BBC RD 1995/11

BBC RESOURCES

Research and Development Report

LINE SHUFFLING: Development of a scrambling system for terrestrial UHF television broadcasts

A.J. Bower, M.A. Ph.D., C.Eng., M.I.E.E.,
C.K.P. Clarke, B.Sc.(Eng.), A.C.G.I. *and*
A.P. Robinson, B.Sc., A.R.C.S.

Research and Development Department
Technical Resources
THE BRITISH BROADCASTING CORPORATION

LINE SHUFFLING: Development of a scrambling system for terrestrial UHF television broadcasts

A.J. Bower, M.A., Ph.D., C.Eng., M.I.E.E., C.K.P. Clarke, B.Sc.(Eng), A.C.G.I.
and **A.P. Robinson, B.Sc., A.R.C.S.**

Summary

This Report describes the development of a scrambling system for overnight downloading of television programmes to video cassette recorders – the BBC Select service.

The scrambling techniques used successfully for many years for satellite broadcasting and cable distribution are often unsuitable for UHF terrestrial broadcasting using VSB-AM. This is because of the constraints of equipment, such as main station transmitters, teletext data regenerators and sound-in-syncs codecs in the broadcast chain. It is, therefore, necessary to use a scrambling system in which the scrambling effect is confined to the active picture regions of the signal, so that the normal synchronising and blanking waveforms are maintained. When the additional requirements of good security and a highly scrambled appearance are added, only two broad techniques remain, the first variously known as Active-Line Rotation, Line Cut and Rotate, or just Line Rotation, and the second known as Line Shuffling or Line Permutation.

In comparative over-air tests of the two systems, the line rotation technique proved particularly vulnerable to multipath propagation, an impairment that could affect as many as 25% of receiving locations. Line shuffling showed susceptibility to hum and field-rate distortions of the television waveform, but the effects could be minimised by optimising the time-constant of receiver AGC and clamp circuits, and by choosing an appropriate shuffling block structure.

A line shuffling system using blocks of 47 lines was developed which operated satisfactorily over most of the UHF transmitter network, although the system did show an increased vulnerability to co-channel interference, compared with normal PAL signals.

Issued under the Authority of

Research & Development Department,
Technical Resources Division
BRITISH BROADCASTING CORPORATION

General Manager
Research & Development Department

(T-35)

1995

LINE SHUFFLING: Development of a scrambling system for terrestrial UHF television broadcasts

A.J. Bower, M.A., Ph.D., C.Eng., M.I.E.E., C.K.P. Clarke, B.Sc.(Eng), A.C.G.I.
and **A.P. Robinson, B.Sc., A.R.C.S.**

LINE SHUFFLING: Development of a scrambling system for terrestrial UHF television broadcasts

A.J. Bower, M.A., Ph.D., C.Eng., M.I.E.E., C.K.P. Clarke, B.Sc.(Eng), A.C.G.I.
***and* A.P. Robinson, B.Sc., A.R.C.S.**

1. INTRODUCTION

1.1 Previous work on signal scrambling

For several years now, many different signal scrambling techniques have been used for television, mainly in the context of satellite and cable services[1]. In the BBC, involvement in the development of standards for direct Broadcast Satellite services led to work at Research Department on the application of scrambling techniques in Multiplexed Analogue Component (MAC) signals. This work[2] was instrumental in the choice of parameters for the component rotation scrambling methods adopted for the MAC/ packet family of coding standards[3]. The work also included the development of a demonstrator system (described in Ref. 2) based on the closely related Active-Line Rotation scrambling method (sometimes known as Line Cut and Rotate or, simply, Line Rotation) applied to System-I PAL signals. Related work was directed towards the Conditional Access (CA) system[4, 5], by which the descrambling process is controlled. More recently, technical advice has been provided on the choice of scrambling systems to carry a PAL-based BBC programme service on satellite (BBC TV Europe, subsequently superseded by BBC World Service Television using D2-MAC)[6].

Also, for several years the BBC has been considering methods of scrambling applicable to the normal terrestrial UHF television broadcasts. The direct application of this work was in the introduction of subscription services for broadcasting to domestic video cassette recorders (VCRs), using the night time hours when the transmitter networks were normally switched off. This technique is known as 'Down-loading'[7]. However, an important indirect feature of the work has been to provide the background technical knowledge to support discussions on alternatives to the Licence Fee system of funding for the BBC.

In 1986, initial experiments in downloading explored the possibility of electronic distribution of film material, in which the intention was to record the signals in scrambled form on home VCRs. This had the advantage that the period of replay could be controlled by the programme provider, allowing for subsequent marketing in other media. Although many scrambling techniques were considered, distortion of the scrambled signals by the domestic VCR made the problem of obtaining good descrambled picture quality off tape too difficult in a low-cost decoder.

Although the film application was not pursued, the concept of downloading to VCRs was switched towards professional applications in which the BBC would act as the carrier for services funded by advertising or sponsorship. In this case, the main requirement for the scrambling system was to make the programme content, invisible to the normal viewer; this was particularly true for the advertisements, to ensure that an adequate distinction could be made from the BBC's licence-fee funded services. At this time the BBC was being encouraged to apply market-tested solutions to scrambling systems for this new application. After a period of test and development, which included instrumentation of a method for automatically controlling the VCR to record when the decoder detected a scrambled programme[8, 9], a descrambler, based on the Discret-1 video scrambling technique[10], was chosen. Discret-1 had been used with considerable success in France for terrestrial broadcasts by the pay-television channel Canal Plus. Using the system, the BBC started experimental night-time broadcasts for doctors[7] in February 1988, with programmes provided by British Medical Television Ltd. (BMTV), but later these ceased as a result of financial difficulties at BMTV.

1.2 The BBC Select service

Despite the failure of the BMTV service, the BBC was sufficiently encouraged by the level of interest in the downloading technique to form BBC Subscription Television Ltd. This was intended to provide a more broadly based range of programme services, principally funded by subscription and collectively known as BBC Select. Although Discret-1 had proved adequate for the BMTV application, there were benefits in providing a new generation of downloading equipment for the BBC Select Service. Several groups of manufacturers responded with proposals for the system, and VideoCryptTM, a joint product[11, 12] of Thomson Consumer Electronics and News Datacom was chosen.

VideoCrypt in its original form, for satellite applications, uses line rotation scrambling. However, previous work by Research Department, carried out during the selection of a system for the broadcasts for doctors, had shown that the line rotation technique could be susceptible to distortions commonly

encountered in terrestrial broadcasting. Trials, carried out by Research Department at the request of BBC Select, confirmed that this susceptibility made VideoCrypt unsuitable for their particular application. The Department therefore carried out further work, by advising the use of a different technique of picture scrambling, known as Line Shuffling; also to optimise the shuffling system parameters to achieve good descrambled picture quality over a wide range of terrestrial broadcast impairments. The line-shuffled downloading system used by the BBC Select service is known as VideoCrypt S™.

The main features of the BBC Select playout systems shown in Fig. 1(a). The night-time transmission requires a high degree of automation for efficient operation, so a programmable playout controller system, developed by BBC Design and Equipment Department*, is used to control the video tape replay. The signals are scrambled for transmission before being passed to the network output. The scrambling encoder, also developed by BBC Design and Equipment Department, uses line shuffling for the picture signals, and spectrum inversion for the sound (described in Section 6). The Subscriber Management Centre provides the interface with the public, handling requests for subscriptions, receipt of payments and the distribution of authorised smart cards to subscribers. Subscription changes are conveyed to the Security Database Computer at Television Centre. The subscriber data from the database is combined with service data (programme codes, channel identification and scrambling mode), encoded by the Security Encoder Computer for security and error protection, and then finally inserted into the video signal by the scrambling encoder. The VideoCrypt software for the security computers was provided by News Datacom and has many similarities to the system used for VideoCrypt satellite broadcasts. The encoding and playout arrangements are duplicated for back-up purposes and for the two networks, making four encoders in all.

The receiving arrangements, shown in Fig. 1(b), consist of an integrated receiver/decoder (IRD) unit, manufactured by Thomson Consumer Electronics, a VCR with infra-red remote control and a normal domestic television receiver. The installer tunes the pre-settable channels of the receiver/decoder to the local BBC channels and configures the unit with the appropriate infra-red codes to match those of the user's VCR. Also, the installer connects the decoder output to the VCR, either using a vacant UHF channel, or by a baseband Scart connection. Authorisation to record particular programme services is provided by a smart card plugged into the receiver/decoder unit. This can either by supplied pre-programmed from the Subscriber Management Centre, or can be authorised for additional services by over-air data signals. The receiver/decoder unit includes a UHF bypass path, so that the VCR and television set can be used normally, when not in use for a BBC Select recording. Fig. 1(c) shows a BBC Selector installed with a television receiver and a VCR.

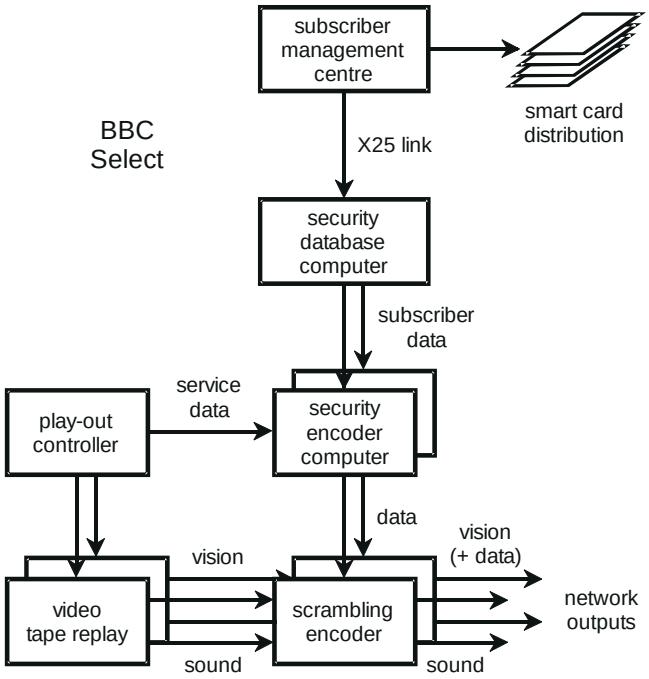
During the day, the receiver/decoder unit is in a powered-down, stand-by mode. At night, when switched on by an internal clock, the unit automatically tunes through the pre-set channels, monitoring the signals for the presence of VideoCrypt data. When such a signal is found, the unit remains tuned to that channel, so than any subscription updates or messages can be received and decoded by the microprocessor in the smart card. When used for the BBC Select service, identical transmissions of subscriber authorisation data are made on the BBC1 and BBC2 channels. When a programme for a service to which the viewer subscribes is about to be broadcast, the receiver/decoder re-tunes, if necessary, to the channel on which the broadcast will take place, and sends infra-red codes to the VCR to start recording the descrambled signals. When the programme has finished, the VCR is switched off by the infra-red codes and the receiver/decoder continues monitoring the data, ready for further transmissions. The recorded programme can then be replayed when convenient.

1.3 Description of the development work

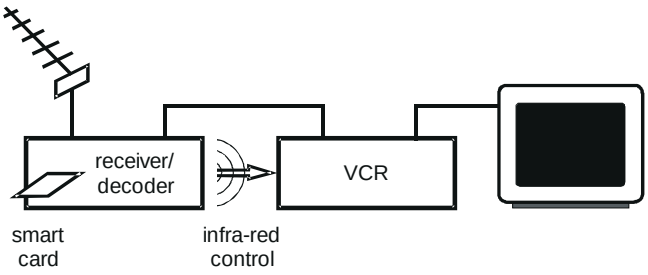
This Report provides an overall description of the work carried out at Research Department to develop the line shuffling scrambling technique for the BBC Select service. It includes, as an Appendix, a brief specification of the scrambled BBC Select signal. This specification is necessarily incomplete, because a more detailed description might prejudice the security of the conditional access system.

The development work commenced in May 1990 with computer simulations of line-shuffled pictures. In September 1990, the decision was taken to construct experimental hardware to allow broadcast tests of line shuffling to be made. This flexible hardware, completed and tested over-air during December 1990, allowed a wide range of shuffling parameters, such as the block size and structure, to be tested. The system was also used in January 1991 for over-air comparison tests between line shuffling and a line rotation scrambling system, in which the line shuffling system proved superior. Duplicates of the experimental coder and decoder were constructed and further tests, designed to assess the performance of line shuffling over network links, were carried out in April 1991 at

* Now combined with Research Department and known as BBC Research & Development Department.



(a)



(b)

(c)

Fig. 1 - The BBC Select system.

Block diagrams showing (a) signal sourcing arrangements and (b) reception equipment. A BBC Select decoder in a practical setting with a television receiver and VCR is shown in (c)

the Midhurst transmitter in West Sussex. As a result of these tests, the parameters of the line shuffling system for the BBC Select service were agreed with Thomson Consumer Electronics in May 1991, and BBC Research Department then started construction of prototype hardware using these parameters.

Initially, one coder and six receiver/decoders were constructed; but later, a duplicate coder was built to assist the testing of prototype decoders at Thomson Consumer Electronics. The experimental coder and decoder, built for the initial tests, were also modified so that they could alternatively be used as baseband input decoders (without tuners) for the second generation equipment. By using the free-access scrambling mode, the equipment implemented the full specification of the video scrambling and data system, apart from the proprietary News Datacom access control. Sound scrambling was also omitted. The multiple decoders allowed an extensive programme of network tests to be made during November and December 1991, during which the performance of the system over approximately half the main station transmitters was checked directly. Further brief investigations into network distortions were carried out during April 1992 at BBC Manchester and at the Winter Hill transmitter in Lancashire.

2. SCRAMBLING TECHNIQUES FOR TERRESTRIAL APPLICATIONS

Before reviewing the suitability of particular scrambling techniques for use in a terrestrial broadcasting environment, it will be helpful to examine, in very general terms, the functions that a conditional access system seeks to fulfil and the performance criteria by which its effectiveness may be assessed.

2.1 Conditional access

Any conditional access system for television combines two main functions: signal scrambling and access control. Signal scrambling renders conventional reception of the picture and sound signals unsatisfactory, while the access control system provides the means for authorised viewers to descramble the signals. In the context of the BBC Select conditional access system, the picture scrambling process consists of transmitting the lines of the video signal in an apparently random order, while the access control system provides the means to produce, at the descrambler, the inverse of the sequence used to permute the lines. Thus, the data signal carries, in encrypted form, information used to initialise the permutations produced by the descrambler. To be used in the descrambler, the synchronising information has to be decrypted by the smart card, which applies separate keys to authorise individual services. The work reported here deals almost exclusively with the signal scrambling aspect of conditional access.

2.2 General requirements of a scrambling system

The effectiveness of a scrambling system can be assessed in terms of the follow parameters:

2.2.1 Transparency

The term transparency is used to reflect the degree of signal impairment that results after scrambling and descrambling. Scrambled signals are frequently more sensitive to distortion than normal signals; so that for a given level of distortion, the impairment to a scrambled and descrambled signal may be significantly more noticeable than the impairment occurring with a clear (non-scrambled) signal.

2.2.2 Opacity

In terms of a picture signal, the opacity indicates the extent to which the picture information is made unrecognisable by the scrambling process. Accordingly, the more opaque scrambling methods reveal less information about the picture. Similar terminology is used to indicate inability to recognise scrambled sound signals.

2.2.3 Security

There are many aspects of security in a conditional access system, but when applied to a scrambling system, this is an indication of how difficult it is to descramble the signals without reference to the access control data. Usually, this depends on the number of possible variations that the scrambling method can introduce, coupled with the presence or absence of tell-tale features in the scrambled signal that might provide clues to the descrambling process.

It is widely accepted that any conditional access system can be defeated, given sufficient resources. In a broadcasting application, therefore, it is appropriate to choose a level of security sufficient to ensure that unauthorised descrambling will remain economically unattractive throughout the lifetime of the system.

2.2.4 Cost

The economic viability of a conditional access service tends to be influenced primarily by the initial cost of the decoder. This is because the decoder has to be provided before any programmes can be received. In broadcast applications, because the number of decoders tends to be large, the cost of the decoders is often the overriding cost in the whole system.

2.2.5 Compatibility

The compatibility of a scrambling technique reflects the degree to which the scrambled signals can be used with existing equipment, originally intended for use with normal signals. In terrestrial broadcast applications, compatibility with the existing distribution system and transmitters is particularly important.

2.3 Terrestrial network constraints

The broadcast networks for the BBC's two terrestrial channels consist of transmitters at over one thousand sites, fed by a complex system of point-to-point distribution links and re-broadcast relays. The networks have been optimised over a period of many years for carrying System-I PAL signals, so the introduction of scrambled signals with different characteristics and sensitivities could represent a significant departure from this. The diversity of equipment types and the scale of the networks dictates that making changes to accommodate scrambled signals would be costly. However, conditional access transmissions from satellites have been used satisfactorily for PAL signals over a period of many years, based on many different scrambling methods. So what are the differences?

Perhaps the most fundamental difference is that satellites generally use Frequency Modulation (FM) for PAL transmissions, while the terrestrial network uses Vestigial Side-Band Amplitude Modulation (VSB-AM). This gives satellite transmission two important advantages: FM provides much better amplitude linearity than AM, particularly high-power AM transmitters; VSB-AM depends on accurate amplitude-frequency characteristics, which tend to be degraded, partly by imperfect instrumentation and partly by propagation impairments, for example, multipath distortion. Thus, while VSB-AM can given satisfactory quality for normal PAL signals, there are many more mechanisms for introducing low-level distortion to the signal than with FM.

