PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 :		(11) International Publication Number:	WO 90/08376
G09G 1/16	A1	(43) International Publication Date:	26 July 1990 (26.07.90)

(21) International Application Number: PCT/GB90/00036

(22) International Filing Date: 11 January 1990 (11.01.90)

(30) Priority data:
8900817.1 14 January 1989 (14.01.89) GB

(71) Applicant *(for all designated States except US)*: UNIVERSITY COURT OF THE UNIVERSITY OF ST. ANDREWS [GB/GB]; College Gate, Saint Andrews KY16 9AJ (GB).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)* : MAITLAND, Arthur [GB/GB]; 15 Canongate, Saint Andrews KY16 8RU (GB). HIRST, Peter, Frank [GB/GB]; 8 Rhoshendre, Wavnfawr, Aberystwth, Dyfed SY23 3PT (GB).

(74) Agent: FITZPATRICKS; 4 West Regent Street, Glasgow G2 1RS (GB).

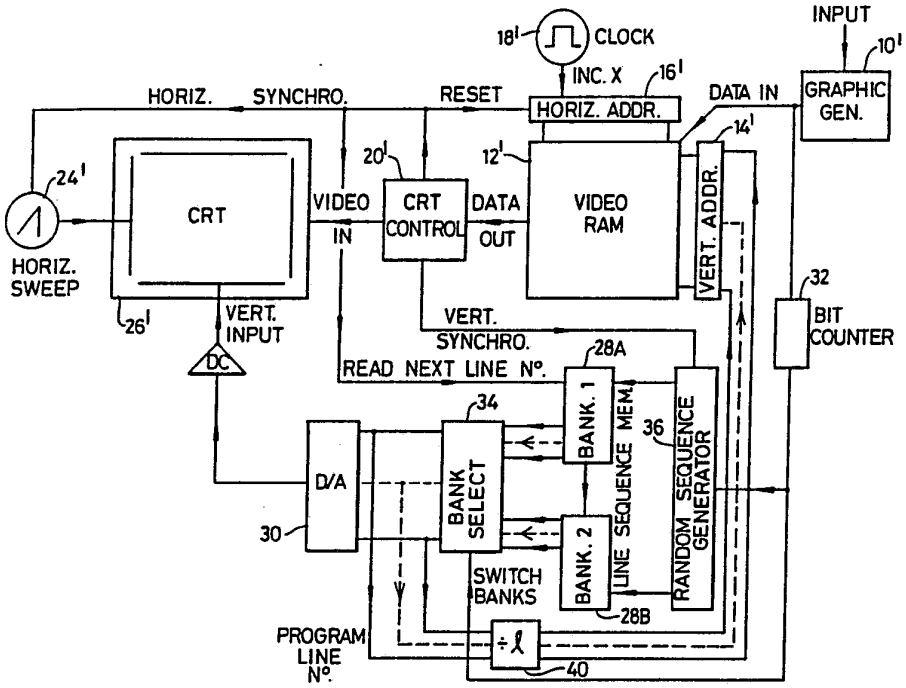
(81) Designated States: AT (European patent), BE (European patent), CH (European patent), DE (European patent), DK (European patent), ES (European patent), FR (European patent), GB (European patent), IT (European patent), LU (European patent), NL (European patent), SE (European patent), US.

