PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H03M 7/30, H04N 7/30, 7/32, H04L 9/00 | A1

(11) International Publication Number: WO 00/25429

(43) International Publication Date: 4 May 2000 (04.05.00)

(21) International Application Number: PCT/AU99/00913

(22) International Filing Date: 21 October 1999 (21.10.99)

(30) Priority Data:

PP 6660	22 October 1998 (22.10.98)	AU
PP 9781	16 April 1999 (16.04.99)	AU
PQ 3360	12 October 1999 (12.10.99)	AU

(71)(72) Applicant and Inventor: ORME, Gregory, Michael [AU/AU]; 2/58 King Street, Annerley, QLD 4103 (AU).

(74) Agent: GRIFFITH HACK; GPO Box 3125, Brisbane, QLD 4001 (AU).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: A METHOD OF COMPRESSING DATA AND COMPRESSIBLE DEVICES

(57) Abstract

A method of compressing data including ordering a first package of data into a plurality of groups of data comprising a plurality of characters, performing a mathematical operation on each plurality of groups to produce a plurality of patterns of characters, identifying predetermined patterns of characters, storing the location of each predetermined pattern in memory and repeating this step, processing each mathematical operation performed with the location of stored predetermined patterns and further predetermined patterns to produce a second package of data of a reduced number of characters including the number and type of mathematical operations performed and, the location of stored patterns and after which mathematical operation they occurred, whereby the first package of data is retrievable from the second package of data.

A METHOD OF COMPRESSING DATA AND COMPRESSIBLE DEVICES

FIELD OF THE INVENTION

The present invention relates to transmission of any data over a transmission medium. In one example the present invention relates to transmission of video data over the internet.

BACKGROUND OF THE INVENTION

Typically the amount of video data which can be transmitted over a transmission line is limited by the bandwidth of the transmission line and the amount of other data which is being transmitted at the same time. Accordingly to reduce the amount of data which is being transmitted it is common to compress the data so that the bandwidth required for its transmission is reduced.

The problem associated with compression of data is that it can result in loss of information or distortion.

Another example is in the transmission of music where data representing the music is compressed and transmitted with a certain redundancy allowable because information which is lost during transmission does not overly affect the quality of the music which is received and audible to a persons ear.

Typically much of the data which is transmitted is digitised. Accordingly audio and video data is transmitted by firstly converting the data into a binary form, that is a series of zeros and ones, data is then transmitted as a sequence of binary numbers and at the receiver is reconstituted or demodulated and processed back into a form closely resembling its original form prior to transmission.

At present the transmission of video data is achieved by first representing each icon in a picture by a binary number and transmitting each of the binary numbers forming the picture as a continuous stream of binary numbers.

Accordingly if millions and millions of icons are required to form a picture a consequently large stream of binary numbers are required to be transmitted to transmit the image represented by the combination of all the icons.

Even with conventional compression techniques a considerable amount of time, on an electronic scale is required to transmit video data and accordingly this results in a moving picture which appears to be discontinuous, because the time between transmissions is able to be picked up by the human eye.

The present invention provides an alternative method of compressing data, including video data, which is aimed at improving the rate at which data can be transmitted and the amount of data which may be transmitted in a unit of time.

SUMMARY OF THE INVENTION

According to the present invention there is provided a method of compressing data for transmission over a transmission medium, including the steps of providing a first package of data, calculating the binary number representative of the package of data, processing the binary number using a mathematical equation to minimise the number of characters by which the binary number may be presented and converting the minimised number to a binary form for transmission over a transmission medium.

It is preferred that the method includes the step of storing the first package of data and processing the first package of data to produce a single binary number representative of the first package, wherein the single binary number is the binary number.

It is preferred that the method includes providing a first package of video data which is representative of a two-dimensional or three-dimensional image at a first unit of time.

The method preferably also includes the step of presenting the package of video data as an array in a first memory, and processing the data stored in the array to a sequential binary number.

It is preferred that the method includes transmitting the converted minimised number over a transmission medium, receiving the minimised number at a receiver, processing the received minimised number to convert the minimised number to the binary number representative of the package of data and processing the binary number to produce the first package of data in memory for display on a display means.

It is preferred that the equation splits the binary number into first and second components which when multiplied together substantially equal the binary number.

It is preferred that the method includes the step of determining the number of icons forming an image of transmission as video data, giving each icon a value zero or one, determining the binary number representing the value of all of the icons when expressed in a predetermined sequential manner and storing the binary number in memory.

It is preferred that the binary number is square rooted to the nth power until a number less than a predetermined number is achieved.

It is preferred that the predetermined number is less than 10 but greater than 1.

The video data may include redundant data which is predetermined.

The redundant data may form part of an image which is not viewed.

The redundant data may be chosen to produce a binary number which is easily able to be minimised in size in a manner previously described.

The video image to be transmitted may be divided into a plurality of areas with each area having a predetermined number of icons.

Each area may be processed to identify the number of icons and to form a binary number representing the icons of that area.

Each binary number of each area may be minimised to create a minimised number and each minimised number may be transmitted as part of the package of data.

It is preferred that the binary number is expressed as an integer to a base determined by the number of characters required to represent the binary number.

It is preferred that the binary number is processed by taking the log of the binary number to arrive at a number where X log Y equals the binary number where X is as close in value to Y as possible (X-Y = a minimum).

According to another aspect of the present invention a system is provided for transmitting a moving picture including the steps of dividing an image at a first time into a first plurality of portions each portion having an associated priority for transmission with respect to another portion, storing each of the first portions making up the image at the first time, transmitting to a receiver each of the portions making up the image at the first time, dividing the image at a second time into a second plurality of portions having an associated priority for transmission with respect to another portion, storing each of the second plurality of portions making up the image at the second time, transmitting the second plurality of portions having a priority above a predetermined value and repeating the above steps for succeeding times within a predetermined time interval.