Another important feature of the terrestrial network is the use of Sound-in-Syncs (SIS) for distributing sound to line-fed transmitters. With this system, digitally-coded sound is placed in the line sync period of the video signal for distribution, and then decoded and replaced for broadcast, at the transmitter, by normal synchronising pulses. Clearly, such a system relies on having normal synchronising pulses at the network input.

In addition, the normal field interval waveforms have to be maintained. There are now no unused lines in the field blanking periods of BBC terrestrial PAL transmissions. Apart from the field sync waveforms, all the lines are allocated to teletext or test waveforms. The presence of teletext data regenerators at several points in the network limits the scope for replacing these waveforms with other data signals.

Other constraints arise because of klystron pulsing, a technique of energy-saving in high-power negative modulation transmitters. As a result, only chrominance signals can extend below black level without distortion. For this and other reasons, the correct operation of the transmitter depends on the signals remaining within the normal luminance and chrominance ranges.

The overall effect of these constraints is to dictate that only scrambled signals that maintain the normal PAL waveform, including synchronising waveforms, blanking periods and signal amplitudes, can be considered. Similar constraints of level and bandwidth also apply to the sound signals. Thus, the scrambling effect has to be confined to the active picture information. Furthermore, any data signals required by the conditional access system either have to conform to the teletext data format, or have to be accommodated within the active picture period.

These constraints immediately rule out many of the techniques commonly used for scrambling satellite transmissions, such as sync suppression or modification. Also, the poor linearity of the terrestrial networks is a disadvantage for scrambling methods that invert portions of the waveform on a time-varying basis. This leaves only a few compatible methods, such as the line displacement technique of Discret-1, which has poor security and limited opacity; active-line rotation, which is considered in Section 3; and line shuffling, which is described in Section 4.

A further difficulty of compatibility will arise when parts of the distribution network are replaced by digital links based on bit-rate reduced signals. Signal scrambling, by its very nature, tends to destroy much of the picture redundancy exploited by bit-rate reduction techniques. This leads to poor coding accuracy and distorted pictures, to an extent that the most effective picture-scrambling techniques, and the most effective bit-rate reduction techniques, are completely incompatible. A pragmatic, but high-cost, solution is to move the scrambling process, so that each line-fed transmitter has its own scrambling encoder.

2.4 Digital scrambling

An alternative to this approach, not so far mentioned, is the possibility of digital terrestrial broadcasting of television. Digital methods offer the possibility of overcoming the distortion disadvantages of terrestrial transmission by encoding the television signals as a

digital bit-stream. In this form, the signals can be scrambled simply by modulo-addition of a pseudo-random binary sequence to the bit-stream, without incurring any of the extra sensitivity to distortion that tends to occur with analogue scrambling techniques. The security of digital scrambling could be made very high and the opacity would be expected to be good. Transparency and cost would depend on the efficiency of the digital coding method. The difficulty is that, although such broadcast emission systems are being considered for the future[13], they would not be directly compatible with existing broadcast networks. When developed, however, such systems could incorporate secure, opaque and transparent conditional access at minimal extra cost.

A compatible digital system could be produced, bearing in mind the constraints detailed in Section 2.3, by replacing the active-picture information of the normal television waveform by a digitally-modulated bit-steam signal. With a reasonable measure of ruggedness, this could yield a data capacity of the order of 10 Mbit/s, similar to the data rates currently being achieved for conventional television formats, by sophisticated bit-rate reduction algorithms. If integrated circuits for bit-rate reduction decoders were produced at low cost, such an approach would form the basis for a viable method of compatible signal scrambling.

3. LINE ROTATION SCRAMBLING

The earliest description of the line rotation scrambling technique is contained in a patent[14] filed by Westinghouse Corporation. Rights to this patent now form part of the MAC system patent package. Development work on line rotation was carried out in France,[15, 16] during the late 1970s, where the system was known as Discret-2. During the early 1980s, the system was applied to MAC signals, and was referred to as component rotation[3]. During the mid-1980s, commercial conditional access systems using line rotation picture scrambling of PAL including the DAVE system in Belgium, Cryptovision in Norway[17], and VideoCrypt in France[11].

3.1 Description of the technique

The waveforms of line rotation scrambling are shown in Fig. 2. The scrambling process consists of first selecting a cut point from a large number of pre-determined positions in the active-line period of the television signal. Then the two parts of the line on either side of the cut position are interchanged, so that the second part of the line precedes the first, as shown in Fig. 2(b). The original positions of the two parts of the line are then reinstated at the descrambler. When a different cut position is selected on each line,

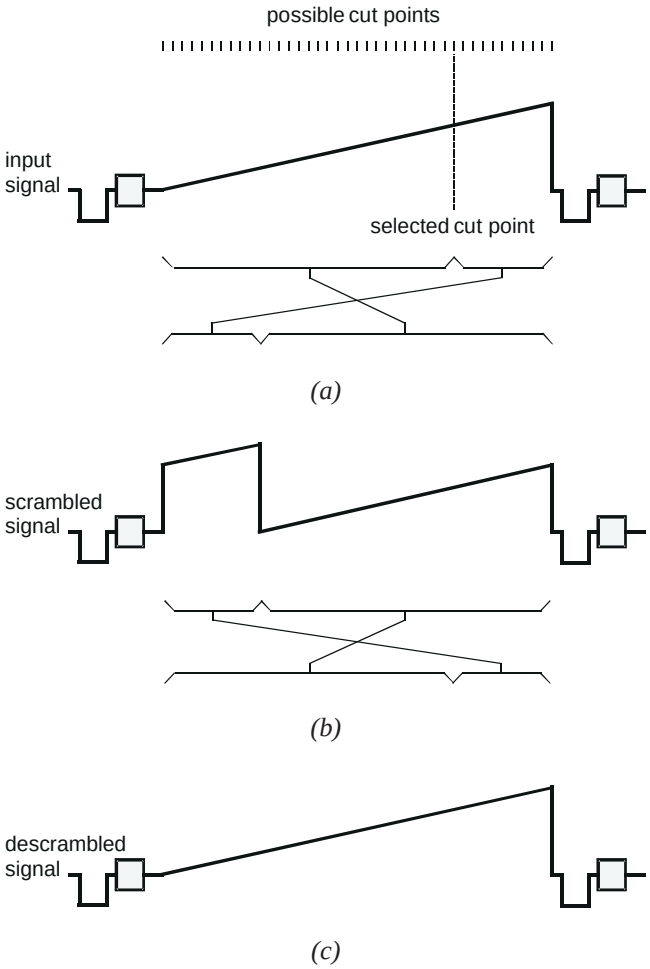


Fig. 2 - Line rotation scrambling.

The active line of the input signal shown in (a) is divided into two parts which are then interchanged to produce the scrambled signal, as shown in (b). The descrambling process consists of restoring the two parts of the line to their original positions (c).

according to an apparently random sequence, this results in a high opaque from of scrambling, as shown in Fig. 3. Although only two segments are shown in Fig. 2, the Westinghouse patent recognises the possibility of using more than one cut point in each line.

A conventional method of implementing a line rotation scrambler is to sample the incoming signal and to write the values into one of a pair of line stores, as shown in Fig. 4 *(previous page)*. During the next line, the store addresses are modified for reading according to the cut position, so that the samples corresponding to the second part of the line are read out first, then followed by the first part of the line to complete the scrambled line. At the same time, the incoming line is being written into the second store. A similar arrangement can be used in the descrambler. Alternatively, the method can be implemented using shift registers with a recirculating connection from output to input, a technique which emphasises the 'rotation' feature.

(a)

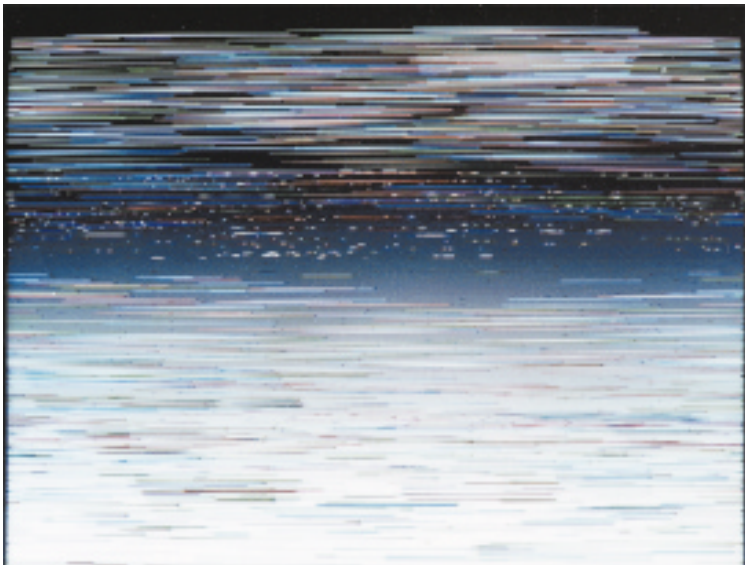
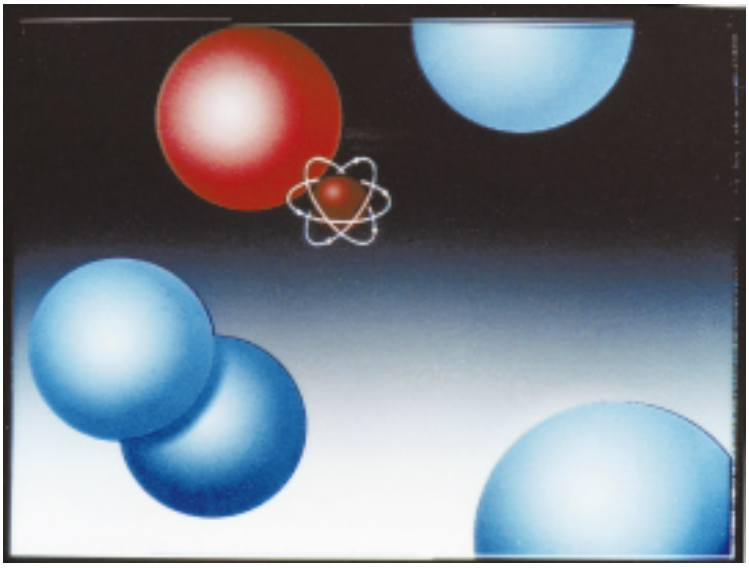


Fig. 3 - Line rotation scrambling using the prototype equipment described in Ref. 2, which uses one of 64 possible cut positions on each line.

(a) the scrambled picture and (b) the descrambled picture.

(b)



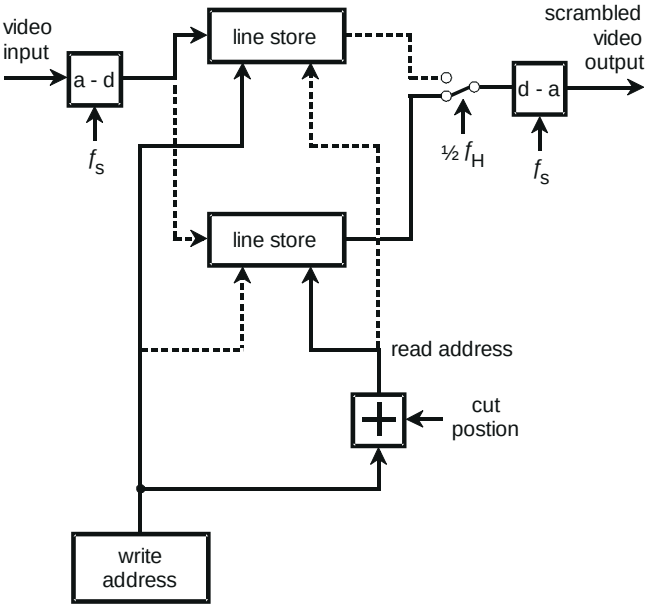
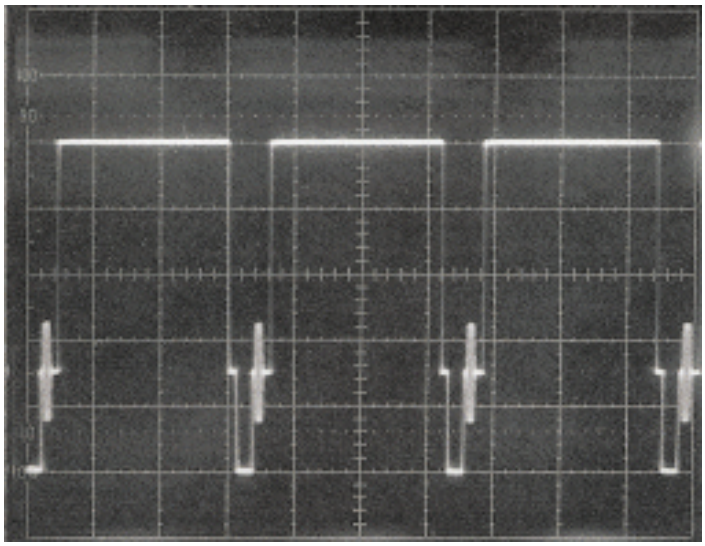
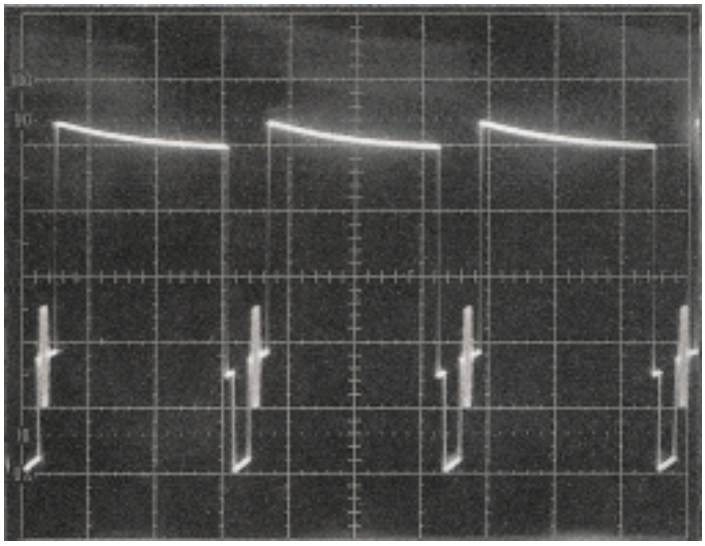


Fig. 4 - Block diagram showing the main features of a line rotation scrambler.



(a)



(b)

Fig. 5 - Line tilt.

(a) a normal signal and (b) a signal affected by exaggerated line tilt.

In practice, the line rotation process is more complicated than this, requiring the region surrounding the cut point to be transmitted twice to provide an overlap. Also, it is necessary to shape the transitions of the line segments to avoid the effects of distortion and to ensure security. These features are described in more detail elsewhere[2, 17].

3.2 Sensitivity to line tilt

Line tilt describes the effect in which the video signal does not maintain a fixed black level reference throughout the line period, thus resulting in a slope or tilt from one end of the active line period to the other. This is shown in an exaggerated form in Fig. 5. Small amounts of line tilt can arise in the UHF transmission chain from a variety of causes, such as inadequate low frequency response, perhaps resulting from the vestigial sideband filtering, or imperfect power supply regulation. In addition, the tilt can be either static, affecting each line to the same degree, or picture-dependent, or both.

On normal PAL signals, the effect of line tilt is virtually imperceptible, merely making one side of the picture slightly darker than the other. However, the effect on signals scrambled by line rotation is much more serious, superimposing streaky (line-to-line) noise on the descrambled pictures. This is because the descrambling process breaks up the uniform tilt distortion, due to the change of cut-point position from one line to the next. The effect is shown in Fig. 6, which compares the appearance of the line tilt impairment on normal signals with that on scrambled signals.

In the scrambled signal, the portion of signal adjacent to the cut point position is repeated to give an overlap and appears at both ends of the active line. Thus, a measurement of tilt in the scrambled signal can be made by comparing the two ends of the scrambled active line. Integrating the difference for each line of the picture for several pictures, produces a correction signal that takes account of both static and picture-dependent tilt. Such tilt correction techniques can successfully eliminate the streaking impairment.

(a)

(b)

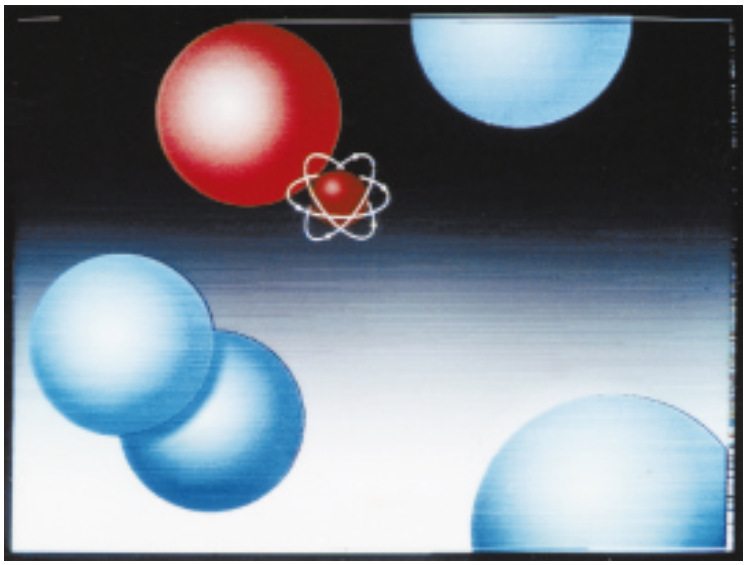


Fig. 6 - The effect of line tilt on (a) a normal (non-scrambled) signal and (b) the streaking effect produced after descrambling a line rotation scrambled signal.