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: SECURITY SYSTEM FOR VISUAL DISPLAY UNITS AND PERSONAL COMPUTERS

(57) Abstract

An electronic security system for protecting visual display units (VDU's) and personal computers against remote electromagnetic surveillance of data displayed on cathode ray tubes (CRT's) operates by scrambling the scanning pattern of the CRT (26') such that it is scanned in a non-consecutive manner. A random sequence generator (36) scrambles the order in which data is read from the video RAM (12') of a VDU and a digital to analogue convertor (30) controls the scanning pattern of the CRT (26') such that the data output from the video RAM (12') is displayed on the CRT (26') at the correct position whilst the CRT (26') is scanned in a non-consecutive order. In the described embodiment complete horizontal lines are scanned in a random order, however the system could be adapted to scramble the order of vertical columns, portions of rows or columns, or individual pixels. In order to hinder decryption, the scanning order can be changed at random or periodic intervals, or whenever the displayed data is altered significantly.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	ES	Spain	MG	Madagascar
AU	Australia	FI	Finland	ML	Mali
BB	Barbados	FR	France	MR	Mauritania
BE	Belgium	GA	Gabon	MW	Malawi
BF	Burkina Fasso	GB	United Kingdom	NL	Netherlands
BG	Bulgaria	HU	Hungary	NO	Norway
BJ	Benin	IT	Italy	RO	Romania
BR	Brazil	JP	Japan	SD	Sudan
CA	Canada	KP	Democratic People's Republic of Korea	SE	Sweden
CF	Central African Republic			SN	Senegal
CG	Congo	KR	Republic of Korea	SU	Soviet Union
CH	Switzerland	LI	Liechtenstein	TD	Chad
CM	Cameroon	LK	Sri Lanka	TG	Togo
DE	Germany, Federal Republic of	LU	Luxembourg	US	United States of America
DK	Denmark	MC	Monaco		

"Security System for Visual Display Units and Personal Computers"

The present invention relates to an electronic security system for protecting visual display units (VDU's) and personal computers against remote electromagnetic surveillance techniques employed by electronic eavesdroppers.

All electronic circuitry is a source of electromagnetic radiation. Electromagnetic emissions from personal computers and visual display units can be detected at some distance and decoded to give an intelligible copy of the information being displayed. Of all the sources of radiation in a desk top computer system, video display unit represents the greatest security risk as the information being displayed is not generally encrypted - it must be readily understood by the operator. Text, for example, usually appears on the screen in plain language numbers in plain numerals, and graphics as an accurate image. Furthermore, the standard technology of VDU's makes the detection and decoding of electromagnetic emissions from them particularly easy.

The high voltage signal across the electron gun of the cathode ray tube (CRT) gives rise to strong radiation, typically between about 1MHz and 30MHz depending on the pixel density of the graphic display. By monitoring radiation of a sufficiently short wavelength with a directional antenna the emissions from one particular VDU can be resolved and then decoded. Even at longer wavelengths, interferometric techniques could be used to obtain the required resolution.

The radio waves emitted from the electron gun and the screen may be complex in detail, but essentially form a simple pulsed signal. The electron beam in the CRT scans across the screen in a linear fashion, line by line. Whenever the beam is allowed to strike the screen a pixel of information is displayed at that point. At this time, an associated burst of electromagnetic radiation is produced.

The linear scanning technique means that the delay between these pulses of radiation gives information about the position on the screen of the pixel. All the eavesdropper has to do is to synchronise his display, which scans in the same manner as the target display, with the incoming pulses and then use these pulses as the basic input for his display. Surveillance equipment which performs this task at a range of up to a few hundred metres outside the building where the target VDU is situated is commercially available at a cost comparable to that of a personal computer system.

At present, the commercially available equipment which gives protection against illicit surveillance, still known by its NATO codename of "Tempest" involves heavily screening the VDU by encasing it in metal and covering the screen with wire mesh. This process is expensive - protected equipment can cost 50 - 200% more than the equivalent, unprotected system. However, theory and experiment show that screening is not a trivial task and it is actually exceedingly difficult (if not impossible) to effectively reduce all electromagnetic emissions from the screened system to zero. Tempest standards actually do allow some leakage to occur and, whilst it is claimed that Tempest equipment is protected from surveillance at distances greater than about one metre, equipment for surveillance at much greater distances, nevertheless is available.

It is an object of the present invention to provide a security system for VDU's and personal computers which provides enhanced security at a greatly reduced cost in comparison with existing techniques.