It is preferred that the associated priority is determined based on the clarity of each portion.

The clearer portions preferably are given a higher associated priority.

It is preferred that portions of the image determined to be most important for viewing are given the higher associated priority over other portions.

It is preferred that darker portions are given lower associated priority.

It is preferred that rapidly changing portions and hard to see portions are given low associated priority.

Preferably if fine detail of an image is not important portions covering the fine detail are given an associated low priority.

It is preferred that the associated priority is based on a scale of one to ten.

It is preferred that the system includes a receiver for receiving transmitted portions.

It is further preferred that the system includes a display means for displaying the portions which have been transmitted.

It is preferred that the system includes receiving and storing low priority portions and displaying the same low priority portions until those portions are transmitted to the receiver with an increased associated priority above a predetermined priority value.

It is preferred that the portions making up the image at any particular time are compressed in accordance with any one of the methods previously described.

The present invention according to another aspect includes a processor for monitoring an image, the processor including a dividing means for dividing video data representing an image at a particular time into a plurality of portions which are segregated based on the importance of one portion with respect to another portion, assigning each portion a priority value according to its importance and storing all of the portions making up the image at a particular time in a first memory location, retrieving those portions from the first memory location which have an associated priority above a predetermined value and transmitting those retrieved portions to a second memory location from which those portions can be transmitted to a destination for display on a display means.

It is preferred that the method of determining the priority of each portion is based on one of the preferred options previously described in relation to the system for transmission of a moving picture.

According to another aspect of the present invention there is provided a method of compressing data including the steps of providing a first package of data, ordering the package into a plurality of groups of data comprising a plurality of numbers, performing a mathematical operation on each group to produce a plurality of patterns of numbers, identifying predetermined patterns of numbers from the plurality of patterns of numbers, storing the location of each predetermined pattern of numbers in memory, performing a further mathematical operation on the plurality of patterns of numbers to produce a further plurality of patterns of numbers, identifying further predetermined patterns of numbers from the further plurality of patterns of numbers, storing the location of each further predetermined pattern of numbers in memory and producing a second package of data including the location of stored predetermined patterns of numbers and further predetermined patterns of numbers and the mathematical operations and the order in which they occurred.

Preferably the method includes the step of representing each predetermined pattern by a symbol of reduced number of characters.

The method may include the step of removing each predetermined pattern of numbers from the plurality of patterns of numbers and storing each predetermined pattern of numbers as a symbol with an associated address and associated number representing the number of mathematical operations that occurred prior to the predetermined pattern of numbers being removed.

Preferably the method includes the step of storing the predetermined pattern of numbers that are produced after each mathematical operation in a look-up table. The method may include the step of providing a storage array for storing different types of predetermined patterns produced over a predetermined period of mathematical operations.

Preferably the method includes the step of storing the location of each predetermined pattern in the plurality of patterns of numbers each time it occurs after a mathematical operation.

The mathematical operation preferably includes the step of subtracting a predetermined number from each group of numbers.

Alternatively the mathematical operation includes the step of dividing a predetermined number into group of numbers.

The mathematical operation includes the step of comparing each group of numbers with a predetermined number and producing a number that is the difference.

The mathematical operation may include the step of removing a predetermined pattern of numbers within each group of numbers.

Preferably the further mathematical operation includes the step of sorting each group of numbers after predetermined patterns of numbers have been stored, the sorting being in accordance with a predetermined criterion.

The method preferably includes the step of shuffling the plurality of groups of numbers to produce predetermined patterns of numbers.

The further mathematical operation may include the step of shuffling numbers within the plurality of groups of numbers to produce predetermined patterns of numbers.

The package of data is preferably stored as a sequence of numbers in memory and after each mathematical operation numbers are reorganised in accordance with a predetermined transformation.

The package of data may be stored as a sequence of numbers in memory and after each mathematical operation numbers and symbols may be reorganised in accordance with a predetermined transformation.

The method preferably includes producing a new package of data including data regarding each mathematical operation required to reverse the sequence of steps and produce the first package of data.

The predetermined transformation may include regrouping numbers in accordance with a specific sequence of locations.

The transformation may include the step of grouping numbers at even number locations together and numbers at odd number locations together.

The transformation may include grouping numbers less than a predetermined number together and other numbers greater than the predetermined number together.

According to another aspect of the present invention there is provided a method of compressing data including the steps of providing a first package of data, ordering the package of data into a plurality of groups of data comprising a plurality of characters, performing a mathematical operation on each plurality of groups to produce a plurality of patterns of characters, identifying predetermined patterns of characters from the plurality of patterns of characters, storing the location of each predetermined pattern of characters in memory, performing a further mathematical operation on the plurality of patterns of characters to produce a further plurality of patterns of characters, identifying further predetermined patterns of characters from the further plurality of patterns of characters, storing the location of each further predetermined pattern of characters in memory, processing each mathematical operation performed with the location of stored predetermined patterns and further predetermined patterns and producing a second package of data of a reduced number of characters which second package of data includes the number and type of mathematical operations performed, the location of stored predetermined patterns and further predetermined patterns and after which mathematical operation they occurred, whereby the first package of data is retrievable from the second package of data.

According to another aspect of the present invention there is provided an apparatus for compressing data including an ordering means for ordering a package of data into a plurality of groups of data comprising a plurality of numbers, a mathematical operation means for performing a mathematical operation on each group to produce a plurality of patterns of numbers, a comparator for identifying predetermined patterns of numbers from the plurality of patterns of numbers, memory for storing the location of each predetermined pattern of numbers in memory, wherein the mathematical operation means is adapted to conduct a plurality of mathematical operations on the plurality of patterns of numbers to produce further pluralities of patterns of numbers and the comparator is adapted to identify further predetermined patterns of numbers from the further plurality of patterns of numbers and a processor is adapted to store the location of each further predetermined pattern of numbers in memory and produce a second package of data including the location of each stored predetermined pattern of numbers and further predetermined pattern of numbers and data relating to the mathematical operations and the sequence in which they occurred.