3.3 The effect of multipath propagation

The effect of multipath propagation on a VSB-AM television signal is explained in Fig. 7 *(overleaf)*. In addition to the direct signal, Fig. 7(a), one or more reflected signals (echoes) can be received as well. As shown in Fig. 7(b), an echo is generally smaller in amplitude than the direct signal and can suffer a delay ranging from less than 1 μs to several tens of μs. Because the direct and delayed signals are combined as UHF modulated signals of the same frequency, the two components can have any value of relative carrier phase, depending on the delay. Thus, the signals can add in phase (as shown in Fig. 7(c)) or in anti-phase, so that the echo signal is inverted, or in quadrature.

With quadrature echoes, the effect is not as great. This is because the UHF demodulator rejects the quadrature component in the double-sideband, low-frequency video portion of the VSB-AM signal. However, high video frequencies, corresponding to the single-sideband portion of the spectrum, are not rejected. Thus, a quadrature echo appears as a series of edges in the picture, but has no DC component.

With normal signals, in addition to the delayed signal appearing on the picture, the presence of an echo can have an adverse effect on the receiver circuitry. As shown in Fig. 7, the latter part of the picture signal in the preceding line is added to the line interval of the main signal. This can cause ‘smearing’, due to the picture signal distorting the clamping period, so that the receiver clamp responds to alter the brightness level of the displayed line. A similar effect can be caused by the echo of the picture signal disturbing the measurement process of the automatic gain control (AGC) circuit, often made during the line pulse period. Both these effects depend on the time-constants used in the clamp and AGC circuits of the receiver. For quadrature echoes, the absence of a DC component significantly reduces the effect on the receiver circuitry.

With line rotation signals, multipath propagation can

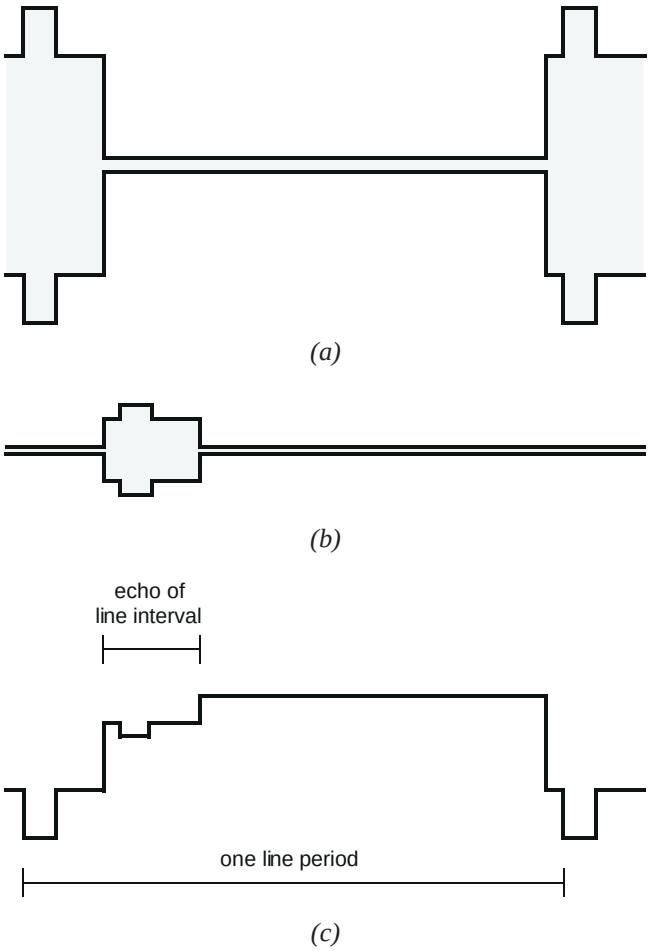


Fig. 7 - Multipath.

(a) the main signal arrives at the receiver at the same time as (b), a delayed echo signal of smaller amplitude. In this case, the two signals add in phase to produce (c), the received signal after demodulation.

adversely affect the quality of the decoded signals in several ways. First, because there is much more line-to-line and picture-to-picture variation in the scrambled signals, the effect on clamp and AGC circuits is less coherent and varies rapidly from line to line. Thus the effect is to introduce streaky noise rather than smearing, although, by using suitably long time-constants in the clamp and AGC circuits, the variations can be integrated out. Secondly, the presence of echoes can distort the periods used for tilt measurement at the two ends of the scrambled line, leading to inaccurate tilt correction which appears as streaky noise. This can be minimised by increasing the number of measurements used to calculate tilt. However, the third effect of echoes is less easy to deal with and arises in the following way.

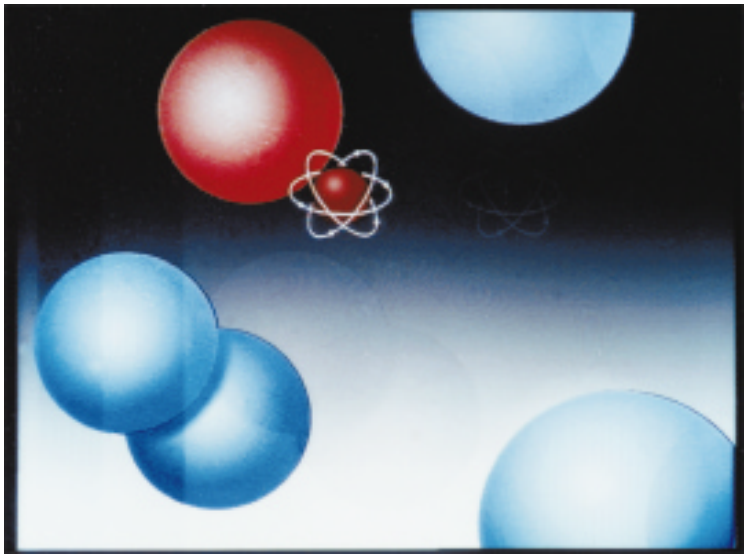
Depending on the echo delay, part or, as shown in Fig. 7(c), all of the line-blanking interval of the echo signal can fall within the active-line period of the main signal. With normal pictures, this appears as a slightly darker band (for an in-phase echo) down the left-hand side of the screen and is not particularly noticeable. The same band affects the scrambled line rotation signal; but when descrambled, the echo of the line blanking interval appears at a different place on each line, related to the position of the cut point used to scramble each line. Echoes of picture information, however, are not affected by the descrambling process, because each feature in the picture and its corresponding echo are both shifted by the same amount in the descrambling process. Fig. 8 compares the appearance of the line interval echo in a normal picture, Fig. 8(a), with that in a scrambled and descrambled picture, Fig. 8(b). The appearance of the line intervals in the descrambled picture has been referred to as the ‘hail of bullets’ effect and, because of its rapid movement, is much more noticeable than the effect of static or quasi-static echoes in the normal picture.

With scrambled signals, the sensitivity of line rotation to this form of distortion is such that a disturbing impairment can result, even when the echoes themselves are virtually imperceptible. A brief survey of domestic reception quality, carried out by BBC Design and Equipment Department, revealed that as many as 25% of people could be affected by sufficient multipath to cause impairment to line rotation scrambled pictures. While, in some cases, it might be possible to reduce the echoes by improving the antenna system, it is unlikely to be practicable to suppress the echoes to the very low levels needed.

In principle, an echo correction circuit could be added to the descrambler to compensate for echoes before the signals are descrambled. In one respect this is somewhat easier than might at first appear, because the timing of the cancellation signal does not have to be very accurate to cancel the low frequency content of the line blanking interval. On the other hand, the range of delays of echoes, and sometimes the number of echoes present at a particular reception site, can be quite large, resulting in a correction circuit of great complexity. Perhaps the most difficult feature, however, is the need to measure and compensate for time-varying echoes. In wet and windy weather, the low-level echoes, which are sufficient to impair line rotation scrambled signals, can vary over a period of a few seconds, as a result of movement of the antennas, trees, etc. This is particularly serious because a significant time is needed to measure the echo amplitudes to a sufficient degree of accuracy in the presence of noise. The implication is that, under these circumstances, the measurement process would never be sufficiently accurate to achieve adequate echo cancellation; and in some cases, would make the impairment worse by adding wrongly-phased correction signals.

With such a large proportion of viewers being affected,

(a)



(b)

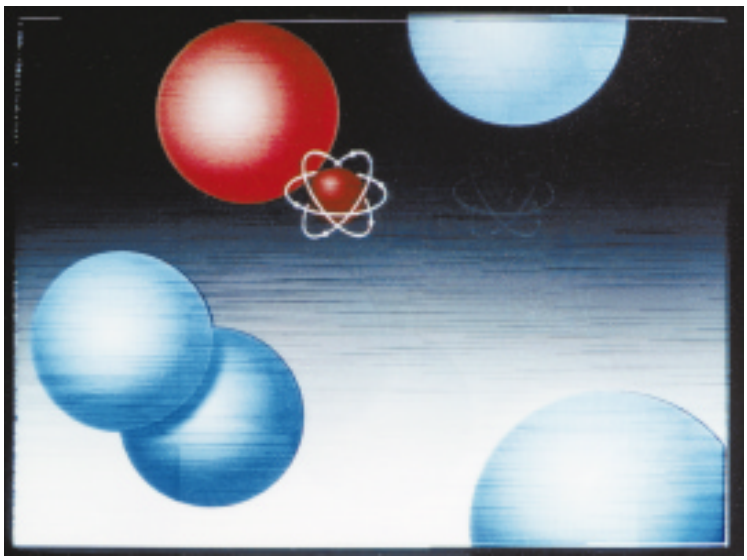


Fig. 8 - Line Shuffling.

The appearance of (a) a normal PAL signal and (b) a descrambled signal by the line rotation technique, each subject to an in-phase echo of 10% amplitude and 12 μs delay.

the problem of echo correction would have to be solved to allow line rotation scrambling to achieve good picture quality in widespread terrestrial use. While a solution cannot be ruled out, it is clear that, in this context, echo correction remains a very considerable problem.

3.4 The effect of co-channel interference

UHF network planning in the United Kingdom is dependent on the re-use of channel frequencies to achieve full coverage with four programmes. As an aid to this, some transmitters in different parts of the country, nominally on the same channel frequency, are adjusted to use an offset in their carrier frequency of approximately ± five-thirds line frequency (± 26.04 kHz) from the nominal value. This minimises the visibility of any co-channel interference (CCI) caused by receiving signals from both transmitters at the same time. With such offsets, interference normally appears as a fine pattern of horizontal lines, similar in appearance to a venetian blind. The pattern can be stationary or moving, depending on the exact value of the frequency offset. With such offsets, a protection ratio of 40 dB is required[18] for continuous inter-ference, and the transmitter networks are planned to meet this limit.

If the received signal is scrambled by the line rotation technique, the susceptibility to co-channel interference is increased. This is because the fine venetian blind pattern is broken up randomly by the descrambling process to produce more noticeable streaky noise. Brief tests have shown that the level of the interfering signal has to be reduced by about 5 dB (corresponding to a planning limit of 45 dB) to make the visibility of the streaky noise comparable to that of the venetian blind pattern of normal CCI. An estimate of the effect of this has been made by substituting the 45 dB figure in the network planning calculations and this suggests that of the order of 6% of the population would be nominally unserved. In practice, this would mean that, in 6% of cases, the reception of scrambled

signals would suffer a noticeable degree of impairment due to co-channel interference.

4. LINE SHUFFLING

The prospect of insuperable difficulties with line rotation scrambling, due to multipath in terrestrial applications, led to the search for an alternative. Until recently, line shuffling had been ruled out in all except professional point-to-point applications by the high cost of storage needed in the decoder. The continuing fall in the cost of digital storage has now removed this drawback, making the technique practicable in a much wider range of applications. Several equipment manufacturers have now produced line shuffling systems, but little has been written describing them and even less information is available on their suitability in terrestrial applications.

The principle of line shuffling was described in the early 1980s[19], although this may not be the earliest appearance of the technique. Line shuffling, or line permutation as it is sometimes known, scrambles the picture by changing the sequence in which the lines of the television signal are transmitted. The original order is then reinstated at the descrambler. Within this broad description, however, there are many alternative ways in which the process can be carried out.

4.1 Choice of basic parameters

Perhaps the most fundamental question concerns which lines should be shuffled. Retaining the normal sequence of lines through the field interval, by excluding the field blanking lines from the shuffling process, is advantageous for maintaining compatibility with network equipment, such as teletext data regenerators. In addition, if the half lines (lines 23 and 623) were shuffled, they would be easily identified in most pictures. However, if left in place, the half lines would provide a useful 'seed' to start unauthorised decoding by a correlation or line- matching system. Because of this, it is necessary to blank the half lines and any other lines of picture that are not subject to the shuffling process. Shuffling is therefore confined to the lines of the active field period.

The shuffling process moves lines by several line periods from their original positions. In practice, this is achieved at the scrambler by sampling the signal and storing the sample values until required. At the descrambler, the signal is again sampled and values stored. Thus the accuracy with which each line is restored to its original position depends on having stable and accurate sampling clock pulses at both the scrambler and descrambler. Any jitter on the sampling pulses between the store writing and reading processes will be transferred to the output signal. In PAL signals, this is particularly damaging as even small timing perturbations result in a significant change of subcarrier phase[20, 21]. Since the effect of any frequency error in the clock oscillator translates into a timing error between writing and reading, the problem becomes more serious as the duration for which a line is stored increases.

The stability of the sampling clock is influenced by the choice of video signal reference for the clock oscillator, either the colour subcarrier burst or the line pulse edge. It is generally easier to achieve accurate and stable sampling with the burst-locked approach, partly because the burst reference compensates for amplitude and level shifts, whereas the line syncs do not, and the burst inherently contains more timing information than the edge of the line pulse. On the other hand, using subcarrier-related clocks has the disadvantage that the number of samples per line is not an integer. Thus the shuffling process no longer moves lines by an exact number off-line periods. This problem can be minimised by sampling at four times subcarrier frequency and gives a picture-locked sampling grid.

A related question concerns whether just the active signal period of the line should be moved in the shuffling process, or whether the colour burst and line pulse should be moved as well. At first sight, it might appear that moving the burst and active-line signal together would ensure that the colour phase relationship was maintained. However, sampling clock jitter, introduced from one burst to the next, would still affect the signal, as the subcarrier reference phase would not follow the burst phase from individual lines. Moreover, moving the colour burst has two major drawbacks.

First, if the shuffling process were to include the burst, the normal burst sequence would be destroyed. This would make the synchronising waveforms non-standard and would prevent the colour burst being used as the sampling reference in the decoder. A special case which avoids this problem is to constrain the shuffling process to move lines only by a multiple of four, so that the colour phase and PAL switch sense are unchanged by shuffling. However constraining the shuffling process in this way leads to significant reduction in security.

Alternatively, if line-locked sampling were to be used, so that the colour burst was moved by exact number of line periods, the burst phase would carry information about the original position of the line. This is because the PAL subcarrier reference phase changes by a constant 270.576 degrees per line and the fractional part (0.576°) accumulates as a remainder. For example,

if a line had been shifted to be 12 lines late, then the remainder would be about 6.9 degrees less than expected. So comparison of the received bursts with an accurate subcarrier frequency oscillator would provide a strong indication of the correct positions of the scrambled lines with sufficient accuracy to prejudice security.

Summarising these considerations, therefore, it is preferable to shuffle only the active-line period of whole lines from the active-field period of the signal. The half lines and any active-field lines not included in the shuffling process should be blanked. A sampling frequency of four times subcarrier frequency, locked to the colour burst, is advantageous for providing a stable, nearly line-locked sampling grid.

4.2 Shuffling in blocks

In a line shuffling system, it is of considerable practical convenience to apply the scrambling process to blocks of lines, with the scrambled lines all remaining within the block. Shuffling algorithms which have no block structure can be envisaged, however, and are inherently more secure than block shuffled systems. In most circumstances, this minor advantage is outweighed by additional complication, particularly for initial synchronisation of the descrambling process. This is because, in a block-shuffled system, much of the synchronisation information can be derived directly from the video sync pulses, while without a block structure this information has to be provided separately.

A simple arrangement for shuffling in blocks is shown in Fig. 9. Both the coder and the decoder contain two stores, each with the capacity to accommodate all the lines of one block. During each block, one store is used for writing and the other is used for reading. The writing and reading stores then interchange for the next block. In the coder, consecutive lines are stored in order by using monotonically-increasing addresses. The reading process then uses a permuted sequence of line addresses to provide the scrambled signal. At the decoder, each scrambled line is immediately stored using the same permuted address as that used to read the line in the coder. The incoming lines are therefore placed at their original positions in the store. The descrambled output is then produced by reading the stored lines in order, using monotonically-increasing addresses. Additional storage is required, in either the coder or the decoder or both, to delay the line and field blanking intervals to compensate for the delay of the scrambling and descrambling processes. In broadcast applications, where the number of decoders greatly exceeds the number of coders, it is preferable to include the extra storage at the coder.

