Apple Computer Inc. v. Burst.com, Inc. Doc. 75 Att. 7

Video Scrambling & Descrambling

for Satellite & Cable TV

Second Edition

Rudolf F. Graf and William Sheets

Newnes

Boston, Oxford, Johannesburg,
Melbourne, New Delhi, Singapore

Dockets.Justia.com

Newnes is an imprint of Butterworth–Heinemann.

Copyright © 1998 by Rudolf F. Graf and William Sheets

A member of the Reed Elsevier group

All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the publisher.

Recognizing the importance of preserving what has been written, Butterworth–Heinemann prints its books on acid-free paper whenever possible.

Butterworth–Heinemann supports the efforts of American Forests and the Global ReLeaf program in its campaign for the betterment of trees, forests, and our environment.

Library of Congress Cataloging-in-Publication Data

Graf, Rudolf, F.
Video scrambling & descrambling for satellite & cable TV / Rudolf F. Graf and William Sheets.—2nd ed.
p. cm.
Includes index.
ISBN 0–7506–9997–3 (alk. paper)
1. Direct broadcast satellite television—Scrambling systems.
2. Cable television—Scrambling systems. I. Sheets, William.
II. Title
TK6677.G73 1998 98–25978
621.388'5—dc21 CIP

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library.

The publisher offers special discounts on bulk orders of this book.
For information, please contact:
Manager of Special Sales
Butterworth-Heinemann
225 Wildwood Avenue
Woburn, MA 01801-2041
Tel: 781-904-2500
Fax: 781-904-2620

For information on all Butterworth–Heinemann publications available, contact our World Wide Web home page at: http://www.bh.com

10 9 8 7 6 5 4 3 2

Printed in the United States of America

replaced. If the boxes were out of warranty, there sometimes was a big charge for a replacement. The replacements always were the latest "hacker proof" models. Therefore, earlier, more easily hacked models, as well as pirates, could be taken out of circulation.

Wizard Hack

The wizard hack consisted of rewriting the operating system software to ignore hits, which are periodic updates sent on the data stream. However, a box needs these updates once a month or so to keep running as new keys are periodically sent. It happens that the software algorithm used to decrypt key information in fact could be used in a reverse manner to decode the internal authorization subkeys the box uses to authorize itself. This software was taken from the decryption processor U7 and modified by hackers to do this.

In the wizard hack, no seed keys or authorization number is needed to operate. A legally operating VideoCipher is used to collect the hits from the data stream. The data are fed into another modified VideoCipher or a separate computer to derive the "wizard numbers." These numbers are then entered into the VideoCipher unit via the front keys on the unit. The wizard box has no ID or keys itself and therefore cannot be addressed via the data stream and shut off.

The wizard box soon was upgraded to have its own keys and ID, which were encrypted to prevent discovery, along with a backup clone in case the ID number went bad. The new box could extract and store new authorization data and was set up so that a keypad entry could produce a screen dump of the data for other units. The newer version VCII+ reportedly deals with this "problem" and is more difficult to hack than its predecessors. However, the cat and mouse game is sure to continue as new hacks are discovered.

B-MAC System

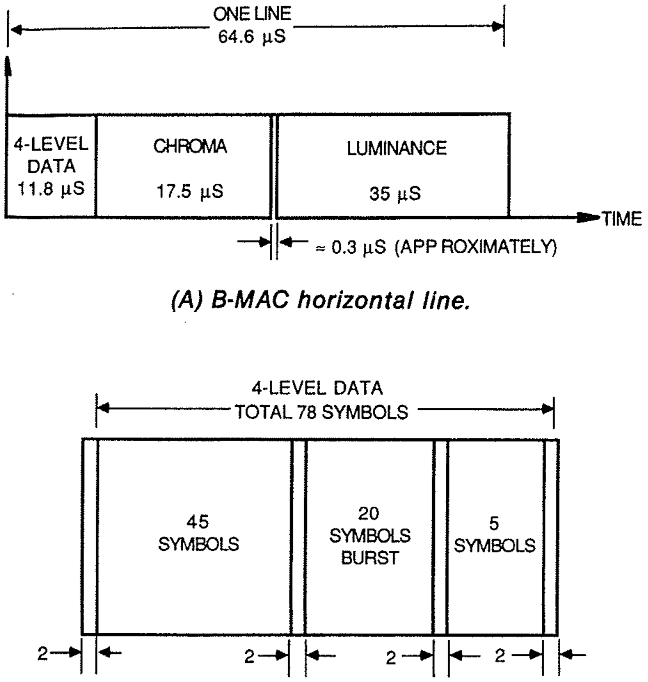
Scientific Atlanta has a system known as *B-MAC*. This is a transmission format (MAC stands for multiplexed analog components) that uses a time-division multiplex (TDM) of analog luminance and chrominance components. While this system is falling out of favor as digital transmission and HDTV are coming into use, it has several interesting technical features and is well worth discussing. For satellite transmission methods, using FM, the NTSC signal spectrum does not make the best use of the FM channel from a signal-to-noise standpoint. A saturated color in a televised scene may overdeviate the transmitter. This causes "sparklies" to appear in these areas of the picture when low-cost satellite receivers, using less than full video bandwidth, are employed. Also, the signal-to-noise ratio is poorest for chroma due to the noise distribution in the FM channel. The B-MAC system uses TDM techniques to circumvent this inherent difficulty.