A security device embodying the invention and described herein is divided, conceptionally, into two parts - an "encoder" and a "decoder". The encoder is installed at some point in the VDU circuitry in an integrated circuit and scrambles the order in which the data is sent to the screen. The decoder does not actually decode the data (which is sent in its scrambled order to the screen) but consists of circuitry which causes the CRT screen to be scanned in the same scrambled order in which the data is being sent to it.

Thus, for instance, instead of scanning lines 1 to, say, 500 consecutively they are scanned in some other order:- line 10, line 358, line 45, etc. Alternatively, a more complex scanning pattern can be achieved by parsing the data into more units (ie parts of lines, groups of pixels or even individual pixels) and encoding the order of these units.

These different scanning orders do not significantly alter the appearance of the VDU picture to the operator since all data appears at the correct location on the screen, but they do break up the normal, linear data flow which allows the radiation from the screen to be easily decoded. Anyone monitoring the emissions from the screen who has no knowledge of the "random" scanning order is faced with a major decryption problem the information can be made intelligible.

If the coding system is updated periodically (optimally every time the information on the display changes) then the decryption can be rendered even more arduous or even impossible. This continuous update of the coding system may be achieved by the encoder producing a new random code and programing the decoder with this code before the visual data is sent.

Accordingly, the invention provides a security apparatus for a visual display unit comprising a cathode ray tube including an electron gun, a cathode ray tube controller and a video memory adapted to hold data representing individual pixels of an image to be displayed on the cathode ray tube, said apparatus comprising means for scrambling the order in which said data are output from the video memory to the cathode ray tube controller, such that the video signal applied to the electron gun from the cathode ray tube controller is non-consecutive, and means for controlling the scanning pattern of the electron gun such that the image displayed on the cathode ray tube appears as it would if the video data were output from the video memory and the cathode ray tube scanned in a normal, consecutive manner.

Preferably, the order in which the data are output from the video memory and the corresponding scanning pattern of the electron gun are altered from time to time. It is particularly preferred that the order is altered whenever the image represented by the data in the video memory is changed significantly. Alternatively, the order can be changed periodically at predetermined or random time intervals.

Preferably also, the visual display unit further includes a horizontal address counter and a vertical address counter which select the video memory locations of pixels which are to be displayed, and said scrambling means comprises a random sequence generator for applying a random sequence of addresses to at least one of said address counters.

Preferably also, said means for controlling the scanning pattern of the electron gun comprises a digital to analogue convertor connected to receive a digital signal corresponding to the random sequence applied to the address counter and to output an analogue signal to control the scanning of the cathode ray tube such that the image is scanned in an order corresponding to the order in which the data are output from the video memory.

In the embodiment described herein, the scrambling means generates a random sequence of vertical addresses and the scanning control means replaces the conventional vertical voltage-ramp generator of the visual display unit such that complete horizontal lines of the image are scanned in a random order.

Preferably, the sequence of the addresses produced by the scrambling means is stored in a line sequence memory, and said line sequence memory comprises at least two memory banks, each capable of holding a complete sequence of addresses to be applied to the address counter, one of which holds the current sequence of addresses and the other of which holds a new sequence to be applied to the address counter when the order of data output and the scanning pattern are to be altered, the apparatus further including

switching means for selectively connecting one or other of the memory banks to the address counter.

Preferably also, means are provided for monitoring the data input to the video memory, activating the scrambling means to generate a new address sequence, which is entered in the currently inactive one of the two memory banks, and for operating said switching means whenever the monitoring of the data input into the video memory indicates that a complete or predetermined fractional change of the data stored therein has taken place.

An embodiment of the invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

Fig. 1 is a schematic block diagram of the video circuitry of a conventional VDU; and

Fig. 2 is a schematic block diagram of the video circuitry of a VDU incorporating a security system embodying the present invention.