The arrangement of Fig. 9, which requires the coder and the decoder to produce the same sequence of permuted addresses at the same time, is, conceptually and significantly simpler than other methods. For example, writing with permuted addresses in the coder would require the same sequence to be reproduced for reading in the decoder two blocks later, because of the delay between writing in the coder and reading in the decoder. Alternatively, if monotonic addresses were used to store the scrambled signal in the decoder, then the inverse sequence of permuted addresses would be required for reading, one block later. There are, however, a number of methods that allow descrambling with a storage capacity of only one block. Each incoming line is therefore stored at the location vacated by the one being read out. One method[22] uses a look-up table to track the positions of the lines held in the store. Another method, known as double permutation, uses permuted addresses at the coder for both writing and reading, in order to compensate for the permuted writing and reading at the decoder.

4.3 Block size

The size of the shuffling block is an important parameter as this determines the minimum amount of storage required in both the coder and the decoder, and contributes to the overall delay that the signal undergoes in passing through the scrambling and descrambling processes. In broad terms, larger block sizes improve security by increasing the number of shuffling patterns. Also, larger blocks make the scrambled pictures more opaque because lines can be displaced further from their original positions. With very large blocks, the advance of the sound signal relative to the picture could give lip-sync problems. Other constraints on the block size are related to the distortions frequently introduced by terrestrial transmission and will be considered in Section 5.

The block size can be fixed or variable, and so can the positions of the blocks on the displayed picture. Using a variable block size tends to improve security by making the positions of the block boundaries irregularly spaced. This introduces an uncertainty as to whether a particular line belongs to one block or another. Making the block size a power of two provides for efficient use of storage devices, and tends to simplify the algorithms by which the scrambled line order is chosen.

4.4 Generation of permutations

For a block of N lines, the permuted addresses of Fig. 9 consist of a set of N numbers, conveniently 0 to N–1, each chosen once in an apparently random order. If $N = 2^n$, where n is an integer, then a sequence of N numbers can be generated by an n-stage binary counter.

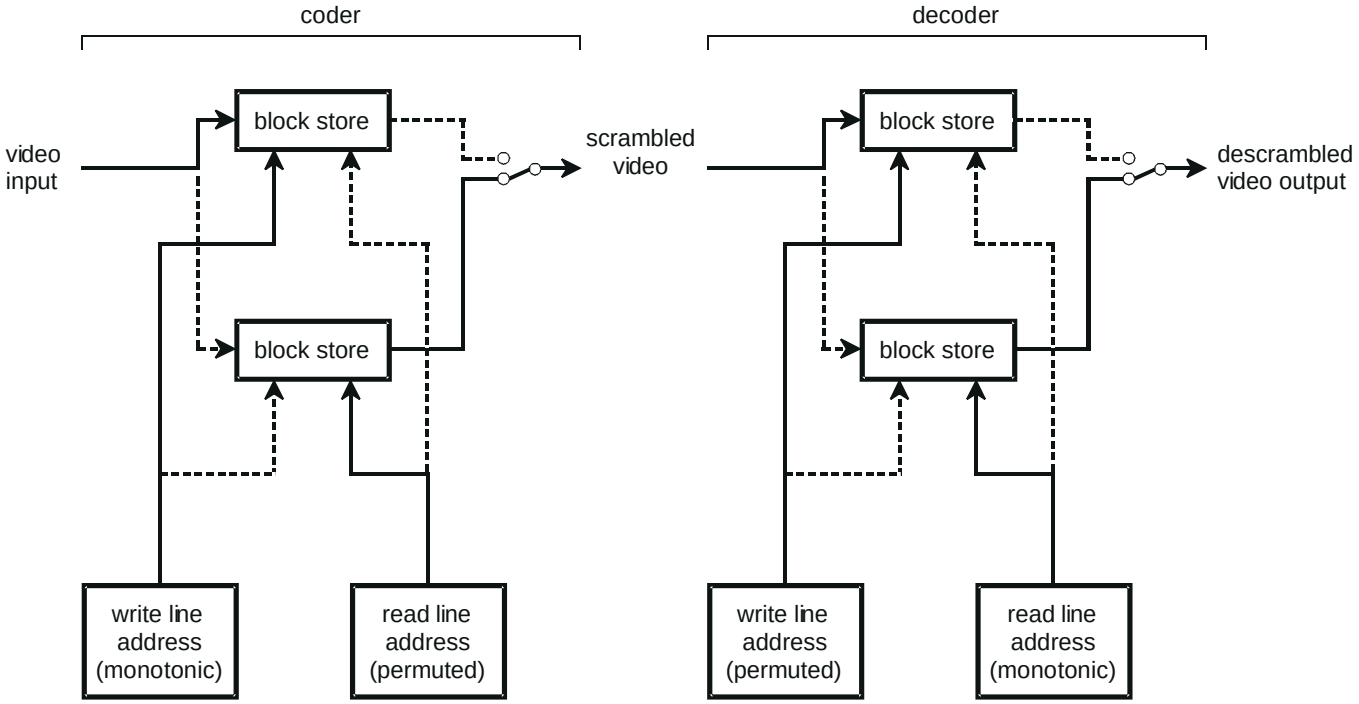


Fig. 9 - Line shuffling.

A simple storage arrangement for a line shuffling coder and decoder. Solid and dashed signal paths are used during alternate shuffling blocks.

The binary sequence can be modified by several logical operations which alter the order of the numbers without causing any to be lost or repeated[23]. For example, new sequences can be produced by inverting any of the counter outputs or interchanging any pair of outputs. Also, a new sequence can be produced by adding a number modulo-*N* to an existing sequence. Fig. 10 shows some logic elements which can be used to modify the sequence, or not, according to the state of one or more control inputs. Unfortunately, with the simple logical operations shown in Fig. 10(a) – (c), the individual bits still exhibit the frequency of the counter bit from which they are derived, that is, one bit will always change from line to line, one will change every two lines, and so on. What is needed is a means of logically combining pairs of bits in the number, while still ensuring that all the combinations are retained. This feature is provided by the exclusive-OR of pairs of bits as shown in Fig. 10(d).

Thus a permutation generator for line shuffling consists of the functional units shown in Fig. 11. A binary counter is reset at the beginning of the block and is advanced by line pulses to produce a new address for each line. Throughout each block, the bits of a sequence selection word are applied to the control inputs of the logic elements to modify the binary count to produce the permuted addresses. If the block contains N lines, where $N < 2^n$, then any permuted addresses outside the range 0 to N-1 can be avoided by advancing the counter until a valid address is produced. In the decoder, the sequence selection word is derived from securely encrypted data sent with the scrambled signal. Good security and opacity are obtained by using a new sequence selection word, and therefore a different shuffling pattern, for each block.

5. INVESTIGATION OF LINE SHUFFLING PARAMETERS

The previous section has described some of the considerations involved in choosing the parameters of a line shuffling system. However, more practical experience was needed of the detailed effects of distortions in VSB-AM terrestrial broadcasting in order to develop a system with the optimum performance. This section describes the results obtained from line shuffling tests made over a period from May 1990 to April 1992. It also gives details of the changes made to the basic technique in response to the difficulties encountered.

5.1 Simulations

Initial assessments of line shuffling were made using computer simulations to assess the appearance of the scrambled signals. Scrambling was first performed by forming a stored test picture into a PAL-encoded four-picture sequence. The active-line information of the picture was then shuffled by displacing lines in a pattern that repeated every eight pictures (about a third of a second). This sequence was sufficiently long to make the changes in the scrambling pattern appear

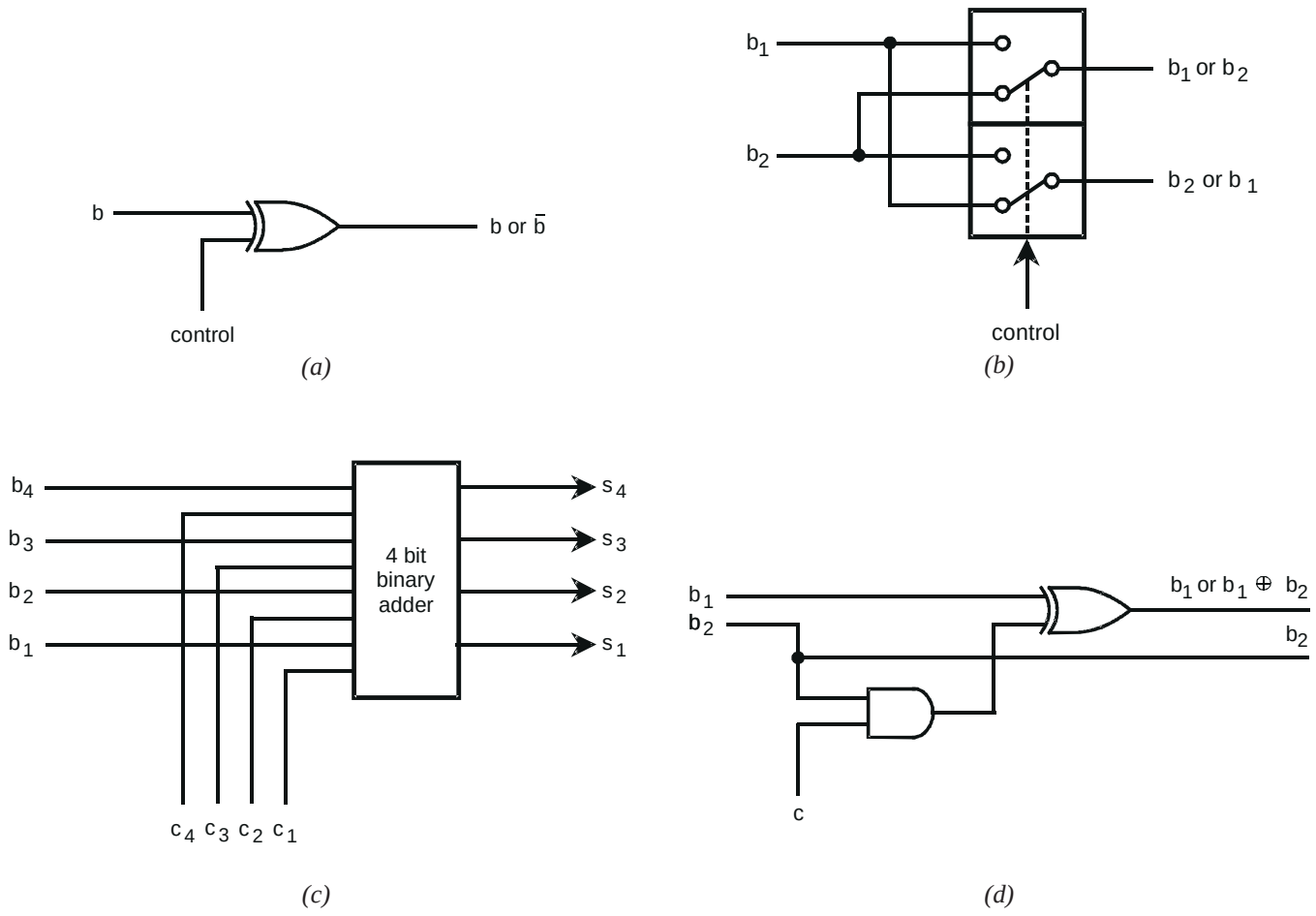


Fig. 10 - Controlled logic elements for modifying the outputs of a binary counter to produce alternative sequences.

(a) bit inversion, (b) bit swapping, (c) introducing an offset (the carry is ignored), and (d) combining bits together.

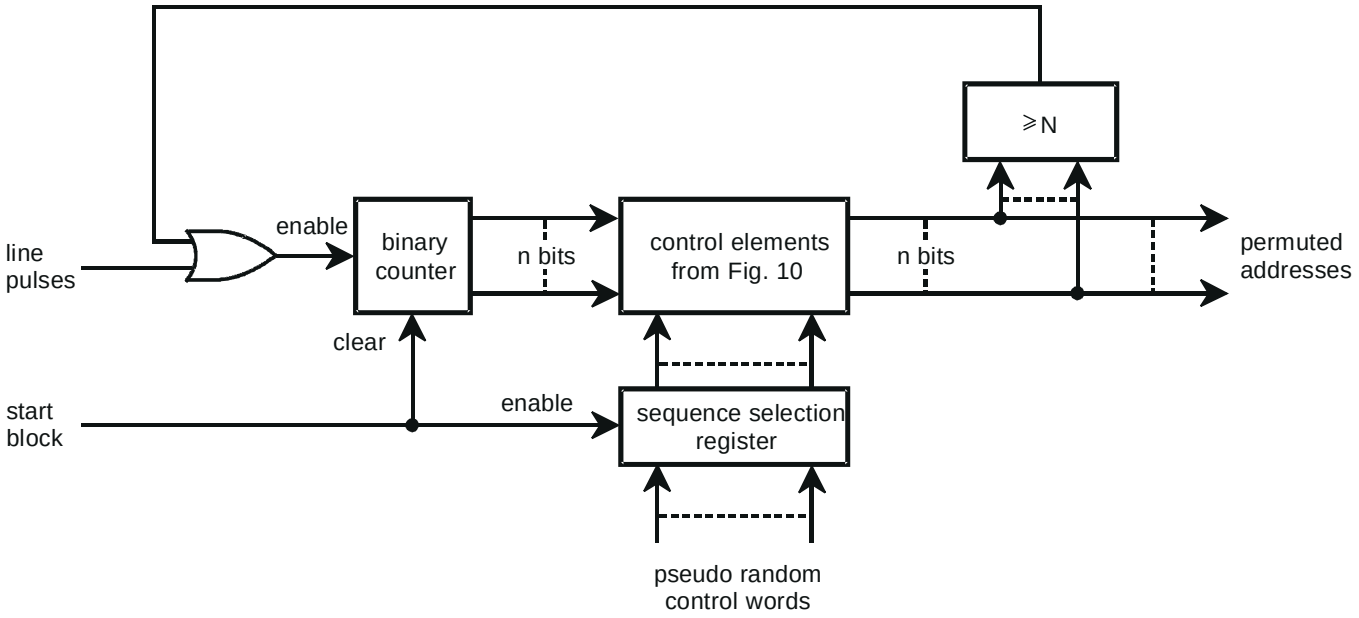


Fig. 11 - A permutation generator for line shuffling.

reasonably random.

Simulations made in May 1990 were performed to view the effects of shuffling the encoded PAL signals and to compare 32- and 64-line blocks. Two versions of the 32-line system were demonstrated: one with the block boundaries coincident on the two fields, and the other with interleaved blocks. The 64-line system had four blocks on the first field, then one block straddling the field interval, and four blocks to complete the second field. The block positions were fixed relative to the picture in all three systems. The appearance of the scrambled pictures for these three systems are shown in Fig. 12. These single-frame exposures are, of course, unable to convey the full effect of the changing scrambling patterns.

Further simulation results were obtained in October 1990 to compare the opacity of differing block sizes, particularly with respect to the readability of on-screen text. Blocks of 31, 63 and 127 lines were compared; first with the block structure reset at the beginning of each field to give fixed blocks, and then reset only at the beginning of the 8-picture sequence to produce blocks running through the picture. Odd numbers of lines per block were used to ensure that the blocks would run through the picture. Although the pictures with the smaller blocks were reasonably well scrambled, the larger blocks were significantly more opaque. The 63-line arrangement was felt to give a worthwhile improvement in opacity over the 31-line blocks. For each block size, visual averaging of the moving blocks made the pictures slightly less opaque than with fixed blocks of the same size. The appearance of the scrambled pictures for the three fixed-block systems and the three moving-block systems are shown in Figs. 13 and 14 *(pages 18 and 19)*, respectively.

5.2 Initial over-air tests

Following the simulations, it was necessary to investigate the effects of normal UHF network and propagation distortions on line-shuffled signals. To make this possible, prototype encoding and decoding equipment was developed at Research Department to scramble the picture in fixed blocks of 32, 64 and 128 lines. The scrambled signals produced were similar in appearance to those of Fig. 13. This equipment was then used for over-air tests carried out during December 1990 and January 1991 from the Crystal Palace transmitter. These tests produced several useful results.

5.2.1 Timing stability

It was found that the four-times subcarrier burst-locked sampling clock allowed the signals to be stored and retrieved without significant introduction of timing jitter, even when the interval between storing and retrieving the signals was one picture period.

5.2.2 Average Picture Level variations

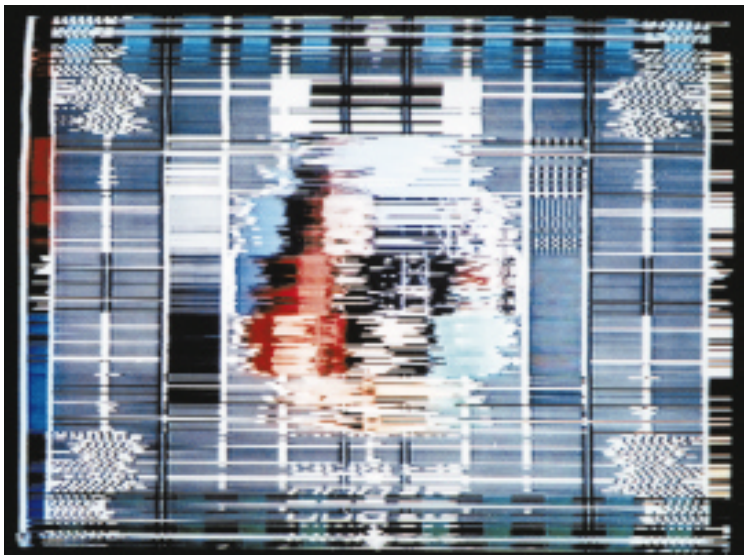
The results in the first tests were sometimes affected by Average Picture Level (APL) variations. This was caused by a.c. coupling between the demodulator and the descrambler producing a low-frequency tilt across the shuffling blocks. When the lines were moved by the descrambling process, the tilt was broken up to appear as streaky, line-to-line noise on the picture. This was avoided if the receiver was connected to the descrambler using direct coupling or, alternatively, a.c. coupling with a time-constant significantly longer than the scrambling block, followed by a clamp. Streaking caused by APL variations when the a.c. coupling time-constant is too short in relation to the clamp time-constant is shown in Fig. 15.

