in cable television technology. He previously served in engineering and general management executive positions with Eidak Corporation, Oak Communications (now TV/COM International), and Jerrold, developing addressable technologies for the cable and satellite industries. He holds a B.Sc. in Physics and Electronics. During the past twenty years, he has authored numerous technical papers in the cable field, and holds several key patents in conditional access and signal security.

Mr. Wechselberger has held various positions with TV/COM International (formerly Oak Communications) since 1980. His staff supports all of TV/COM's cable, satellite, and compression engineering initiatives and he is responsible for a number of key patents. Before joining TV/COM, Mr. Wechselberger was with the General Dynamics Electronics Division. He holds B.S. and M.S. degrees in Electrical Engineering and has published and lectured extensively in the fields of TV signal security, and general conditional access requirements involving communications, and encryption.