Fig. 1 shows schematically the arrangement of the video circuitry of a typical VDU, comprising a graphic generator 10, which provides the basic input data for the VDU, video random access memory (RAM) 12, vertical and horizontal address counters 14 and 16, clock 18, CRT controller 20, vertical and horizontal voltage-ramp generators 22 and 24, and cathode ray tube 26. The video RAM 12 is a block memory which has a memory location associated with each individual pixel of the display. It is convenient to draw the memory as a two dimensional array in order to emphasise the one-to-one bit-mapping between a memory location and the pixel that it controls. Thus, the video RAM 12 stores an exact, pixel by pixel copy of the picture to be displayed on the screen. The address counters 14 and 16 are driven by the clock 18 to address the data stored in the video RAM 12 in sequence, which is output sequentially to the CRT controller 20. The horizontal address counter 16 is incremented on each clock pulse and the vertical address counter 14 is incremented at the end of each complete horizontal line. The CRT controller 20 resets

the counters at the end of each complete horizontal line and each complete vertical scan, respectively.

The CRT controller 20 thus reads off the data stored in the video RAM and also adds horizontal and vertical synchronisation pulses to mark the beginning of each new line and each new frame, respectively. The signal derived from the video RAM 12 may contain monochrome or colour information and is used to control the electron gun (not shown) in the CRT 26. The horizontal and vertical synchronisation pulses are used to trigger the voltage-ramp generators 22 and 24 which drive the scanning apparatus in the CRT.

The electron gun only writes on the screen when the electron beam is scanning from, say, left to right along one of the horizontal lines. During the finite time that the electron beam takes to return to the left hand side of the screen and the beginning of the next horizontal line (the flyback period) the CRT controller 20 sends a horizontal blanking pulse which ensures that the electron gun does not write on the screen and thus cause a spurious trace. If the beam is scanning vertically from the top to the bottom of the screen, then when the beam has reached the bottom right-hand corner of the screen the CRT controller sends a vertical or frame blanking pulse which allows the beam to return to the top left hand corner of the screen without the production of spurious traces. The orientation of the scanning lines is arbitrary (they may be left-to-right or top-to-bottom), as is the direction of scanning (left-to-right or right-to-left) but the scheme described above is, by far, the most common.

An implementation of a coding system, embodying the invention, which scrambles the order in which the horizontal lines of the display are scanned is shown schematically in Fig. 2, wherein parts corresponding to those of Fig. 1 are designated 10', 12', etc. There are two main modifications to the operation of the CRT controller 20' as described above. Firstly, the vertical address counter 14' can be programmed with any address, rather than simply incrementing

up to some address and then resetting. A sequence of vertical addresses in random order is produced by a random sequence generator 36, and is loaded into the line sequence memory 28A, 28B. The randomly ordered list of addresses then defines the order in which the lines are to be scanned. The vertical address counter 14' is programmed with the random list from the line sequence memory 28A, 28B during the horizontal flyback period given by the horizontal blanking pulse. Each horizontal line is still scanned sequentially, as in the conventional system of Fig. 1, using the horizontal address counter 16' and the clock 18'.

Secondly, the vertical voltage-ramp generator 22 of Fig. 1 is replaced with a digital-to-analogue (D/A) convertor 30 which is also programmed from the line sequence memory 28A, 28B to produce the electron beam deflection appropriate to the particular horizontal line being displayed. The D/A convertor 30 is also programmed during the horizontal flyback period. The horizontal flyback period will always be of sufficient duration to allow time for the electron beam to move to the beginning of the next line to be scanned.

In order to provide the maximum degree of encryption the line sequence memory is periodically reprogrammed with a new sequence. The use of more than one line sequence for a given set of information displayed on the screen, however, provides alternative coding which tends to ease decryption of the information. Thus, the optimum coding is achieved if the line sequence memory is reprogrammed every time there is a significant change in the information displayed on the screen. This timing can be derived from digital circuitry 32 (comprising a bit counter) which counts the number of bits written to the video RAM 12' and initiates reprogramming of the line sequence memory when this number corresponds to the amount of information displayed in one complete screen (or some fraction of a screen full). Alternatively, the timing can simply be derived from a clock and set at, say, a few seconds - this system being preferred when, for instance, graphics are being displayed and a

processor external to the CRT controller is directly programming the video memory.