According to another aspect of the present invention there is provided a method of encrypting data including the steps of providing a first package of data, ordering the package of data into a plurality of groups of data comprising a plurality of numbers, performing a mathematical operation on each group of data to produce a plurality of patterns of numbers, identifying predetermined patterns of numbers from the plurality of patterns of numbers and storing the location of each predetermined pattern of numbers in memory, performing a further mathematical operation on the plurality of patterns of numbers to produce a further plurality of patterns of numbers, identifying further predetermined patterns of numbers from the further plurality of patterns of numbers, storing the location of each further predetermined pattern of numbers in memory and producing a second package of data including the location of each stored predetermined pattern of numbers and further predetermined pattern of numbers, data relating to each mathematical operation and the sequence in which each mathematical operation occurred.

It is preferred that the encryption method includes any one of the preferred method steps associated with the method of compressing data.

A preferred embodiment of the present invention will now be described by way of example only.

The preferred embodiment of the present invention will be described in relation to graphics data.

Assuming that it is desired to transmit a picture over the internet, the picture can be scanned by a scanning device which reduces the picture to a digital equivalent consisting of a series of zeros and ones.

The picture is thus transformed into a series of binary digits which represent graphics data.

Because the picture is two-dimensional, if it is assumed that icons represent the colour of the image at each point on the picture, the picture can be considered an array of icons.

Accordingly each of these icons is represented by a binary code which is stored in memory when the picture is scanned by a scanning device.

It follows therefore that the stored picture is represented by an array of binary numbers each at a different memory location or alternatively the array of binary numbers can be written as a continuous stream of binary numbers in a memory storage device.

In order to transmit the video data representing the picture to a computer terminal somewhere on the internet the video data must be modulated so that it can be transmitted down a communication line such as a hardware transmission line to the ultimate receiver. At the receiver the video data is demodulated as it is received and can then be displayed or stored as required.

As part of the transmission process the binary number for each icon is transmitted separately over the transmission line. Consequently if there is 100 million icons making up the picture then 100 million binary numbers must be transmitted each representing a particular icon.

The time taken to transmit each of the binary numbers representing each of the icons is therefore at least 100 multiplied by how many characters make up each binary number multiplied by the time it takes to transmit each binary number separately. Furthermore additional time is required in the modulation process and in other data which must be transmitted at the same time in order to ensure the integrity of the transmitted data.

To reduce the amount of time required to transmit each of the binary numbers referred to above it is proposed that a compression procedure be introduced in order to reduce the amount of data which needs to be transmitted in order to allow the picture to be reconstituted at the receiver end of the transmission line.

As part of the compression procedure the picture which is being transmitted must be analysed to determine a single binary which represents it. This step can be achieved quite easily because when the picture is scanned by a scanning device and is thus being digitised, the picture is then stored as a sequence of binary numbers. Therefore zeros or ones, which when placed sequentially one after the other can be considered a single very large binary number or possibly a series of binary numbers with each binary number representing a line of icons in the overall array making up the picture.

Assuming that a single binary number is to be used to represent the picture, this binary number can be converted to a more manageable number mathematically by changing the base, for example to base 10. In the process of converting the binary number to base 10 there may be a remainder portion which when subtracted or added to the rest of the number which has been converted to base 10 equals the very large binary number which represents the picture.

Having converted the very large binary number to base 10 a minimisation step can be introduced using a mathematical formula which has the sole purpose of reducing the number of characters required to represent the numerical value of the very large number.

Thus as part of the step of analysing the picture individual portions of the picture can be stored in different memory locations with each portion having a designated priority value or clarity value. Thus portions of the image which are stored with a high level of clarity or priority correspond to the parts of the image which must be transmitted before others having a lower priority. Furthermore if it is necessary only to view clearer parts of the picture then the portions of the picture having the higher priority value can be transmitted and the others can be disregarded altogether.

In one embodiment the amount of data sent by the above procedure could be reduced by not sending the parts of the image less noticed by the viewer who is receiving the data at the end of a communication.

As an example, a moving object in a video might be harder for a viewer to see its detail clearly. In this case moving objects might have some detail removed or data reduced in them in various ways as this loss of detail will be less noticed and can allow more detail to be sent of stationary and slow moving objects.

In another example, the eye might not notice as much detail in a part that is soon to be covered by a moving part of the image, and also might not notice as much in an area recently exposed by a moving part having left it. In a video of a walking man for example, the eye might not see details on the moving legs well, and may not see clearly the areas which the legs have just exposed, and where they will shortly obscure. Again this detail removed can allow the sending of more detail in areas where moving objects are not revealing and obscuring detail, without increasing the amount of data sent per second overall.

Darker coloured areas might not be as easily discernible, as well as areas where there is little contrast or colour change. For example, in a scene of a walking man, we might not see clearly details in his shadow, or in areas of a lawn where the colour or shade differences are slight. In this case one might remove more detail so as to send more detail where colours and shades change more rapidly such as the edge of the lawn and sidewalk, or where the edge of the man's face contrasts against the sky or against his hair or eyebrows.

Some smaller details when next to certain other, perhaps larger or more noticeable areas in some way, may be deleted or reduced in detail without the viewer noticing much difference. The saved information may again be used to transmit more detail in other areas.

Some colours may be preferentially treated for more detail as for example, fleshy tones, which would contain more facial details, which are preferable for the viewer. On the other hand sky blue colours might be sent with less detail. Of course, any of these and other parameters can be adjusted as desired for certain effects or special subjects, such as videos that contain more nature shots or more moving parts. Programs might be able to analyse video and by applying different amounts of these and other changes be able to optimise the amount of detail sent.