5.2.3 Multipath distortion

When tested with multipath distortion, it was found that this affected the line-shuffled signal by three separate mechanisms, all resulting when the echo of the previous line overlapped different parts of the direct signal. The same mechanisms are present when normal transmissions are affected by multipath, but the effect is typically greater in line-shuffled signals. This is because, in the shuffled signal, the over-lapping echo signal generally changes rapidly from line to line, having been broken up by the scrambling process. The process of overlap is illustrated in Fig. 7.

Television receiver circuits derive a signal for Automatic Gain Control (AGC) by measuring the signal amplitude during the line-blanking interval. Domestic receivers tend to use the bottom of syncs as the reference level (the peak amplitude in a negatively-modulated signal), while professional receivers have the alternative of using a back-porch reference. If the echo of the previous line overlaps the reference level of the AGC circuits, then this causes an AGC error. In a normal signal, the error is generally steady, causing a smearing effect on the displayed picture, whereas with the rapid variations of the scrambled signal, the error shows up as streaky noise. This is shown in Fig. 16. With shuffled signals, the effect can be minimised by using a slower than normal AGC time-constant, so that the control loop settles to the average level of a large number of lines, rather than responding to the variation of individual lines. This requires an AGC time- constant that is long compared with the length of the shuffling block. Fig. 16 compares the effect of an echo on line-shuffled signals received using short and long AGC time-constants.

A second effect of multipath distortion occurs when the echo overlaps the clamping level of the a-d

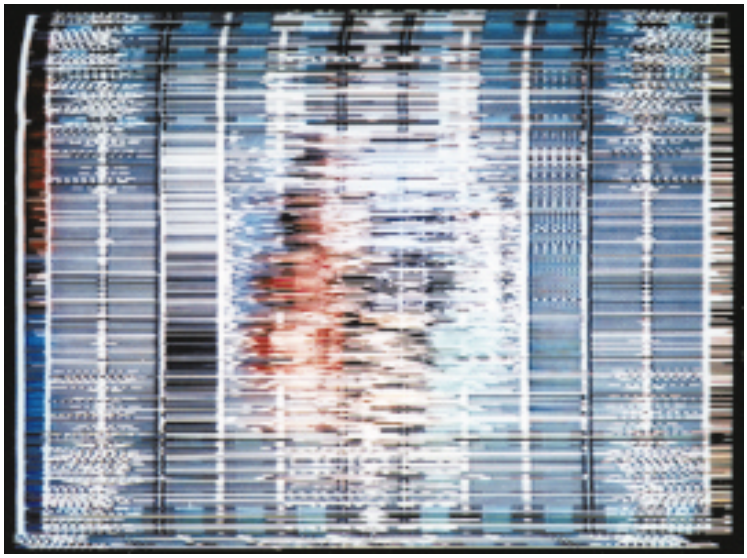


(a)

(b)

Fig. 12 - Line Shuffling.

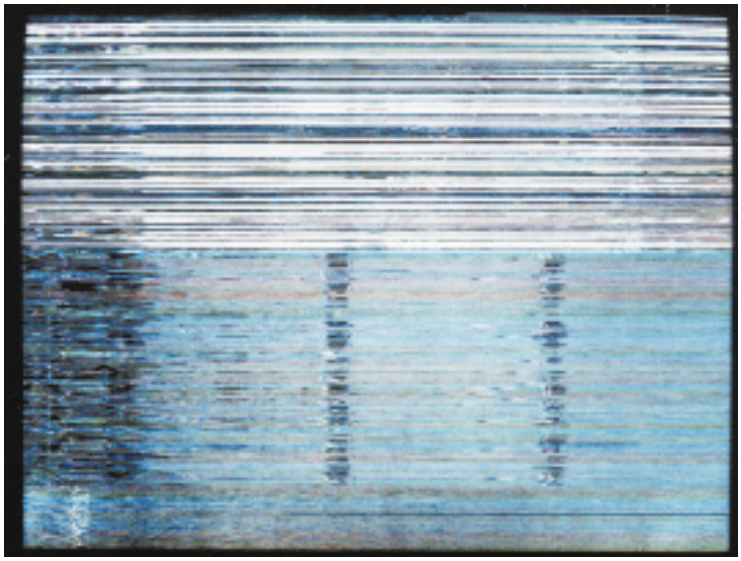
32-line blocks (a) coincident and (b) interleaved on odd and even fields, and (c) 64 line blocks with 9 blocks on each picture.



(c)

(a)

(b)

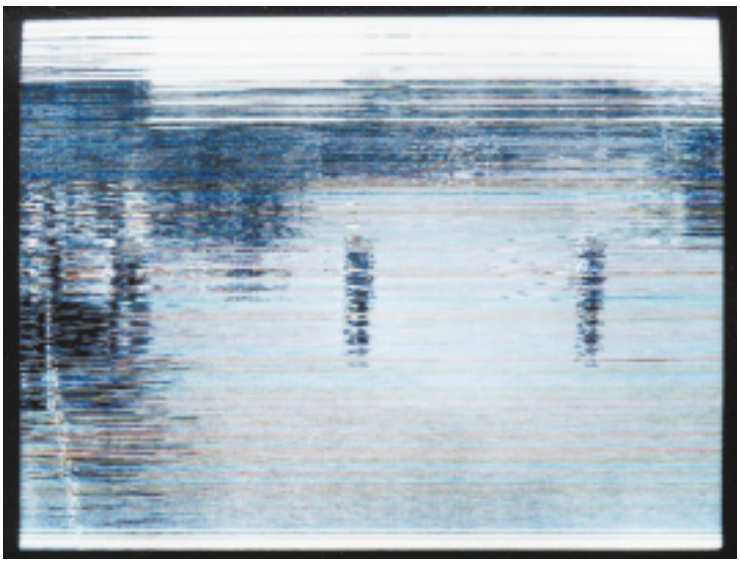


(c)

Fig. 13- Line Shuffling.

Fixed blocks of (a) 31 lines, (b) 62 lines, and (c) 127 lines, reset at each field interval.

(a)



(b)

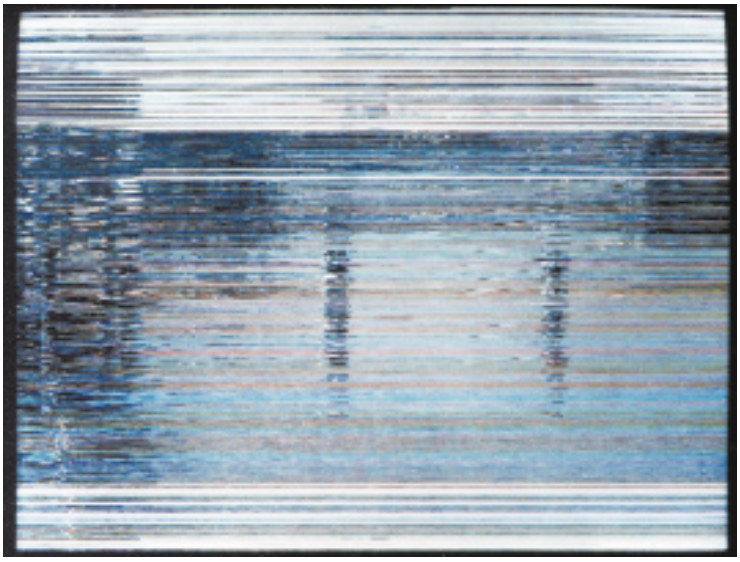
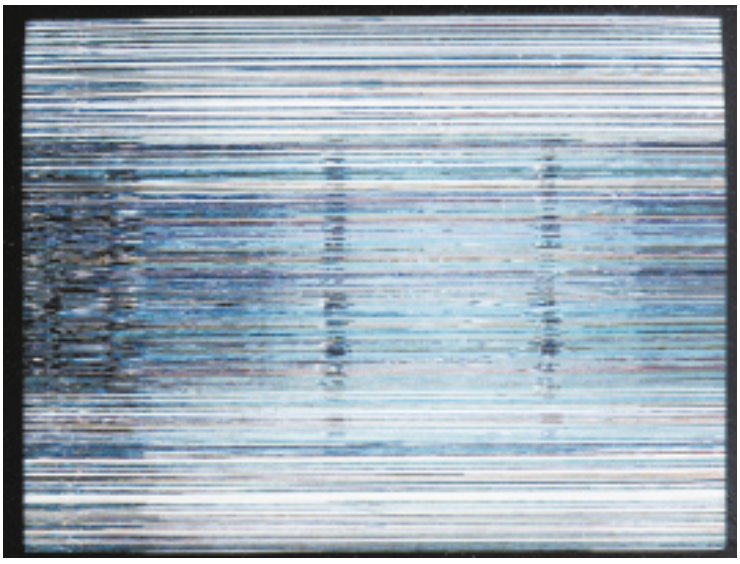
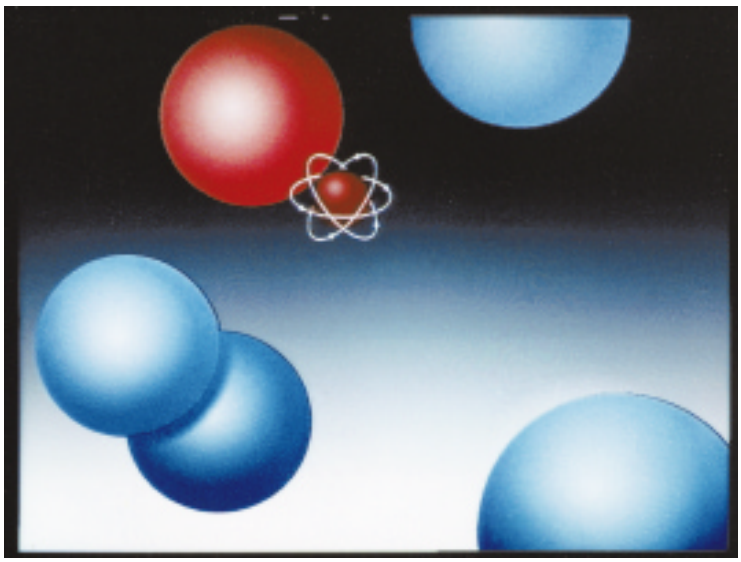


Fig. 14 - Line Shuffling.

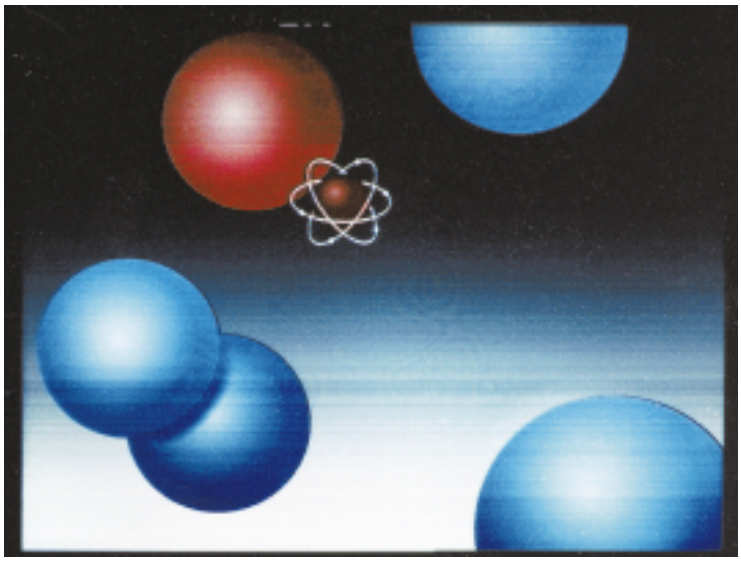
Moving blocks of (a) 31 lines, (b) 63 lines and (c) 127 lines, without resetting at the field intervals.

(c)





(a)



(b)

Fig. 15 - Line Shuffling.

The effect of average picture level variations when a.c. coupling with a short time-constant is used (a) for normal (non-scrambled) signals and (b) for scrambled signals.

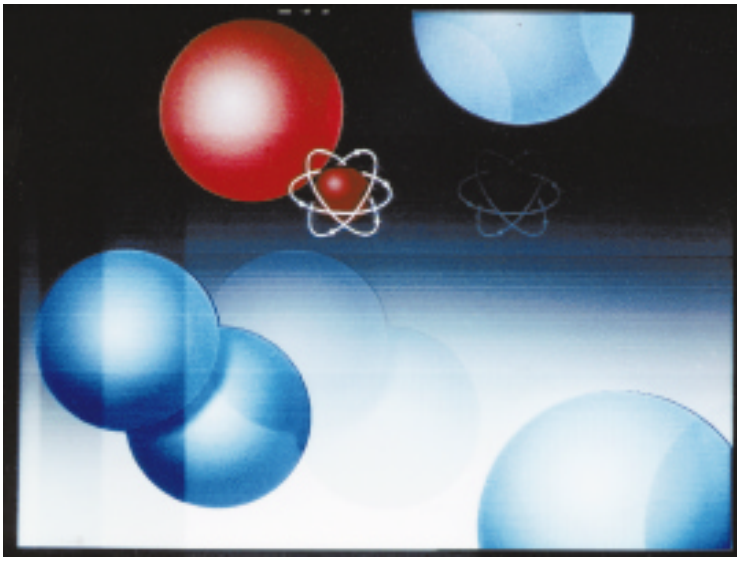
converter in the descrambler. A fast clamp would respond to the variations of the echo signal, thus altering the brightness of the following active line. As with the AGC loop, this can be avoided by using a slow clamp, with a time-constant that is significantly longer than the shuffling block.

While using a slow clamp avoids the introduction of clamp errors, the clamp reference period (the back porch) is still impaired by the echo signal. The potential, therefore, remains for any fast clamp in subsequent circuitry, such as in a picture monitor, to reintroduce the distortion. However, this can be avoided by arranging that the descrambler reinserts a stable black level during the clamp reference period. A block diagram of a black-level reinsertion circuit is shown in Fig. 17.

The third effect of multipath distortion occurs when the echo of the scrambled signal overlaps into the active period of the next line. Echoes on the same line are descrambled in the same way as the direct signal, so appearing as normal echoes in the descrambled picture. However, echoes from the previous line are not descrambled correctly, so these appear as streaking at the left hand side of the picture, the width of the affected region being determined by the amount by which the echo delay exceeds the duration of the line blanking interval. A simulated long delay echo demonstrating this effect is shown in Fig. 18. If present, such long delay echoes are generally of small amplitude, so although nothing (apart from echo correction before the descrambler) can be done to reduce the effect, the degree of additional impairment is rarely significant.

When the system was retested in January 1991, using time-constants optimised for minimising the effects of multipath, the results for normal and line-shuffled signals were found to be substantially identical. In each case, the normal appearance of the echo signals was the main impairment to the picture, even with

(a)



(b)

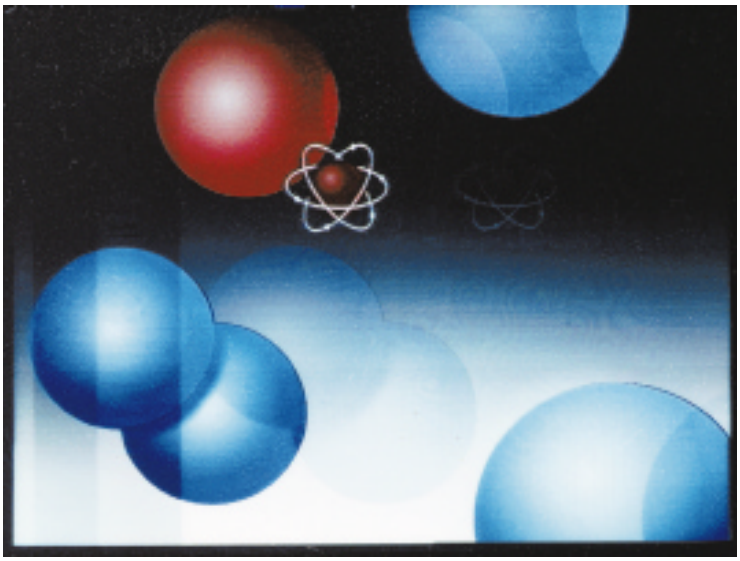


Fig. 16 - Line Shuffling.

The effect of a 12 μs echo of 20% amplitude on a shuffled 64-line block signal with receiver AGC time-constants of (a) 450 μs (fast) and (b) 10 ms (slow)

relatively long delay echoes of up to 10% amplitude.

5.2.4 Hum modulation

In the first over-air tests with the experimental line shuffling equipment, hum was not a problem. However, when a longer AGC time-constant was used to improve multipath suppression, the presence of low-level hum modulation of the signal envelope became apparent on some transmitters.

In the scrambled signal, hum causes a variation in level across each block. The descrambling process breaks up this gradual variation to produce streaky noise. For a given level of hum, streaking is particularly noticeable if the hum waveform is non-sinusoidal, with a high slope at some parts of the waveform, as can occur from poor power supply smoothing. In addition, for some block sizes, the hum alters the average level of one block compared with the next. This results in the block boundaries becoming noticeable in the descrambled picture. The effects of hum are shown in Fig. 19.