The actual reprogramming of the line sequence memory must be fast enough to be completed within the vertical flyback time. The simplest way of achieving this is to have two banks 28A and 28B of line sequence memory and switch between memory banks 28A and 28B during vertical flyback. In Fig. 2 the necessary switching circuitry is represented by the "bank select" block 34. The memory bank which has just been switched out can then be reprogrammed from the random sequence generator 36 during the relatively long period between line sequence memory reprogramming. In the case where there is more than one scan line per pixel, circuitry, represented by a "divide by " block 40, may be introduced between the bank select circuitry 34 and the vertical address register 14', which gives the pixel line number appropriate to the current scan line (being equal to the number of scan lines per pixel).

A line scrambling system, based upon an integrated circuit, may be fitted easily at the design stage of a personal computer or VDU and can also be retrospectively fitted to existing equipment, replacing parts of the original circuitry, to provide a cheaper and more secure alternative to Tempest equipment. For even greater security the system could be installed in Tempest equipment. The embodiment described herein only randomises the order in which complete horizontal lines are scanned, however it will be appreciated that a similar approach could be applied to randomise the order in which individual pixels or groups of pixels are scanned within each horizontal line.

For still greater security the apparatus may be augmented by the addition of a semi-random noise generator to mask noise and clock frequency signals generated by the computer or VDU which might otherwise provide useful information of assistance in the decryption of the scrambled video signals.

CLAIMS

1. A security apparatus for a visual display unit comprising a cathode ray tube including an electron gun, a cathode ray tube controller and a video memory adapted to hold data representing individual pixels of an image to be displayed on the cathode ray tube, said apparatus comprising means for scrambling the order in which said data are output from the video memory to the cathode ray tube controller, such that the video signal applied to the electron gun from the cathode ray tube controller is non-consecutive, and means for controlling the scanning pattern of the electron gun such that the image displayed on the cathode ray tube appears as it would if the video data were output from the video memory and the cathode ray tube scanned in a normal, consecutive manner.

2. The apparatus of claim 1, wherein the order in which the data are output from the video memory and the corresponding scanning pattern of the electron gun are altered from time to time.

3. The apparatus of claim 2, wherein the order is altered whenever the image represented by the data in the video memory is changed significantly.

4. The apparatus of claim 2, wherein the order is changed periodically at predetermined or random time intervals.

5. The apparatus of any of claims 1 to 4, wherein the visual display unit further includes a horizontal address counter and a vertical address counter which select the video memory locations of pixels which are to be displayed, and said scrambling means comprises a random sequence generator for applying a random sequence of addresses to at least one of said address counters.

6. The apparatus of claim 5, wherein said means for controlling the scanning pattrern of the electron gun comprises a digital-to-analogue convertor connected to receive a digital signal corresponding to the random sequence applied to the address counter and to output an analogue signal to control the scanning of the cathode ray tube such that the

image is scanned in an order corresponding to the order in which the data are output from the video memory.

7. The apparatus of claim 6, wherein the scrambling means generates a random sequence of vertical addresses and the scanning control means controls the vertical position at which the cathode ray tube is scanned such that complete horizontal lines of the image are scanned in an order corresponding to the order in which the data are output from the video memory.

8. The apparatus of any of claims 5, 6 or 7, wherein the sequence of the accresses produced by the scrambling means is stored in a line sequence memory, and said line sequence memory comprises at least two memory banks, each capable of holding a complete sequence of addresses to be applied to the address counter, one of which holds the current sequence of addresses and the other of which holds a new sequence to be applied to the address counter when the order of data output and the scanning pattern are to be altered, the apparatus further including switching means for selectively connecting one or other of the memory banks to the address counter.