In some variations for example, faces might be detected and their details sent more, as viewers often put a high value on facial expressions, This might be done for example by using make up of a colour detected by the camera and devices used, all of which are claimed here. Contact lenses of a colour may also be worn or a hair dye or rinse to give colours the camera and devices detect to transmit with greater detail.

To facilitate this transmission one might break up an image into for example 3 transmissions that blend into each other when superimposed on each other.

One might have a low detail image where parts are dark, of low contrast and colour changes, and of moving objects and of parts recently revealed or about to be obscured by moving objects.

The middle image would be of intermediate details, and the high detail image of stationary sections with sudden changes of colour and shading. Each might be sent separately and reassembled into an overlay of the 3 video feeds by the receiver. The total amount of data is about the same as sending one image, but sending 3 like this would improve picture quality while increasing transmission speed.

Examples will now be described of different ways of implementing a system for transmitting selected parts of a picture.

According to one example it is considered that still frames are sent, say twenty frames per second. That is, in this case there would be twenty still photos sent each second, which when viewed in sequence give the appearance of motion.

In a given still frame there are many details, some more and less important to the observer to appreciate the movie. For example, it may be more important for the viewer to see facial expressions than the exact pattern of blades of grass in a lawn.

Consider then a scene of a man walking across a lawn. There are details such as lawn, flowerbeds, concrete pathways, and tree branches swaying in the breeze.

As examples, various features of this scene are more important to the observers than others. These examples are:

1. Sudden changes in colour and/or brightness may be more important to all observer than smaller changes.
2. Smaller details may not be as noticeable when close to large details.
3. Details on moving objects may not be as visible as details on stationary objects.
4. Some colours or brightness may be more important to the observer than others.

Imagine then in a frame of 800 by 600 pixels that there is some information that can be removed without significantly affecting the observer.

800 pixels wide
00000000000 600 pixels deep.
00000000000
00000000000

Initially one might mute some pixels, with X representing a muted pixel as shown below.

OXOXOXOXOXO...
XOXOXOXOXO
OXMOXOXOX0

If one now viewed the whole frame, much of the picture could still be seen even with the muted pixels. The unmuted pixels remaining are here called reference pixels. Each reference pixel has a value of red, green, and blue say from 0 as dark, to 127 as maximum brightness. By various values of red, green and blue most colours can be represented.

Each reference pixel is compared to the reference pixels closest to it, and some of course will be similar in colour to its neighbours and some will be quite different. If neighbouring pixels are similar enough in brightness or colour then the muted pixel can be left to be, for example, filled in by the receiver with a value perhaps mid way between the colours and/or brightness of the 2 reference pixels. If the reference pixels are too different then the pixel in between might be unmuted and sent as its original colour/brightness.

In areas where the colour/brightness are very similar some reference pixels may themselves be muted and restored as an average by the receiver. Some parts may look like illustration (a) below.

Illustration (a)

OXXXOXOOXXXX...
XXXOXXXXXOOO...
XXXXXXXOXOOOXXX...
OOXXXXXXXXXXXX...

In this example, there are many reference pixels that have been muted, and the receiver might restore them with a gradient of colour/brightness which could be in steps of changes, or a curve depending on the situation. For example, if 2 reference pixels are separated by 5 muted pixels, and one is black (Red 0, Green O,Blue 0) and the other is another colour (Red 127, Green 100, Blue 20) each of the muted pixels may be restored as having a colour 20% of the difference between the 2 pixels as shown in Illustration (b).

Illustration (b)

...OXXXXXO...

The first X might have a value of Red of 1/5 of 127 say 25, the next with a value of 50, then 75, 100, and 127 is the reference pixel. The Green values might be 20,40,60,80, and the Blue values 4,8,12,16. Each X would be filled in in this way.

The whole frame has much information removed, but the receiver may notice little difference.

In some sections there may be groupings where the reference pixels are denser than in other sections. Where a grouping of reference pixels is small and near a large grouping then it may be desirable to remove that grouping as such small details may not be as noticeable to the viewer as shown in Illustration (c).

Illustration (c)

OOOXXXXXXXOOOOOXXXXX...

OOXXXXXOOOOOOOXXXXX...

OXXXXOOOOOOOXXXXXXX...

XXXXXXXXXXXXXXXXXXX...

In this case the small grouping of O's in the upper left corner might be replaced by X's as it may be too near a large grouping of O's to be noticeable by the viewer.

In other cases more reference pixels may be left if their colouring is considered important to a scene. For example, flesh tones may be left in more than sky blue tones as the flesh tones may be conveying a higher priority detail such as facial expressions.

In the case of moving objects, it is often more difficult to see details on them than on stationary objects. A simple example might be if someone picked up this page and waved it around while trying to read it. Only when stationary would these words be easy to read, and so if a moving page was being filmed it might not be necessary to broadcast many details that could not be seen anyway.

The example here is to compare frame by frame. Say then we are looking at a movie of a man walking across a lawn with tree branches waving in the background, but everything else is stationary. We might find it difficult to see details on the trousers of the man, and also perhaps leaves on the moving branches. One is also unlikely to see details in an area just before it is obscured by a moving trouser leg, and one might not also notice details just revealed by a trouser leg.

Comparing then 3 frames in such a scene as shown in Illustration (d); Frame 1 shows a moving trouser leg in different places in frames 2 and 3. Frame 1 has details in it that will be obscured by a trouser leg in frame 2, and also has details obscured by the leg that will be revealed in Frame 2. These details may not be considered as important as details of stationary objects. Odd frames in the film are then compared, such as frame 1,3,5,7,...

Frames 2,4,6,8,... are muted in this example.