Except under fault conditions, the amounts of hum modulation present on the signal envelope are usually small, although even 2 mV on the demodulated video signal can cause noticeable streaking if the receiver has slow AGC. However, the AGC loop increasingly suppresses hum modulation as the speed of the AGC

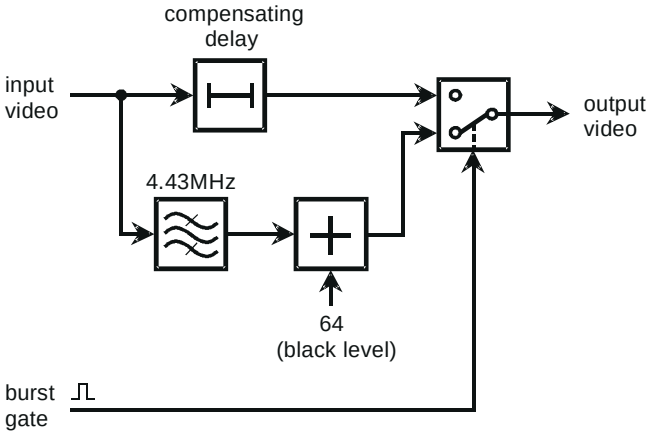


Fig. 17 - Block diagram for black level reinsertion.

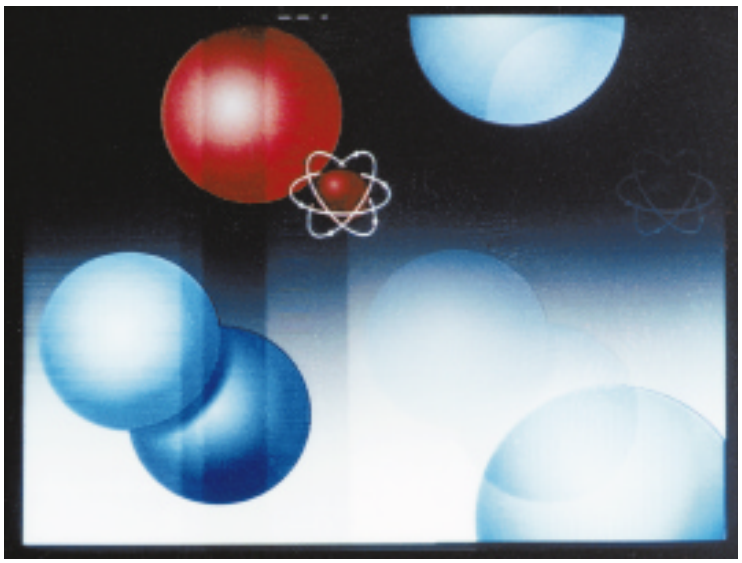
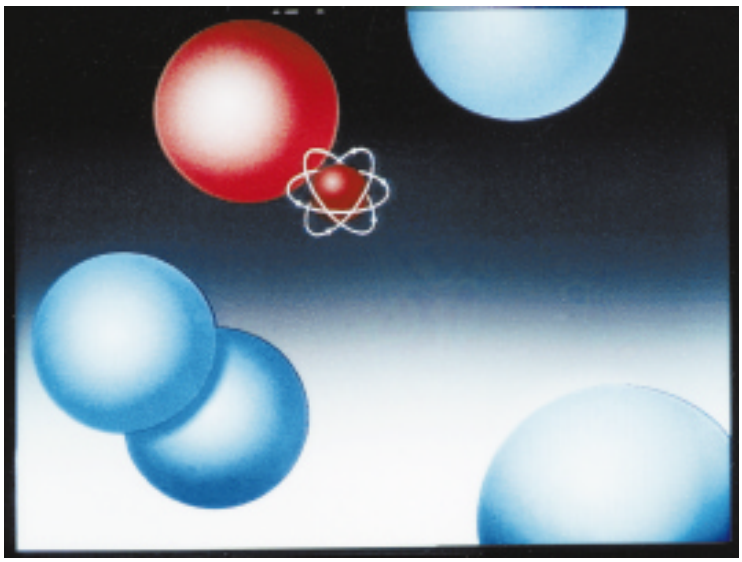
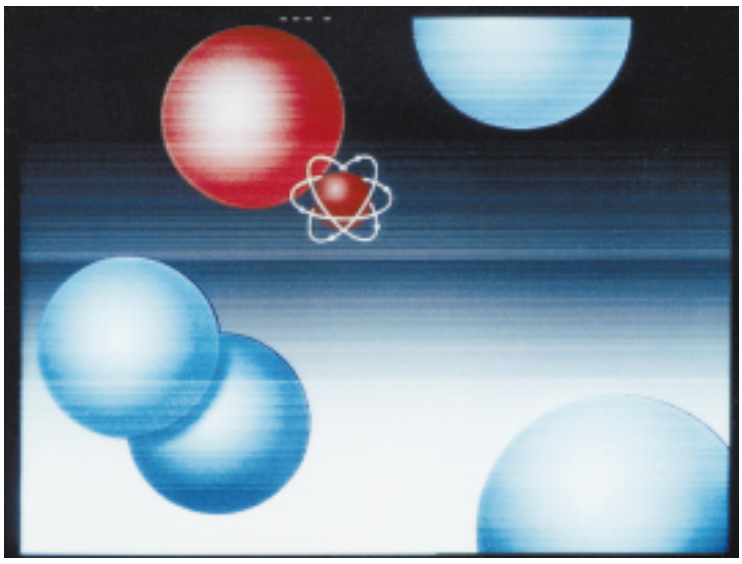


Fig. 18 - Line Shuffling.

The effect of a 24 μs, 15% echo producing streaking at the left-hand edge of the descrambled picture, (receiver AGC time-constant 10 ms).



(a)



(b)

Fig. 19 - Line Shuffling.

The effect of 100 mV sinusoidal hum modulation (100 Hz) with a slow receiver AGC time-constant of 10 ms and a soft clamp. Pictures produced by (a) a normal PAL signal and (b) a 64-line block scrambled signal. While in (a) the normal hum bars are barely visible, (b) shows streaky noise and the block boundaries.

increases. With fast AGC, very high levels of hum modulation can be suppressed, so that no impairment results in the descrambled picture.

5.2.5 Co-channel interference

During reception tests using a misaligned antenna, some streaking was noticed which could not be explained in terms of multipath propagation or hum modulation. This was explained as being the result of co-channel interference.

Co-channel interference affects line-shuffled signals to an extent similar to that occurring with line-rotation scrambling, as described in Section 3.4. The descrambling process breaks up the Venetian blind pattern to produce streaking, which is visually more disturbing. Again, at or near the –40 dB planning limit, the interference has to be reduced by about 5 dB to maintain the same level of disturbance as in a non-scrambled signal.

5.2.6 Comparison with line rotation

Following the initial tests, it was found that most of the impairments of line shuffling were significantly reduced by using 64-line rather than 128-line blocks. Also, 64-line blocks were preferred over 32-line blocks for being more opaque. So a system using 64-line, fixed blocks with increased AGC and clamp time-constants was used in a further test in January 1991. When compared with line rotation scrambling under the same conditions, this test confirmed the superiority of line shuffling in circumstances where multipath was encountered. The tests did show the susceptibility of the shuffling system to hum modulation, but this was judged to be much less serious than the problem of multipath in line rotation scrambling.

5.3 Optimisation of the block arrangement

While the 64-line fixed block system represents a broad optimum, this prototype arrangement was not the most convenient for decoders for volume production, because of the need to take account of several additional constraints.

First, there was the requirement, mentioned in Section 4.2, to advance the active lines of the scrambled picture by one block relative to the synchronising waveforms. This would then compensate for the inherent one-block signal delay in the descrambling process and so remove the need for the decoder to include a delay for the synchronising waveforms.

A second requirement for the production decoders was the provision of capacity for the transmission of conditional access (CA) data. CA data is transmitted at a relatively low instantaneous bit rate, because of the need to ensure highly reliable reception. In order to avoid incompatibilities with the teletext system, it is necessary to use lines from the active picture period, with four lines per field providing an adequate capacity. Thus, with the half-lines excluded, only 283 lines per field were available for shuffling. So for fixed blocks of 64 lines, a short block of 27 lines was needed to complete each field.

Consideration was then given to the alternative of using equal-sized blocks and not resetting the structure at the field interval. Necessarily, this causes the block structure to run through the picture, which has several unwanted effects. These drawbacks were demonstrated by brief tests carried out with a 62-line, moving block system in April 1991.

Any moving block system suffers additional complication because there is no explicit relationship between the picture and the block structure, which complicates the initial synchronisation process. Blocks of 62 lines were chosen so that the block structure could be reset at the beginning of each conditional access key period (16 pictures). Even then there was a remainder of four non-scrambled lines in the final field. Also, moving blocks have the disadvantage that some blocks straddle the field interval, comprising a mixture of lines from the two fields. This has the effect of accentuating any field-rate distortion in the signal because lines from either side of the field interval, where the distortion tends to be at its maximum, can be placed adjacent to one another in the descrambled picture. Also, as the blocks run through the picture, the range of displacement of any line from its original position is up to twice the block size. The susceptibility to distortion is therefore more like that of a fixed block system of twice the size. A further factor is that, when the blocks are moving, impairments can introduce a disturbing brightness flicker, produced by the impairment varying according to the position of the block.

Another proposal was to use fixed blocks that were more nearly equal in size by using five blocks, one with 59 lines and the remaining four with 56 lines. This overcame the difficulties of the 62-line system, but additional control circuitry would have been required in the decoder to provide for the two block sizes. A simpler, fixed block alternative was to use six blocks, each of 47 lines, with the remaining line per field blanked as with the half lines. Reducing the block to this size has lost a little in opacity and security compared with the 64-line system, but the smaller block has the advantage of reduced susceptibility to distortion. Further development was therefore based on the 47-line system, details of which are contained in the Appendix.

Fig. 20 - Line shuffling.

The picture produced by a signal scrambled in six blocks of 47 lines each. The scrambled lines are advanced by one block relative to the field interval, so the bottom of the scrambled picture contains information from the top sixth of the original picture.

5.4 Network tests

The brief tests in April 1991, carried out at the Midhurst transmitter, had confirmed the suspicion that network links and older transmitter equipment might introduce additional impairments to the ones already seen with test transmissions from Crystal Palace. It was clearly necessary to investigate this aspect more closely, particularly as the characteristics of the 47-line system might be different from those of the 64-line blocks, which had been used for most of the previous tests. In view of this, a new design of 47- line encoder and six decoders with built-in receivers were constructed. The appearance of the 47-line block scrambled picture is shown in Fig. 20.

One feature of the new receiver/decoders that differed from earlier versions was the use of faster AGC. The choice of AGC time-constant was already understood to be a compromise between multipath performance and the suppression of hum modulation; but on further consideration, hum suppression was felt to be more important. This was because: if a transmitter introduced hum, all the received signals would be affected, whereas only individual reception sites would be affected by multipath. Also, even with a fast enough time-constant to suppress hum, the multipath performance, although not optimum, was still reasonably good.

With the six receiver/decoders and a series of tests over several weeks in November and December 1991, it was possible to examine the quality of the descrambled signals from BBC1 and BBC2 at approximately half the main sites in the transmitter network. The sites were carefully chosen to be representative, in terms of the signal path to the transmitter and the transmitter type, configuration and age. This produced a mass of results which showed that, although some transmitters gave descrambled pictures of virtually unimpaired quality, a minority did suffer from noticeable impairments.

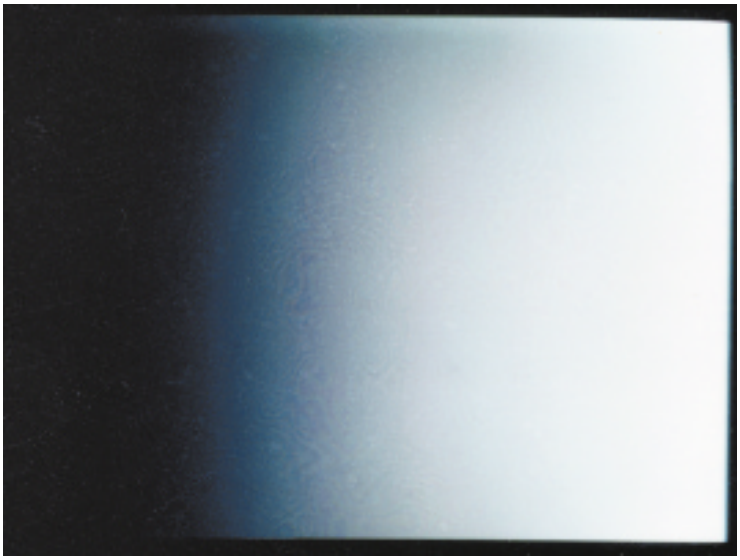
The picture impairments encountered in these tests were principally of two forms, referred to as ‘field hook’ and ‘hum’, which sometimes occurred independently and sometimes together. Although both impairments produce streaky noise in the picture, the appearance of each is somewhat different.

Field hook is a distortion of level which affects the first few lines transmitted after the field interval. After decoding, these lines can occupy any position in the second block of the descrambled picture, due to the one-block delay in the descrambler, so the streaking is concentrated in this region of the picture. This is shown in Fig. 21. The visibility of streaking due to field hook depends to an extent on the number of lines affected, but the impairment starts to become noticeable with a shift in level of about 5 mV.

It should be emphasised that the hum impairment observed here does not occur by the same mechanism as the hum modulation previously encountered and described in Section 5.2.4. Hum modulation is a modulation of the transmitted signal envelope and in these tests would have been suppressed completely by the fast AGC of the receiver/decoder. In this context, hum is a distortion affecting the active-line periods of the signal. All the shuffling blocks in turn are affected by streaking, as the distortion, related to the mains frequency, drifts through the field. The appearance is similar to that of hum modulation, shown in Fig. 19, and starts to become noticeable when the amplitude exceeds a few millivolts peak-to-peak, although the visibility is affected by the shape of the hum waveform. The effect is more disturbing when field hook and hum are both present.

These two distortions share the common feature that

(a)



(b)

(c)

Fig. 21 - Line Shuffling.

The effect of 20 mV of field hook. Pictures produced by (a) a normal signal, (b) a signal shuffled in 47-line blocks and (c) a signal delayed by the decoder, but not descrambled (the clear/delayed mode).

the active-line periods and line intervals of the signal are not distorted in the same way. Indeed, this is the essence of the problem because it prevents the AGC and clamp circuits of the receiver/decoder from removing the distortions. This implies that the distortions are linked to the reinsertion of sync and blanking waveforms, which occurs in sound-in-syncs decoders at various points in the network and in high-efficiency pulsed klystron transmitters. Hum and low-frequency distortions which might cause hook are certainly present on the lines feeding transmitters. It may be speculated, therefore, that the distortions occur either because these impairments are not fully removed by clamping before blanking is reinserted, or because the reinserted waveforms themselves suffer from low-level distortions. This view was supported by the brief investigations held at BBC Manchester and at the Winter Hill transmitter during April 1992.

6. CHOICE OF SOUND SCRAMBLING TECHNIQUE

Although the provision of sound scrambling was not seen as essential for the BBC Select service, a secure, high-quality sound scrambling method was desirable, increasing the range of potential applications. The original VideoCrypt line-rotation system, as used on the Astra satellite, provides no sound scrambling method, broadcasting the sound directly as clear signals. BBC Research Department was also, therefore, asked to advise on the possibilities for sound scrambling.

6.1 Sound scrambling techniques

With the early sync-suppression vision-scrambling techniques used for satellite broadcasting, separate sound scrambling was unnecessary. This is because many television receivers mute the sound when line or field syncs are lost. Thus, sync suppression automatically silenced the sound as well. However, such techniques cannot be used for terrestrial broadcasting, for the reasons given in Section 2.3.

For terrestrial broadcasting applications, the techniques used for scrambling television sound signals can be divided into three main categories: time-domain methods, frequency-domain methods and digital encoding. These are outlined in the following sections.

6.1.1 Time-domain methods

Just as the order of parts of the video waveform is altered by line rotation or line shuffling, the same principle can be applied to scrambling a sound signal. The process is more complicated, however, because the sound signal contains no equivalent to the sync pulses and blanking intervals in a video signal. Dividing the sound signal into segments and shuffling the segments requires a time reference to be added to the signal to allow the segments to be identified and re-ordered at the descrambler.

A further difficulty is that such scrambling methods are prone to introducing distortion at the segment frequency. This problem is reduced by making the duration of the segments about 30 ms, so that the block fundamental frequency falls at 33 Hz, below the normal audio range. However, as several segments need to be stored, both in the scrambling coder and in the decoder, the processing delay can easily reach 250 ms, thus requiring a video compensating delay of about 12 field periods.

In addition to these problems, the technique is costly, because of the large storage requirements, not particularly secure or transparent, and the scrambled signals are not always unintelligible.

6.1.2 Frequency-domain methods

Sound scrambling in the frequency domain consists of shifting the spectral components to new positions in the audio range by modulating the signal on to one or more in-band carriers. Variations of the basic method consist of altering the carrier frequency to change the shift, or dividing the signal into sub-bands which can then be shifted individually to different positions in the spectrum.