9. The apparatus of claim 8, wherein means are provided for monitoring the data input to the video memory, activating the scrambling means to generate a new address sequence, which is entered in the currently inactive one of the two memory banks, and for operating said switching means whenever the monitoring of the data input into the video memory indicates that a complete or predetermined fractional change of the data stored therein has taken place.

1/2

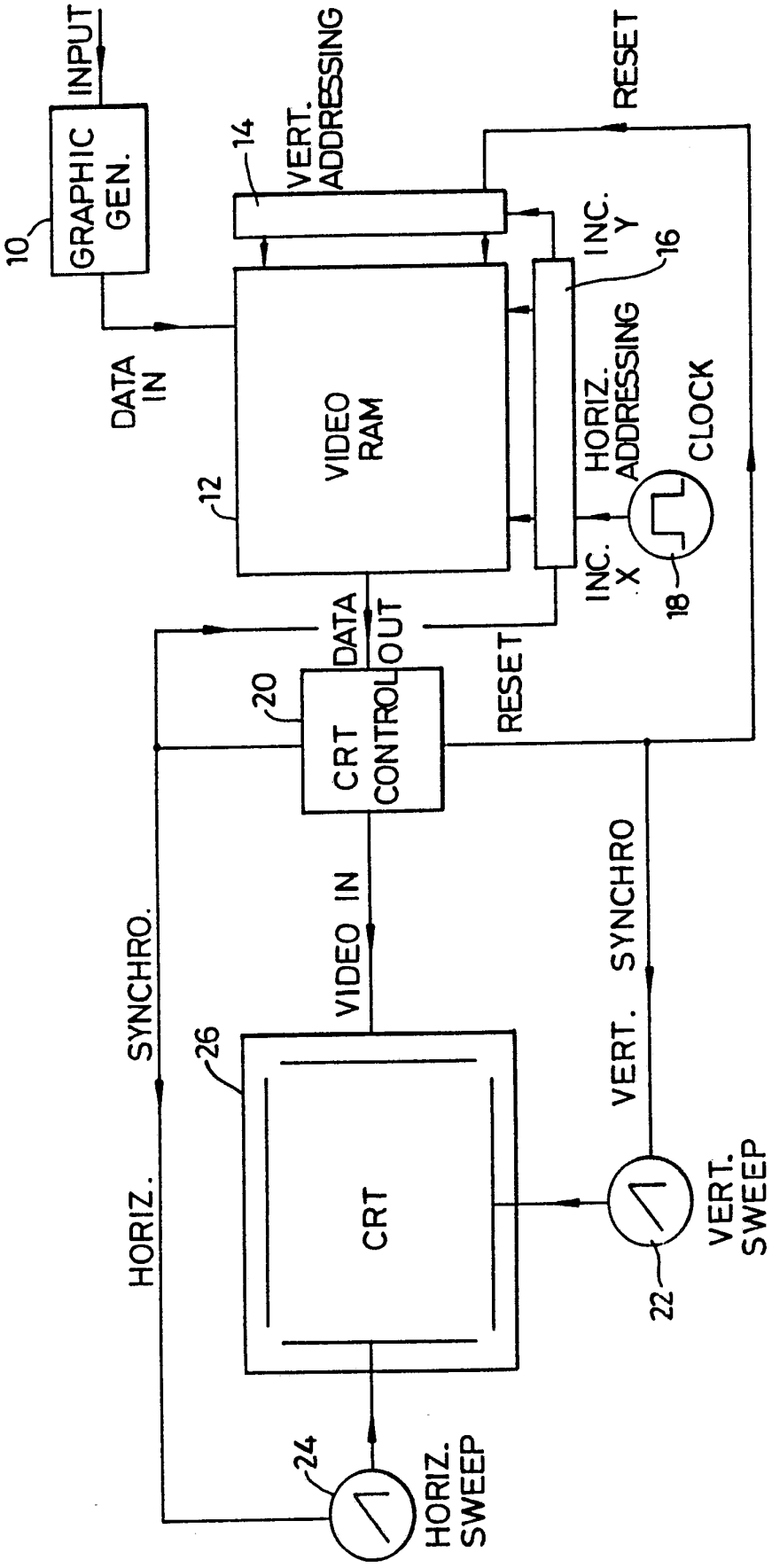

INPUT
GRAPHIC GEN.
10
VERT. ADDRESSING
14
RESET
INC. Y
16
DATA IN
VIDEO RAM
12
HORIZ. ADDRESSING
CLOCK
INC. X
18
DATA OUT
RESET
20
CRT CONTROL
SYNCHRO.
VIDEO IN
VERT. SYNCHRO
26
HORIZ.
CRT
VERT. SWEEP
22
24
HORIZ. SWEEP