Illustration (d)

Frame 1	Frame 2	Frame 3
0000000	XXXXXXX	000000000
000000	XXXXXXXX 00000000	
0000000	XXXXXX	00000000
0000000	XXXXXXXXX 0000000	

Frames are then compared with each corresponding pixel, for example each pixel in the upper left hand corner in frames 1,2, and 3. If this pixel in Frames 1 and 3 were sufficiently different in colour/brightness then it might be assumed that this difference was due to movement in the film, or some change equally suitable for our purpose. In this case then the pixel would remain muted and would be restored by the observer as say mid way between the colour/brightness values of that pixel in Frames 1 and 3. In some cases more frames may be skipped for the given corresponding pixel. For example, there may be regular change of a given pixel between frames 2 to 8 that each value of this pixel might be muted then restored according to a formula in frames 3,4,5,6, and 7

In the case where a pixel of a stationary object did not change substantially over say 10 frames, it may be desirable to mute that pixel in frames 2 to 8, so the receiver replaces a gradient of that pixel in those frames. If the pixel did not change at all then the receiver would put a pixel of the same colour/brightness as in frames 1 and 8, in frames 2 to 8.

In the case where there were groupings of reference pixels so that some describe movements of small objects close to large ones, then all those pixels may be muted as the larger movement may be more noticeable to the observer. As some objects move they may become a colour/brightness that was preferential, such as skin tones, and so more details may be retained when they are in this range.

In cases where a film has been processed in this way it may be desirable to adjust the values of the remaining reference pixels so they do not stand out. An option is to avoid situation where these pixels are joins between straight line changes of colour brightness so they may be altered and the gradients changed to give smother nonlinear changes. This could also be processed by the receiver. In some cases the muted pixels could be replaced by specialised hardware such as in a 3dfx card, according to various preferences

In an additional case, one might separate information according to how often it changed. For example, if there were pixels in Frame 1 that did not change until frame 5 then a frame composed of those pixels might be removed from frame 1, and transmitted separately to be played along with frame 5. The remaining pixels of frame 1 might contain some that did not change until frame 3, and those pixels could be removed and made into a separate frame to be played along with frame 3. In this way a given frame "x" could be in fact many superimposed frames blended together, and the effect may be to reduce the amount of information sent.

There are many other criteria in which some pixels could be muted to be restored by the receiver, all of which are claimed.

In the case of the making of graphics such as for example games, it may be desirable to draw so that for example when things move there is less detail to put on the screen. For example, when a game character moves the devices may transmit less pixels to be restored to a picture for the observer than when the game character is stationary, with the program filling in the spaces between pixels again with gradients of colour/brightness. A sword wielded by the character might require less pixels to be transmitted of the sword, where the sword just was, and where the sword will shortly be. When the sword was stationary however, more pixels would be sent of its details.

In some variations an object that comes closer to the observer may require the transmission of more pixels than when it is far away. Such might be calculated according to such criteria as distance. When an object is at an angle to the viewer more pixels might be transmitted of the front edge of the object, than the back edge. Pixels might represent polygonal shapes rather than just squares as shown in Illustration (e).

Illustration (e)

OXXXO OXXO
XXXXX XXXXXX
OXXXO OXXXXXXXO

In each of these figures the X's might be filled in with appropriate shadings according to various criteria, by hardware and/or software.

Some of the devices in the transmission of the signal may be designed as follows. Once some of the pixels are muted, one essentially has parts of a line that need not be transmitted as shown in illustration (f).

Illustration (f)

OOOOXXXXX00XXXOOOOOOXXXXX

In illustration (f) the X's as muted pixels need not be transmitted. One example of the techniques is to reduce each series of X's to one X. This muted pixel might be transmitted as for example, completely black (Red 0 Green 0 Blue 0) and all other black pixels adjusted to dark grey so as not to be confused (such as Red 1 Green 1 Blue 1). The illustration (f) might then look like this:

OOOOXOOXOOOOOOX

and the number of X's transmitted separately at 5,3,5. The remaining O's and X's might then be further compressed by techniques to make the signal even smaller.

There are many criteria here for deciding which pixels are to be muted, and these can overlap in many ways. The decision to mute a given pixel might be made on the basis that it is, for example, part of a moving object, part of important details, and/or of preferential colours. In such cases one might apply each criteria to each pixel. Pixels that passed all criteria would obviously stay, and those that failed all would be muted. Those that passed some and failed others might be muted according to a weighting of how important each criteria is compared to others, and some that narrowly pass might be allotted in a probabilistic manner. That is if a criteria prevailed by 20% to mute some pixels then 70% (50+20) might be randomly muted preferentially to that criteria rather than that criteria totally dominating and all being muted. This would leave other pixels that might be otherwise totally left out information still represented in the film.

There can be additional information inserted into frames by giving some pixels values that are impossible. For example, there may be a limited number of colours so that a certain combination of red, green, and blue in a pixel is not one of those colours. That pixel can be a signal for the receiver for a particular effect. For example, that pixel in between 2 reference pixels may mean that a particular curve gradient such as a cycloidal, logarithmic, or circular, might be used that might pass through that pixel. In another variation if a pixel is left in that should have been removed by the various criteria then that pixel might be a signal.

Muting of pixels may be done with any criteria for any purpose. As an example, one might apply criteria to each of Red, Green, and Blue separately or mute on the basis of brightness separately from hue. In a frame of say red did not change sufficiently between reference pixels then those muted might have a gradient of red values between them. Some of those muted pixels might be sufficiently different in Green and Blue, and so those pixels would become reference pixels for Green and Blue but not red.

Characteristics of computers and receivers used to view the pictures may be used to determine greater detail. For example, 3dfx cards in computers often build up images from sketchier information for games. In similar ways, video could be encoded so such cards or other, even specially designed ones might add features desirable, perhaps making the video appear more as it did before encoding. Such devices might be used in other transmission paths, all of which are claimed, such as video encoded on a game cd so that the 3dfx card add details perhaps making them more life like or for other effects. This would be a way of improving transfer rates of video from cd, as could all of the ways discussed here.