A simple version of the frequency-domain method known as spectral inversion has been used in several broadcast television applications, including the Canal Plus terrestrial transmissions based on Discret-1[10], and in the trial BMTV downloading service[7]. The principle of this method is shown in Fig. 22, in which the baseband sound spectrum Fig. 22(a) is modulated by suppressed-carrier amplitude modulation on to a carrier, Fig. 22(b), near the top of the audio band, to produce the modulated spectrum shown at Fig. 22(c). The signals are descrambled by accurately regenerating the carrier frequency at the decoder and demodulating to shift the spectrum back to its normal position.

Clearly, the carrier frequency has to be chosen for compatibility with the upper limit of the audio band; in particular, the 14.8 kHz bandwidth of the sound-in-syncs distribution system. The Discret-1 spectral inversion used a 12.8 kHz carrier, allowing the decoder to regenerate the carrier from the video signal (256 times the 50 Hz field frequency). This means that, in order to avoid aliasing during the modulation process, and allowing for practical filter characteristics, the audio input signal has to be band-limited to about 10 kHz, the part removed being shown dashed in

Fig. 22(a). Also, after modulation, a high-quality filtering technique has to be used at the coder to suppress the upper sideband of the modulated signal, shown dashed in Fig. 22(c). Inadequate filtering at this point can result in the bass response of the descrambled audio being severely impaired.

Most broadcast television standards use frequency modulation to carry the sound signals. Pre-emphasis is used to boost the amplitude of the high frequencies to counteract the triangular noise spectrum of frequency modulation. Corresponding de-emphasis is used at the demodulator. In normal sound signals, the high frequencies occur at much lower amplitudes than those of the low frequencies, so pre-emphasis is unlikely to cause overloading. However, when the sound signals are scrambled by spectral inversion, the high-amplitude low-frequency components occur at the high-frequency end of the spectrum. These unusually high-amplitude components are further boosted by pre-emphasis, so overloading is very likely to occur. To avoid this, the scrambled signal is produced at an amplitude some 12 dB lower than a normal signal. Although this significantly degrades the signal-to-noise ratio of the scrambled sound, the normal margin of FM sound is such that adequate quality is still maintained.

While the spectral inversion technique is insecure and provides quality somewhat inferior to normal television sound, its great advantage is the simplicity of the descrambling process. In addition, the scrambled sound signal is rendered reasonably unintelligible.

6.1.3 Digital coding methods

If the sound signals are digitally encoded, this allows digital scrambling by the modulo-2 addition of a pseudo-random sequence to the sound data, with similar advantages to those already described in Section 2.4 for scrambling digitally-encoded picture signals. However, the existence of the NICAM-728 digital sound coding system makes digital scrambling a much more immediate possibility for the sound. Nevertheless, standardisation of NICAM-728 has yet to be extended to cover digital scrambling, although the subject has been discussed internationally for several years. Also, NICAM coverage through the BBC transmitter networks, although already serving more than 87% of the population, is unlikely to be complete for several years. Therefore, although NICAM offers high-quality, secure and unintelligible scrambling, it is not as yet a complete solution.

6.2 Sound scrambling for the BBC Select service

When the question of sound scrambling for the BBC Select service was under consideration, experimental NICAM digital sound transmissions were already being broadcast on a regular basis from some transmitters. Clearly, the use of digital scrambling had attractions for the Select service, but this could not be countenanced on its own because of the several years envisaged for achieving complete NICAM coverage. Because of this, the possibility of using NICAM in conjunction with an analogue scrambling system, to give temporary coverage in areas not served by NICAM transmitters, was given serious consideration.

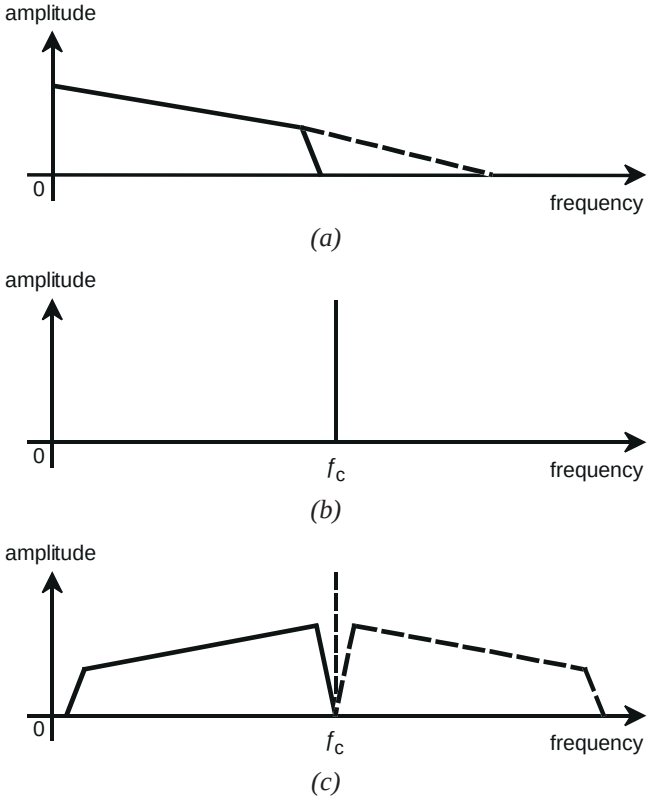


Fig. 22 - Sound scrambling by spectral inversion.

(a) the band-limited audio spectrum, (b) the carrier frequency, and (c) the spectrum produced by convolving (a) and (b). The unwanted upper-sideband in (c) is removed by filtering.

Unfortunately, this approach had several drawbacks; the principal one being that the cost of each decoder would be increased by the need for two sound descramblers, one digital and one analogue. Also, at line-fed transmitter sites, the analogue sound is generated from the incoming digital stereo sound-in-syncs signal. The analogue sound would therefore need to be scrambled by a coder at the transmitter, which, in turn, would require control data from the vision signal. Bearing in mind the need for main and reserve duplication, this would have involved considerable complication and expense. Alternatively, the sound-in-syncs feed could have carried the sound in analogue scrambled form, but this would have negated the performance advantages of NICAM. Reluctantly, therefore, it was concluded that scrambled NICAM could not be used for the BBC Select service.

The only possibilities remaining were to use a low-cost analogue scrambling technique with little security and degraded sound quality, or to transmit clear (non-scrambled) sound. In fact, the decision was made to provide both, because the option of switching-off the sound scrambling was reasonably economical to implement. This gave an element of flexibility, allowing the choice between quality and restricted access to be made on a service-by-service basis.

Spectral inversion was chosen as the scrambling method because of its simplicity (and hence low cost) and its known characteristics in a terrestrial environment, as it had been used for the BMTV transmissions7. The carrier for spectral inversion was chosen to be 12.51 kHz, derived by dividing the four-times colour subcarrier video clock by 1418, a factor which was convenient for the decoder circuitry. Further details of the sound scrambling system are given in the Appendix.

7. CONCLUSIONS

Although many different scrambling techniques have been used satisfactorily for satellite broadcasting, terrestrial broadcasting places a number of additional constraints on the methods that can be used for scrambling PAL colour television signals. This is principally for two reasons: firstly, the terrestrial distribution network includes several types of equip-ment (such as sound-in-syncs codecs and teletext data generators) which are not required in satellite broadcasting. Secondly, Vestigial-Sideband Amplitude Modulation is used, rather than the more linear Frequency Modulation system used for satellite channels. For these reasons, only scrambling methods that confine their action to the active-picture period and maintain compatible signal ranges are suitable for terrestrial broadcasting.

Scrambled signals can be particularly susceptible to low-level distortions, with which a clear (non-scrambled) signal suffers no perceptible visual impairment. For BBC Select (a scrambled service downloading programmes overnight to domestic video recorders), good picture quality was required in a terrestrial broadcasting environment. In addition, the scrambled signals were required to be reasonably secure, opaque (visually unintelligible) and to have low-cost decoders.

In this context, line rotation scrambling is known to suffer from line tilt and echoes caused by multipath propagation. Very low level echoes, which in themselves are not disturbing, could lead to noticeable impairments when affecting the scrambled picture. This poses a particularly difficult problem because as many as 25% of reception sites may be affected by such levels of multipath propagation. While the line-tilt impairment can be corrected successfully at the receiver, the possibility of correcting for echoes with sufficient accuracy to solve the problem seems remote, thus making line rotation scrambling unlikely to be suitable for use in such a terrestrial environment.

An alternative technique, known as line shuffling, is also susceptible to distortions introduced by terrestrial transmission, such as multipath propagation, hum and field-rate distortion. However, the effect of these distortions can be reduced significantly by careful choice of the parameters of the line-shuffling system. This is achieved by constraining the shuffling process to work with relatively small blocks of lines, fixed in position on the picture, and with no blocks spanning the field intervals. It is also important to choose suitable time-constants for the automatic gain control and clamp circuitry of the receiver/decoder unit. A new line shuffling system has been developed incorporating these requirements and, known as VideoCrypt S, has been manufactured for the BBC Select application.

Although line shuffling allows the impairments to be minimised, there are some types of distortion, such as that arising from co-channel interference, which remain a problem for both line shuffling and the line rotation technique. It has been estimated that, for scrambled transmissions, this would result in somewhat poorer pictures being obtained at perhaps 6% of reception sites. For the longer term, the introduction of a broadcast system based on digital coding and incorporating digital signal scrambling is likely to form a more satisfactory basis for conditional access television services than any technique involving scrambling the analogue signals.

8. REFERENCES

1. GALE, B. *and* BYLIN, F., 1986. Satellite and Cable TV Scrambling and Descrambling. Baylin/Gale Productions.

2. KNEE, M.J., 1985. DBS pay television: picture signal scrambling. BBC Research Department Report No. BBC RD 1985/12.

3. EBU, 1986. Specification of the systems of the MAC/packet family. EBU Doc. Tech. 3258-E.

4. EDWARDSON, S.M., 1984. Scrambling and encryption for direct broadcasting by satellite. IBC ’84. IEE Conference Publication No. 240, pp. 273-281.

5. EDWARDSON, S.M., 1986. A conditional access system for direct broadcasting by satellite. BBC Research Department Report No. BBC RD 1986/11.

6. ELY, S.R., 1990. BBC conditional access television services. Proceedings of the ACSA 90 (Accès Conditionnel aux Services Audiovisuels) Conference, CETT, Rennes, pp. 301-316.

7. ELY, S.R. *and* SHUTTLEWORTH, S.R., 1988. Conditional access scrambling techniques for terrestrial UHF television broadcasts. IBC '88. IEE Conference Publication No. 293, pp. 318-322.

8. BBC, 1986. Off-air control of domestic television equipment.
Inventor: SANDBANK, C.P.
UK Patent No. 2,192,473.

9. BBC, 1988. Remote control of downloading.
Inventor: ROBINSON, A.P.
UK Patent No. 2,219,160.

10. MARTI, B. *and* MAUDUIT, M., 1975. DISCRET, service de télévision cryptée. *Revue de radiodiffusion-télévision*, No. 40, pp. 24-30.

11. LEDUC, M., 1990. Systèm de télévision à péage à contrôle d'accès pleinement détachable, un exemple d'implémentation: Videocrypt. Proceedings of the ACSA 90 (Accès Conditionnel aux Services Audiovisuels) Conference, CCETT, Rennes, pp. 81-94.

12. HASHKES, J. *and* COHEN, M., 1990. Managing smart card for Pay Television: the VideoCrypt Approach. Proceedings of the ACSA 90 (Accès Conditionnel aux Services Audiovisuels) Conference, CCETT, Rennes, pp. 213-224.

13. CCIR, 1992. Digital terrestrial broadcasting in the VHF/UHF bands. CCIR documents 1990-1994. Document 11/77, draft new recommendation.

14. WESTINGHOUSE CORPORATION, 1975. UK Patent No. 1,503,051. A secure television transmission system.

15. French Patent No. 2,431,809. Procédés et dispositifs de brouillage de de débrouillage pour images de télévision.

16. CCIR, 1981. Scrambling of television signals by the Discret system. CCIR documents 1978-1982, 4th June, Doc. 11/265 (France).

17. CHRISTIANSEN, M., RØSTE, T. *and* SKÅLVIC, J.N., 1987. A video scrambler/ descrambler concept for the PAL format. Journal I.E.R.E.**,** **57**(1), January/February, pp. 27-35.

18. CCIR, 1990. Radio-frequency protection ratios for AM vestigial sideband television systems. Recommendation 655-1. Recommendations of the CCIR, Geneva, XI-1, pp. 74-89.

19. BLOCK, R.S. *and* MARTIN, J.R., 1980. Method and system for secure transmission and reception of video information particularly for television, 25th February. International Patent Application No. WO 81/02499.

20. DEVEREUX, V.G., 1974. Application of p.c.m. to broadcast quality video signals. *Radio and Electron. Eng.*, **44**(7) July, pp. 373-381 and **44**(9), September, pp. 463-472.

21. DEVEREUX, V.G., 1977. Permissible timing jitter in broadcast PAL colour television signals. BBC Research Department Report No. BBC RD 1977/14.

22. COHEN, H. *and* FOULLET, J-M., 1988. Procédé et dispositif de permutation de lignes de télévision par bloc. French Patent Application No. 88 00361, 14th January. Publication No. 2,626,131.

23. DIFFIE *and* HELLMAN, 1979. An introduction to cryptography. *Proc. I.E.E.E.*, **67**(3) March, pp. 408-411.

24. BBC, 1987. Scrambling of analogue electrical signals.
Inventor: PARKER, M.A.
UK Patent No. 2,207,328.

APPENDIX

Specification of the Scrambled BBC Select Signal

This Appendix provides a limited specification of the parameters of the scrambled BBC Select signal, based on the VideoCrypt-S line-shuffling system. The general waveform and broadcast emission parameters of the signal are those of the PAL System-I standard, as detailed in 'Specification of television standards for 625-line System I transmissions', published in 1984 by the Department of Trade and Industry.

A.1 VISION SIGNAL

The scrambled video signals produced by line shuffling differ in several ways from those of a normal PAL signal. Some of the active lines are moved from their original positions, some are replaced by data waveforms and some are blanked. However, the main characteristics of the waveform, that is, the signal amplitudes and bandwidths, the line and field synchronisation waveforms and the blanking periods, are all maintained in standard form.

Although the scrambled signal maintains the correct signal amplitudes, it should be noted that, if PAL-decoded, some of the PAL signal components may be larger than normal. Shuffling the lines, and then PAL-decoding the scrambled signal (such as would occur if the shuffled signal were recorded on a component tape recorder), can cause the U and V components of the PAL signal to be interchanged. The larger V components passing through the U channel could be clipped by the recorder circuitry if fully saturated colours were encountered; though in other respects, the recorded signal could be descrambled satisfactorily.

A.1.1 Sampling parameters

Although the scrambled signal is broadcast in analogue form, the shuffling process is carried out by digital processing using a sampled version of the original signal. Because of this, the parameters of the sampling process have an influence on the resulting scrambled signal and, for correct operation, have to be reproduced in the descrambler.

The sampling frequency is four-times the PAL colour subcarrier frequency, that is, 17.734475 MHz. The phase of sampling is locked to the mean phase of the subcarrier reference burst, so that samples are taken at the 45°, 135°, 225° and 315° points relative to the 0° subcarrier reference phase (the +U axis). This is shown in Fig. A.1. The samples are, therefore, taken at the peaks and zero-crossings of the 135° and 225° burst waveforms.

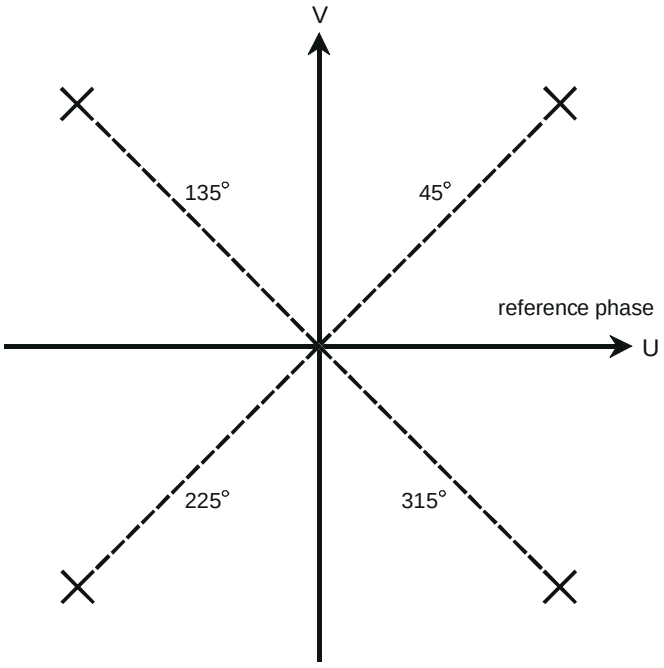


Fig. A.1 - Vector diagram showing the four sample-phase positions used in the coder and decoder of the line shuffling scrambling system. The subcarrier reference phase is the +U axis.