Fig. 1

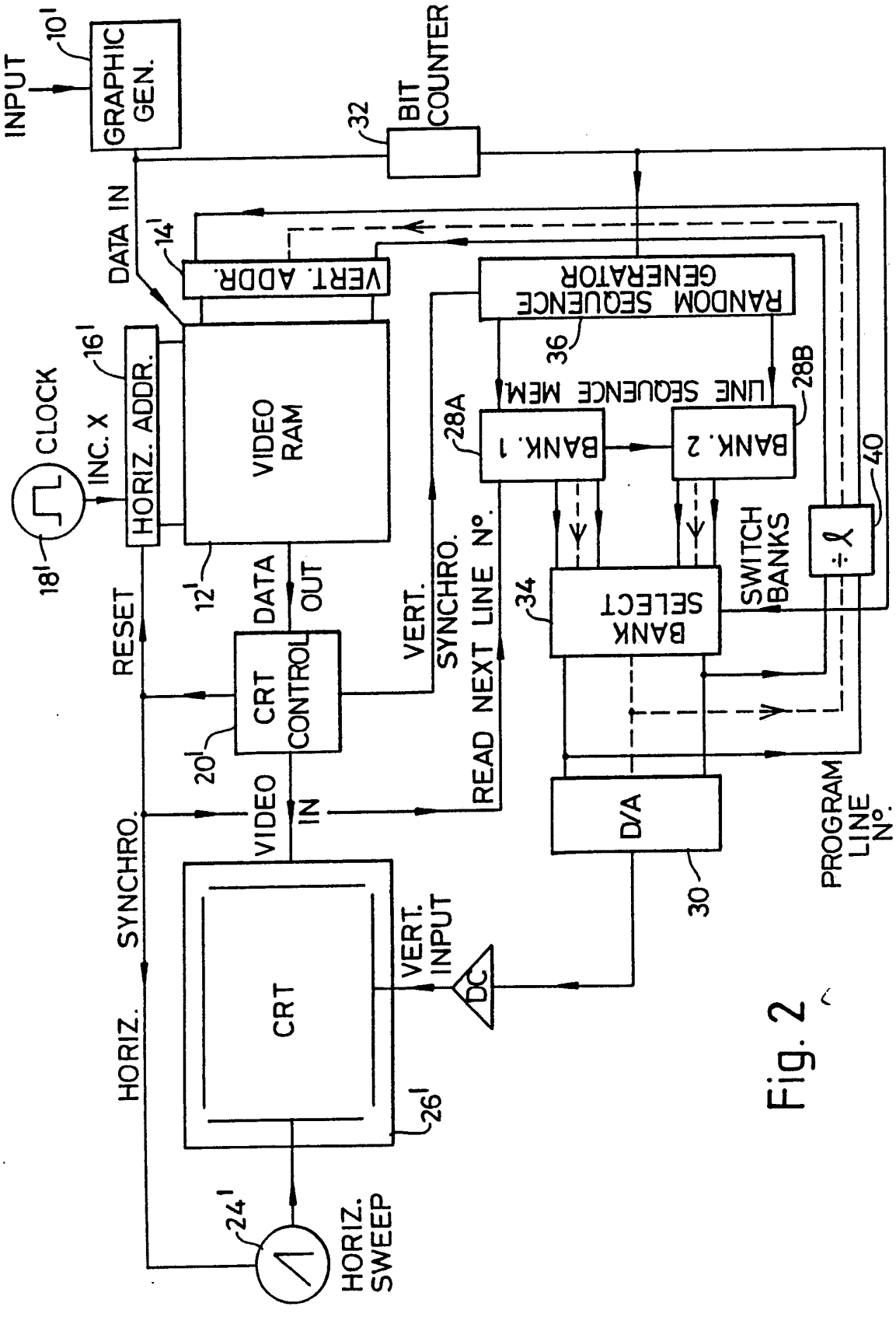

INPUT
10'
GRAPHIC GEN.
BIT COUNTER
32
DATA IN
14'
VERT. ADDR.
RANDOM SEQUENCE GENERATOR
36
LINE SEQUENCE MEM
28B
BANK. 1
BANK. 2
28A
16'
HORIZ. ADDR.
INC. X
CLOCK
18'
VIDEO RAM
12'
DATA OUT
RESET
CRT CONTROL
20'
VERT. SYNCHRO.
READ NEXT LINE N°.
34
BANK SELECT
SWITCH BANKS
÷ 2
40
VIDEO IN
SYNCHRO.
HORIZ.
D/A
30
PROGRAM LINE N°.
CRT
VERT. INPUT
DC
26'
24'
HORIZ. SWEEP

Fig. 2

INTERNATIONAL SEARCH REPORT

International Application No PCT/GB 90/00036

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) [6]

According to International Patent Classification (IPC) or to both National Classification and IPC

IPC[5]: G 09 G 1/16

II. FIELDS SEARCHED

Minimum Documentation Searched [7]

Classification System	Classification Symbols
IPC[5]	G 09 G

Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched [8]

III. DOCUMENTS CONSIDERED TO BE RELEVANT [9]

Category *	Citation of Document, [11] with indication, where appropriate, of the relevant passages [12]	Relevant to Claim No. [13]
X	US, A, 4669117 (W. VAN ECK) 26 May 1987 see figure 2; column 3, lines 2-31; column 4, lines 19-34; column 4, line 60 - column 5, line 25; abstract	1,2,4
Y	--	5-7