Another related aspect of the present invention utilises the philosophy of looking for recurrent and desirable patterns of data that can be substituted for smaller patterns of symbols. Having identified these patterns the objective is to minimise the data in A reversible way so that fresh patterns are created for further compression. The data can then be mixed repeatedly for as long as is desired.

In the initial compression stage, arithmetic and sumlength encoding can be employed. Additionally the following original devices can be used.

As an example consider a series of numbers which one desires to compress:

985632814573289876

It is possible to consider this number as pairs of numbers in for example base 100. Thus the numbers can be grouped as

98 56 32 81 45 73 28 98 76.

Using an arithmetic subtraction step it is possible to subtract numbers to make the overall numbers smaller. Thus if the number 32 is subtracted from the previously identified stream of numbers the following numbers are produced

66 24 00 49 13 41 -4 66 44.

The number 32 would be identified in the arithmetic operation as the number subtracted and could be stored in a look-up table as the first mathematical operation.

From the resultant series of numbers 66 can be written in a smaller base than 98 and so on. By analysing each pair of numbers produced it is apparent that the number of 8's and 9's should be reduced so that overall the numbers can be represented by a smaller number of binary numbers. Furthermore smaller numbers like 1, 2 and 3 are more common.

Using this technique increases the probability of patterns occurring. One might be more likely to get a pattern like 1234 to occur, so a symbol for 1234 would be used more often.

Also a number such as 11111 is compressible as (5)1.

The next step is to define a set of transformations on the data. For example one might have a thousand numbers in a row one wishes to compress. By using various techniques, some already known, it is possible to replace some patterns with symbols and abbreviate other patterns.

According to another embodiment of the present invention instructions are provided to shuffle numbers, symbols, etc. For example the first, third, fifth, seventh.... may be reversed in order, while the second, fourth, sixth etc. numbers are placed at the end of the overall sequence of numbers thus leaving the odd numbers at the beginning of the sequence of numbers and the even numbers at the end of the sequence.

The result is a fresh set of numbers that can be put back in the original format by reversing the transformation which has occurred.

In the new order of numbers which are created one uses the compression techniques as before or others.

In the case of a hash table or library of patterns one applies a similar transformation to those as well.

One thus looks for patterns as before and compresses additionally one row as a library of patterns twice as large and if those patterns occur in the data, they can be denoted by symbols and the number of reorderings in which they occur. In some cases the number of reorderings might be omitted if the pattern has happened only once or its position is not ambiguous.

Another embodiment of the invention increases compression possibly at the cost of slower decompression. One can use these variations if particular shuffling does not give sufficient compression. One may omit that shuffling and go onto the next shuffling pattern. Say for example the minimum amount to be gained from a shuffling/compression cycle is 5%. On decompression this is reversible, as if on deshuffling/decompression it is found that the data does not increase in size by 5% it is assumed that cycle was omitted on compression and then one goes to the next deshuffling cycle.

In this way it is possible for example to try 10,000 shufflings of which only 500 were compressing enough. On decompression the program checks and discards 9,500 shufflings as it can tell from the small inflation (e.g. less than 5%) that the cycle was not used.

It is also possible to insert symbols to represent that shufflings should be ignored. Thus in a stream of characters if upon one shuffle particular patterns are not observed then a symbol can be either inserted in the stream of numbers or in another register to indicate that the shuffling step did not result in allocation of additional symbols representing patents.

According to another embodiment reordering could occur with the first, fourth, seventh, tenth numbers being moved, then the second, fifth, eighth, eleventh numbers being reversed and placed at the end of the stream of characters followed by the third, sixth, ninth, twelfth numbers. A comparator would then check the resultant stream of numbers for the occurrence of patterns which are stored in another location. Any patterns that occurred would be represented by a particular symbol which could then be inserted in the stream of numbers in place of the particular pattern of numbers.

Alternatively the pattern of numbers could be removed all together and the removal of such patterns would be recorded in a look-up table so that every time a reordering of numbers occurred the patterns resulting after that reordering would be recorded in the look-up table along with their position in the sequence of numbers and the number of the reordering that has taken place. For example whether the reordering was the first reordering or the ninety ninth reordering.

Using the techniques described symbols which represent patterns may themselves form patterns as they are mixed with the stream of numbers and they can thus be compressed as well. It is important that no ambiguous steps be allowed unless for a particular purpose, otherwise the operation may not be reversible to the original data.

As an example shuffling symbols may lead to a chance arrangement of symbols denoting a compression that did not occur. In this case some special symbols may be employed to break up the wrong indicators.

Messages may also be inserted in the body of the data. For example if the shuffling compression is done 1000 times then after 1000 numbers a marker might be inserted indicating the cycles or a number 1000 found somewhere is set out with symbols as the cycle number.

To give an example of how this system does not contradict the counting theorem, consider data of 1 million digits reduced to say 1000 digits. The theorem basically states one cannot describe 1 million different numbers using 1000 digits, but one might for example have applied anything from 100 to 100,000 cycles to get the compression. 100,000 cycles might only need adding the numbers 100,000 somewhere, six digits to indicate all these possibilities.

It follows therefore that the 1000 digits times 100,000 could describe one hundred million and more variations.

Of course the shuffling patterns can be of any kind and might be tailored to various data. The best may be a simple algorithm that is stored easily and is fully reversible for decoding.

These devices can also be used as a form of encryption since if one does not know the algorithm one cannot reconstruct the data.

Say for example even in a standard 1000 cycle decompression the original had 10,000 possible variations in any of those cycles. This alone could give rise to 1000 (to the power of 10) different possible algorithms to try for decompression. In another variation one might have a key that directs the shuffling each cycle. It might be for example a million to one possible shufflings, a person would have to sift through in just one cycle. In 1000 cycles the 1000 E 1 million combinations would have to be tried to find the original.

In another variation one might encrypt data with a key, and again repeat the process as many times as desired. The key might contain parameters for the shuffling algorithm as well as for decoding.