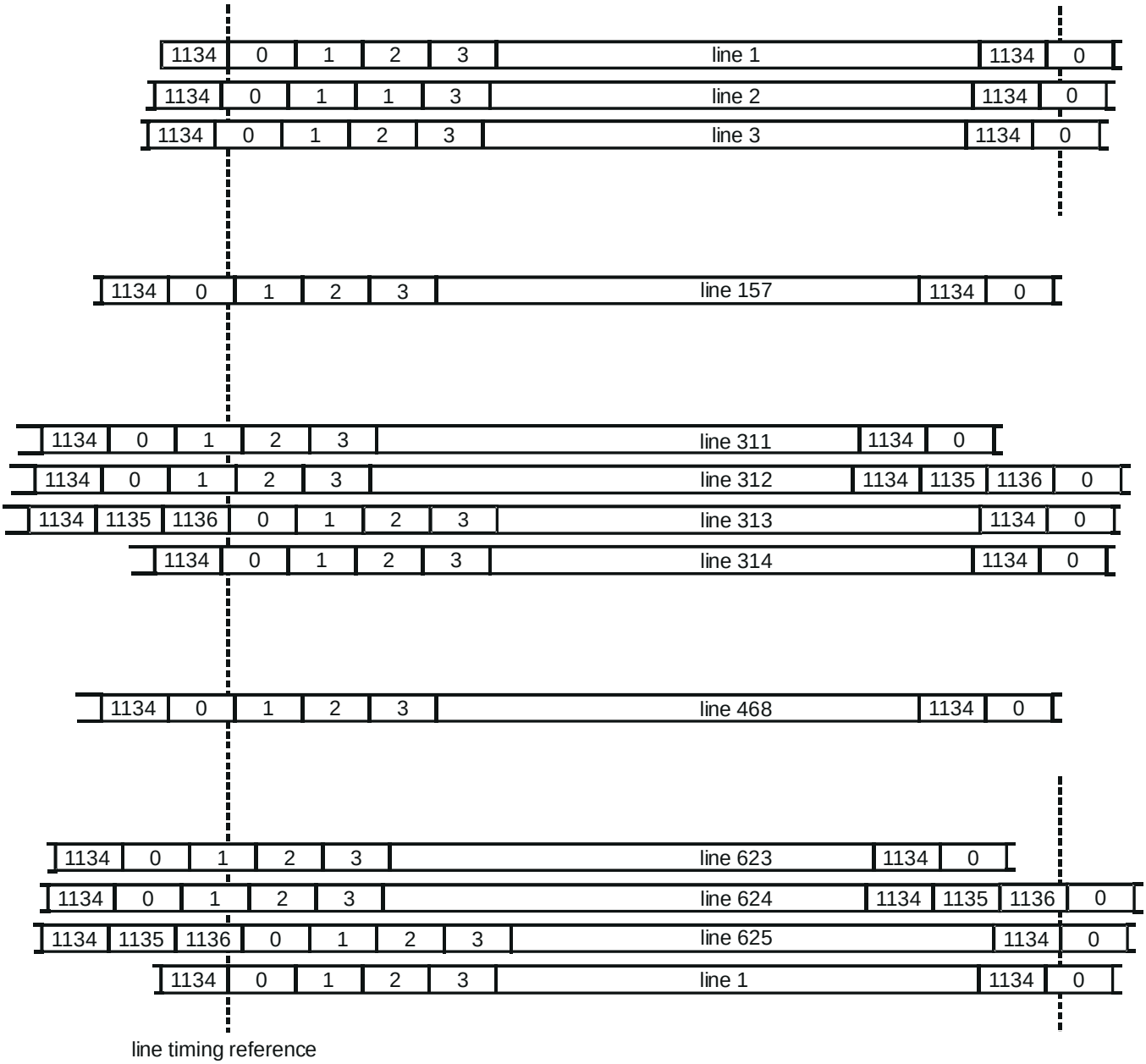


Fig. A.2 - The system of sample numbering used in the line shuffling scrambling system. Lines 312 and 624 contain 1137 samples, whilst all other lines are made up of 1135 samples.

Sampling at four-times the subcarrier frequency results in a picture-locked pattern of sampling sites. The sampling structure is also very nearly line-locked, there being 1135.0064 sample periods per line, or two samples extra per field. Because of this, it has proved convenient to group the samples into ‘lines’, such that all the lines of the picture except two contain 1135 samples, and the remaining two contain 1137 samples each. Lines 312 and 624 are the lines containing 1137 samples, so that the pattern of samples is as shown in Fig. A.2. The transitions between the groups of 1135 or 1137 samples (the ‘lines’ of the sampling structure) are loosely synchronised to the line timing reference (the line sync falling edge) of the analogue signal.

When a line of signal is shuffled, only the active-line portion is moved. The range of samples that can be moved without disturbing the line waveforms, taking account of the tolerances of the sync, burst and blanking waveforms, is shown in Fig. A.3. Apart from adhering to these limits, there is no necessity for the group of samples moved in the decoder to be identical to those moved in the coder. The position of the samples moved will vary relative to the line timing reference by ±1 clock period down the field, because of the skew of the sampling structure shown in Fig. A.2.

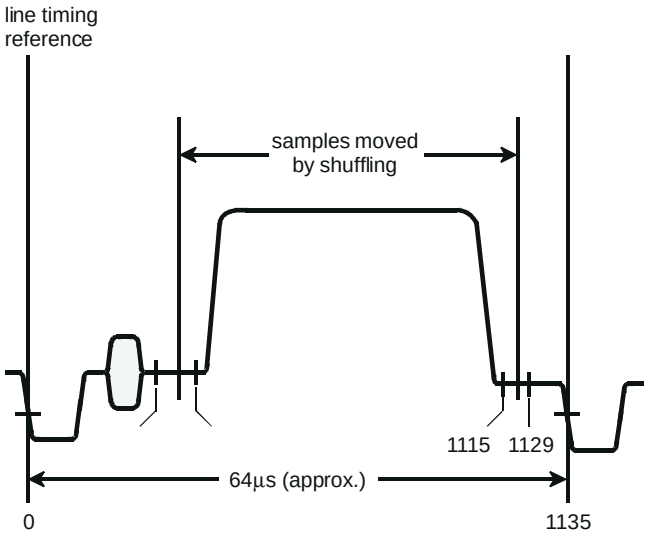


Fig. A.3 - Definition of the samples which can be moved by the line shuffling process relative to a zero reference at the line sync edge.

The start position has to fall between 151 and 165, and the end position between 1115 and 1129. Nominal values taking the middle of each range are samples 158 to 1122, or a total of 965 samples. The samples moved will vary in position on the line by æ1 clock period down the field because of the sample skew shown in Fig. A.2.

A.1.2 Structure of the shuffled picture

The shuffling process only affects the active-picture lines of the signal, that is, lines 23 to 310 on the first field and lines 336 to 623 on the second field.

In the scrambled signal, four active-picture lines on each field are set aside for VideoCrypt S data signals. These are lines 24 to 27 on the first field and lines 336 to 339 on the second field. The form of the data waveforms on these lines is described in Section A.1.3.

In the shuffled signal, lines 28 to 309 and 340 to 621 inclusive contain shuffled lines, consisting of six blocks of 47 lines on each field. Each shuffled block contains lines originating from positions one block later in the input signal. The positions of the blocks and the lines from the original picture that each block contains are shown in Table 1.

The half lines, lines 23 and 623, and the last full line of each active field, 310 and 622, are not moved by the shuffling process, but are blanked in order not to prejudice security.

Table A.1 - Definition of the shuffling blocks.

Block	Extends from ... to ...	Includes original lines
1	28-74	75-121
2	75-121	122-168
3	122-168	169-215
4	169-215	216-262
5	216-262	263-309
6	263-309	340-386
7	340-386	387-433
8	387-433	434-480
9	434-480	481-527
10	481-527	528-574
11	528-574	575-621
12	575-621	28-74
		(from next picture)

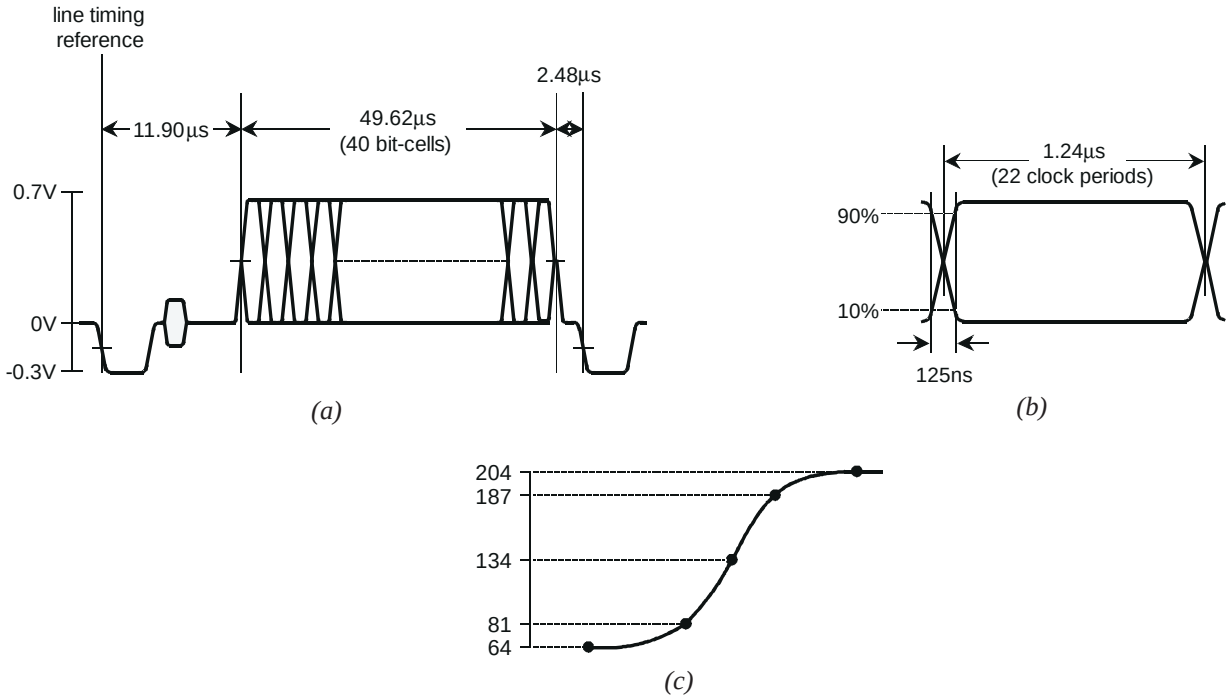


Fig. A.4 - Amplitude and timing details of the data waveforms on lines 24-27 and 336-339.

(a) the nominal position of the 40 bit-cells relative to the line timing reference, (b) the duration and rise and fall times of an individual bit-cell, and (c) the signal levels, in terms of 8-bit reference levels, used to synthesise the rising and falling edges of the data waveform.

A.1.3 Data signal waveforms

The waveform of the data signals on lines 24 to 27 and lines 336 to 339 is shown in Fig. A.4. The 0 and 1 levels of the data waveform are defined as the black and white levels of the video waveform, corresponding to eight-bit digital coding levels of 64 and 204 in a signal coded with 5 mV per step.

Each line contains 40 bit-cells, each of duration 22 clock periods or 1.24 µs, shown in Figs. A (a) & (b)). The start of data, signified by the half-amplitude point of the first bit-cell, occurs nominally 11.90 µs after the line-timing reference point, although the positions of all the bit-cells are dependent on the subcarrier-to-sync phase of the incoming signal. As the decoder uses the line synchronising information to locate and sample the data waveform, correct data decoding depends on this timing relationship being preserved. Broadcast transmitters, in which the synchronising pulses are reinserted or carried in a separate signal path, can introduce large variations in sync-to-data timing.

The bit transitions, shown in Fig. A.4(c), are generated from sample values of (in eight-bit terms) 64, 81, 134, 187 and 204 for a rising edge, and 204, 187, 134, 81 and 64 for a falling edge. The transitions therefore have a nominal duration of 0.125 µs (10–90%).

A.1.4 Data signal content

The four data lines of one field are used to carry ten bytes of source data, consisting of an information byte, eight bytes of security data and a check byte. The check byte is formed by adding the information byte and the eight security bytes, modulo-256. Each byte is coded for error protection using a Hamming 8,4 code, so that the ten bytes are increased to ten 16-bit words for transmission. The Hamming coded words are then subject to a process of interleaving, which distributes the 160 bits in a complex pattern into the four data lines of one field.

The information byte can be of five different types: header, frame count, sub-header, system and channel. The header and sub-header bytes are always transmitted on the data lines of the first field, while the frame count, system and channel bytes are transmitted on the second field data lines.

Header

Header bytes are used for synchronising the data sequence and take only the hexadecimal values 81, 92, A3, B4, C5, D6, E7 and F0.

Frame count

The frame count byte takes the hex values 00 to FF and is incremented by one at each frame (picture) interval.

Sub-header

The sub-header bytes are also used for synchronisation and take the values 18, 29, 3A, 4B, 5C, 6D, 7E and 0F.

System

The system byte indicates the structure used in the data lines, the video scrambling mode and the access control mode (see Section A.2).

Channel

The channel byte indicates the broadcast channel (either BBC1 or BBC2) and whether sound scrambling is being used or not.

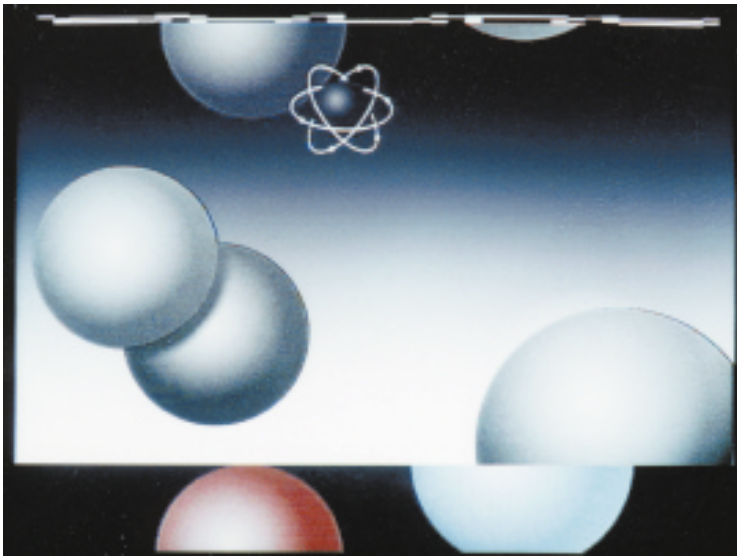
A.2 VIDEO SCRAMBLING MODES

The BBC Select scrambling system can operate in a number of different scrambling modes. There are three principal modes: Clear, Free-Access Scrambled and Controlled-Access Scrambled. With Clear transmissions, the signal remains essentially unaltered by the scrambler. With the Free-Access mode, the signal is scrambled by line-shuffling, but a fixed control word is used in both the scrambler and descrambler. Possession of a decoder is, therefore, sufficient to descramble the signals. With Controlled-Access scrambling, new control words are added to the signal in encrypted form every 16 pictures. These have to be decrypted by a smart card before the signals can be descrambled.

In the Controlled-Access mode, in addition to the Full-Shuffled mode, there are two alternative scrambling modes, known as Clear Delayed and Half-Shuffled. The Clear-Delayed mode incorporates all the scrambling processes except that the lines of a block are not shuffled. This is useful for diagnostic purposes under fault conditions. In the Half-Shuffled mode only the first field is scrambled, while on the second field the lines within each block are not shuffled. This allows the content of the scrambled picture to be seen, while providing an annoying disturbance to the picture. The Clear-Delayed and Half-Shuffled modes are shown in Fig. A.5. Both modes are fully descrambled by an authorised decoder. The Half-Shuffled mode is also available in free access.

A.3 SOUND SIGNAL

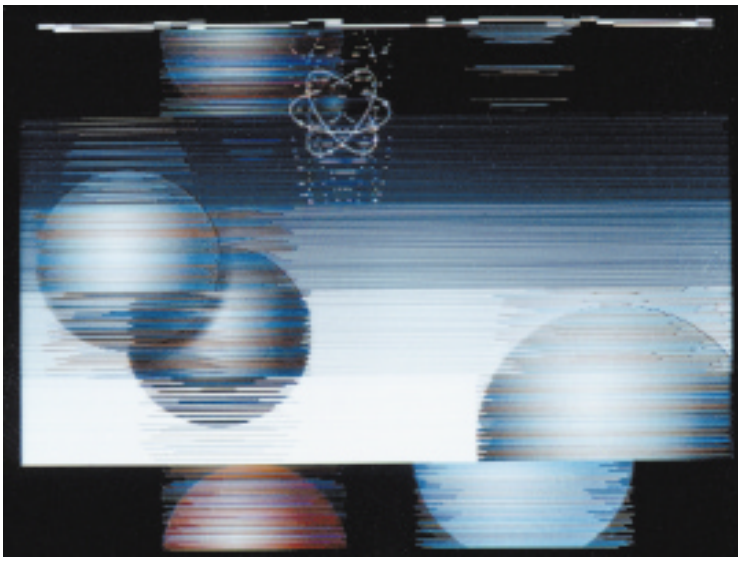
The sound signal can be either clear or scrambled, a condition which is indicated by the value of one bit in the channel byte. When scrambled, the sound signal is conveyed as spectrally-inverted modulation of the FM sound carrier using an inversion frequency of the video clock frequency (four-times colour subcarrier) divided by 1418 (equals 12.51 kHz). The scrambled signal is reduced in level by 12 dB to take account of the subsequent pre-emphasis of the FM signal. The two channels of stereo sources are averaged to produce a combined monophonic signal for scrambling.



(a)

Fig. A.5 - Additional scrambling modes of the BBC Select system.

(a) the Clear-Delayed mode and
(b) the Half-Shuffled mode.



(b)

Published by BBC RESEARCH & DEVELOPMENT DEPARTMENT, Kingswood Warren, Tadworth, Surrey, KT20 6NP