Y	WO, A, 8201955 (NCR CO.) 10 June 1982 see figures 1A,1C; page 4, lines 22-30	5-7
	--	
A	US, A, 4566002 (MIVRA et al.) 21 January 1986 see figures 4-6; column 5, line 57 - column 6, line 60	8,9
	--------	

* Special categories of cited documents: [10]

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

IV. CERTIFICATION

Date of the Actual Completion of the International Search	Date of Mailing of this International Search Report
22nd May 1990	27. 06. 90
International Searching Authority	**Signature of Authorized Officer**
EUROPEAN PATENT OFFICE	M. Peis / M. PEIS

ANNEX TO THE INTERNATIONAL SEARCH REPORT ON INTERNATIONAL PATENT APPLICATION NO. GB 9000036 SA 33878

This annex lists the patent family members relating to the patent documents cited in the above-mentioned international search report. The members are as contained in the European Patent Office EDP file on 18/06/90
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US-A- 4669117	26-05-87	NL-A- 8401989	16-01-86
		CA-A- 1229931	01-12-87
		EP-A- 0168861	22-01-86
		JP-A- 61092086	10-05-86
WO-A- 8201955	10-06-82	US-A- 4352100	28-09-82
		EP-A- 0067172	22-12-82
US-A- 4566002	21-01-86	JP-A- 55130582	09-10-80
		JP-A- 55147787	17-11-80
		JP-A- 55147788	17-11-80