The encryption step might utilise for example available techniques such as DES or BLOWFISH.

To facilitate the compression it may be desirable to structure the number in other forms to give more patterns. For example one might structure the number as a 2D or 3D lattice, or a lattice or larger dimensions.

For example the same number may give rise to more patterns if a given digit is next to more numbers. The numbers

12345678902468101357

may have more patterns if written as

12345678

90246810

1357

or any other polyhedral shape eg tetrahedral lattice.

In the above reordered grouping of numbers occurring in the stream of numbers, there are three patterns 2,2; 4,4; and 6,6; which are not apparent in the normal layout. Structuring data this way may enable more patterns to be encoded and after each shuffling more patterns again may be found for compression.

The algorithms applied to change a pattern of numbers can themselves be stored in a dictionary or look up table. Thus frequently occurring pattens can be stored in the look up table, but also frequently useful algorithms to convert some patterns to be the same as others already in the look up table, can themselves be stored and denoted with a special symbol when they are to be used. Instead of finding patterns and listing them in a look up table, one can also list algorithms that create set patterns in a look up table. One can even list them according to Huffman or arithmetic coding, and all other systems. For example, the most commonly effective algorithm to make a pattern in the look up table would be given the smallest symbol to represent it and so on, through the ones that work more rarely being represented by larger symbols.

In one embodiment it is possible to search for a set sequence and compression patterns as one compresses, and if the numbers are represented in a 3D lattice, the resultant cube would change shape as patterns are changed. In order to retrieve the original number each of the shufflings or reorderings must be reversible.

Using the above techniques a stream of numbers may be compressed regardless of whether it is part of a multi-dimensional lattice. Similarly numbers which are normally completely distinct may be combined and compressed using the above techniques.

According to one embodiment patterns may also be defined in ways analogous to techniques in for example art programs. For example a sequence 98567 reduces to 43012 (-5) symbolises the numbers have each been reduced in size by 5, but one might imagine if each number was a unit of brightness that each has been darkened by 5 units. In another example 9753 altered to 4321 might be compared to the adjustment of contrast and brightness together. To reverse, the brightness changes back to 6543 then the contrast is increased to a change of two units instead of one to 9753.

It may be desirable to place a sequence 4321 with other patterns 1234 and this could be written as 1234R symbolising a reversal of the numbers. Alternatively 3412 might be written as 12R34 meaning the terms on both sides of the R are to be flipped or reversed. All other algorithms like this to adjust a pattern are also claimed.

According to another encryption device consider a body of text and where each letter appears, a number is placed in brackets beside it representing how far it is from the start of the document. For example if E was the letter in "now is the..." one would put "now is the(9)..." and so on for all letters. One then rewrites the text so as to list the positions of each letter. For example one lists the number where each A appears, then where each B appears and so on through the text including where the spaces and punctuation marks appear.

The encrypted data cannot be examined for word or letter frequency and from here may be encrypted in other ways.

According to another embodiment of the present invention the compression and encryption techniques described above may be used to combat computer viruses.

If information is sent from one point to another it can be compressed and/or encrypted by the techniques previously described.

It is essential in this operation either (1) the compressor/encryptor can operate so the receiver can use this information and/or (2) the decompressor/decryptor can retrieve this information to a useable state.

It is then possible to set out software and hardware in the following manner. One might have for example an operating system or program such as Windows or Unix that has many functions including copying, initialising programs, etc. These can be constructed so that one part of the operating system encrypts/compresses its instructions to another part, which may require the key to be decompressed/decrypted in order for these instructions to operate. This set up would ideally be performed so that one part of the program cannot acquire the means to decipher instructions by an undesirable route.

Assume therefore that the program sends a message encrypted to tell another part to erase some files. The receiving section either decrypts this message or asks for a code authorisation. A virus then could not make the copy section obey it because it would lack the code keys. Also an invading virus or program would have to be very large to crack codes, perhaps too large to escape unnoticed.

A program might be loaded on such a computer, so that it is activated by a code encryption from the manufacturer. As part of this process it receives keys to do certain operations with the permission of the operating system. If this program later becomes infected it may not be able to spread the infection because it lacks authorisation keys or the virus lacks the keys to gain access, even though it has infected part of the program.

Since a program is assumed to have keys an unauthorised instruction could be set as a signal to close down the system and raise the alarm. A file save might be encrypted with a key. If a virus attempted to change this file it would be requested to provide the key which it could not have. Such encryptions could also be used to prevent pirating of programs.

Codes could be protected from interception by trapdoor like techniques. Program A encrypts an instruction and sends it to program B. B encrypts the instruction again and sends it back to A. A removes its encryption and sends it to B which decrypts it and executes the instruction. At no time could an instruction be accessed uncoded nor could a key be intercepted.

A virus or such like attempting to access a code file would find it encrypted and would not have the key. If it did not get the key the codes would be useless to it.

On sending the instructions coded a program may additionally interrogate the sending section not just for codes but for coded responses indicating a correct installation or a correct pathway or authorisation. A program might have ten encrypted subsections to authorise an instruction. This might interrogate the process to ensure that 10 code authorisations are provided and that a virus has not inserted itself between the programs. Logs may be left of all operations.

The effect is that any unauthorised instruction would fail by not having the correct key, and because it would not have the key to define a correct path of decision making to an authorised input.

Systems like this would be extended to the Internet and other networks where two way communication maintains code authorisations.

In the case for example Word Macro viruses the original operating system and Word would vet each other so a macro could never get to the point of inserting itself. Any macros would also contain a certificate from the original program that the receiver would use to verify the macro was intact. This certificate would contain in it an authorised code and may also have the macro encrypted and only able to operate if correctly decrypted.

The text of the message could be encrypted as well so it could not be possible to extract the certificate and alter it.