Basic Theory

Time-division multiplex is the principle of sending portions of several information channels in a timed sequence. For example, a TDM system can send the information content of an NTSC signal in several time-sequenced groups. Synch can be sent, followed by the chrominance information, and then the luminance. The data can be stored, combined, and converted to video. In addition, multilevel data (security, addressing, stereo audio, teletex, etc.) can be sent along with the synch information. NTSC signals are frequency-division multiplex (FDM) in nature. All data are sent at the same time (chrominance, luminance, color burst, audio, etc.) on different frequencies; that is, on the picture carrier, color subcarrier, and sound subcarrier. Because subcarriers can be eliminated in a TDM system, crosstalk and intermodulation between components is no problem, since the components are not present at the same time.

Since the same rate of information transmission (the TV program) is required, the need for sequential transmission of the various components requires their time compression (Figure 10–3). On a satellite channel, the bandwidth necessary to do this is available. *Time compression* is an exchange of time for bandwidth. For example, if we play a record twice as fast, all audio is doubled in frequency and the record takes half the time to play. Twice the audio bandwidth is needed in this case. This process also is used in tape duplicating to speed up production. It should be an obvious concept to anyone who has ever played a record or tape at a speed other than the one at which it was recorded.

Another benefit of B-MAC is that, since the chrominance signal is at the baseband, the noise performance of the chroma channel is improved. By transmitting only one chroma component per line, either (R-Y) or (B-Y), chroma transmit time can be reduced 50%. This makes the storage of chrominance information necessary at the receiver, either digitally or using analog methods. The chrominance signals are filtered to restrict bandwidth to 2 MHz or less. The (R-Y) and (B-Y) components are band limited, and alternate data samples are discarded to reduce the data rate to about seven samples per microsecond. A data rate of 14.31818 MHz is used, since it is better suited to NTSC translation (four times 3.579545). For digital video, a clock rate of 13.5 MHz has been recommended for studio use of component-coded digital video. This, after discarding alternate samples, gives 7.16 samples per microsecond. The (R-Y) and (B-Y)



(A) B-MAC horizontal line.

(B) Data format.

Fig. 10-3. Time compression of video components.

samples are stored in 384-byte memory. By reading out the memory at 7.16 MHz × 3 = 21.48 MHz, the signals can be time compressed to 17.5 µs. Using a similar method, the luminance signal is compressed to 35 µs. This leaves about 11.5 µs for the data.

The data rate used is 1.86 Mbits per second for the data, audio, and synch. The data pulses are two- or four-level symbols during the blanking intervals. Actually, 1.573 Mbits/s are provided during the horizontal blanking intervals, and the six digital audio channels take 1.510 Mbits per second. The remaining 62.5 kbits are used for a utility data channel. This data channel is encrypted and controlled by the broadcaster for utilization by each user. Unused audio channels can be used as data channels. The six audio channels are Dolby®* digital audio and use 251.7 kbits/s, including error coding. The frequency response is 20 Hz–18 kHz at a 30-dB bandwidth. The audio channels can be encrypted and decrypted separately.

The vertical interval contains all the control data synchronized with the four-level data in the horizontal lines. The first lines (1–8) carry control data for synch and for clock data recovery. The synch is on only one line in the vertical blanking interval and allows receiver lockon at only 1-dB carrier-to-noise (c/n) ratio of the received signal. Lines 9–13 contain teletext information, with 40 ASCII characters per each line.

Modes of Operation

The B-MAC system also provides for up to 256 million addresses, or about 1 million per hour, with redundancy. Decoders contain multiple addresses for independent programmers. Audio and data can be DES encrypted, with keys and codes changing four times per second.

Video scrambling is accomplished by a time-shifting process on each line. The width of the digital data packet can be varied, sending more data on one line than on the preceding line (or less). This either delays or advances the start of each line, producing a slewing of the individual lines (Figure 10–3). No data are omitted—merely sent in advance or saved for later. This effectively scrambles the picture. Descrambling is done by reversing the process. Since merely the transmission time is shifted, no loss in picture quality occurs.

The B-MAC system has a technical edge on noise performance. The threshold of the system is defined as the c/n ratio at which the FM demodulator used in the system produces 100 "clicks," or cycle slips, per second, with a 24-MHz BW IF system (±1 dB). Above the threshold, the B-MAC chrominance signal is 8.3 dB better than the B-NTSC. Audio performance on three of the six audio channels essentially is perfect at c/n ratios down to 6.7 dB, with a total loss at about 4.7 dB.

Conclusion

The B-MAC system has been used for program distribution to TV stations and for use in certain nations. It is being discontinued, in some parts of the world, at this writing. The system is an alternative to VCII and has technical merit with regard to color quality.

* Dolby is the registered trademark of Dolby Laboratories, Inc.