According to another embodiment of the present invention it is possible to use the above techniques to put an encryption device in a dongle and have many files in the program recorded in an encrypted state. To operate the program sends the encrypted file to the dongle which decrypts it and send it back. In this way if the program was hacked and the dongle removed it would not be because the files remain encrypted.

According to a further embodiment when a program is first installed the operating system at another input may change all or part of the codes between the sections so if any virus has accessed some of the codes they would then be useless.

According to another embodiment section may agree to alter codes between themselves according to randomly generated criteria, so no external output can bread the codes.

Such devices can be used to any depth of programs and any exchange of any data in any form. For example each file in a program might be encrypted different to any other, so the program must know the different key to unlock each one. Also the file once decrypted may contain a code that instructs the program to find a key n the next file it uses and so on.

In some cases compression could involve regarding a binary file as a large number N and to find an algebraic expression that equals N, but takes up less room. The devices in this section for example enable one to find a more accurate logarithm of N and then use that to find an expression. Another application of this would be to find the factors of for example large numbers, sometimes for the purposes of breaking a code.

These techniques involve the use of a device which for convenience will be called an Add Logarithm. It is known for example how normal logarithms work, by adding the exponents together of numbers with the same base, it is equivalent to multiplying the numbers together.

For example 3^2 by 3^2 equals $3^{2+2} = 3^4$

One can also construct an "Add Log" for $3^2 + 3^2$ squared $= 18 = 3^{2+x}$, X in this case would be the Add Log of the second exponent.

In another example $2^3 + 3^4 = 2^3 + X$ where X is the Add Log that equals 3^4. Typically the add log would be in the same base, here base 2.

This device is useful in factorising large numbers. Consider a 1000 digit long number very difficult to factorise by today's technology. This number can be broken down into Add Logs to make the task easy. Say the number is 123896467... and so on for a 1000 digits. This could be written as $123 \times 10^{997} + 896 \times 10^{994} + 467 \times 10^{991}$ + and so on. One might find the log of the first term to base 10 and then the Add Log of the second term, a number which added to the log of the first term gives the log of first two terms added together.

One then finds the Add Log of the third term which when added to the log of the first two terms gives the log of the first three terms added and so on for all 1000 digits. Adding all these together gives the log of the whole number N but because the calculations have been restricted to small numbers higher accuracy is achieved.

Plotting these Add Logs will find that they fall on some form of curve, probably a form of log curve. Knowing the properties of this curve enables the construction of tables similar to normal logs or building programs and devices that calculate and utilise the Add Logs.

An example only of determining the curve is given. Consider one wishes to add $2^2 + 2^2 + 2^2 +\ldots$ and so on to infinity. It is clear that the Add Log of each term will be smaller than the one before. This reduction in size would fall on the Add Log curve. From this curve one could find the Add Log for numbers with different bases in a similar way to normal logs. For example $2^2 + 3^2 + 4^2 +\ldots.$ in an infinite sequence, can have the add logs of each number calculated by converting each term to base 10 or the whole can be converted to another base, say base 10.

Each term may be calculated in reference to the term before and perhaps not necessarily needing to add all the previous logs together.

This enables one to continue to work with smaller individual terms.

As an additional illustration assumes one wishes to find an accurate logarithm for a large number N. One might prepare for this by for example breaking up a smaller number M into a 1000 equal pieces and finding the Add Log for each 1. At this point one might determine the Add Log of each of those 1000 numbers to a higher degree of accuracy. One might then change each of these Add Logs to equal 1000 parts of N by adjusting each. The result is that each Add Log would be convertible to its corresponding Add Log for N by a formula.

Thus using the above techniques it is possible to have a method of compressing data by providing a large sequence of numbers, splitting the large group of numbers into groups of numbers as $AX^{Y} + BX^{Y-1} + CX^{Y-1} + CX^{Y-2} + DX^{Y-4} + \ldots$, where A, B, C, X, Y are whole numbers.

It is preferred that the expression above is able to be written as

$$AX^{Y + Z1 + Z1 + X3} + \ldots$$

Where Z1, Z2, Z3, ... is the Add Log for each term in the above expression.

It is preferred that each of the terms in the expression are plotted to form a curve so that values for Add Logs can be determined by tables constructed using a plurality of curves covering a range of values.

According to another embodiment of the present invention a method is provided for preventing unauthorised copying of CD's.

It is preferred that a CD is provided with a coating having pits burnt in it to encode information. Theoretically there can be no special encoding as one can always make a CD image of all the data. If however one had a variable coating on the CD the computer could determine if it was a copy or not. For example, part of the CD would be coated with a thin film that reading the disc slowly burns through. The program when installed tests the CD by attempting to read a blank part of the CD over and over. After a time the thin coating will burn through and reading this section will result in the program determining that the section has the special film and certify the CD as genuine.

If after repeated reading the signal does not change, the program may determine the CD is a copy and reject it.

Doping like this could be placed at any point on the CD so an image copy would probably put the section in the wrong place even if blank CD's like this were duplicated to pirate copies.

In another variation it may be possible to burn the standard coating so that extra laser light on that section later will punch a hole through completely, making a special coating unnecessary.

In another embodiment a CD might have a second coating in a particular section. This coating would have the property of being burnable by a standard CD laser, either from a single or multiple exposure.

Under the coating is a sequence of dots representing a code. At the beginning the CD cannot read this code as it is under the coating,

To read the CD the burner at first reads a pattern on the layer that will burn away. It must read this code to decrypt certain files, for example for installation. On reading these files the outer layer partially burns away, leaving another code underneath which decrypts other files.

To activate the desired part of the CD one might require that both parts are decrypted, and each time a tracker is used to represent a use of those files. When those layers are all used up the CD cannot be used anymore.

Such a process cannot be copied unless someone made the CD and then put a second layer on. Such a procedure would be much more difficult for a typical pirate.

According to another related aspect of the present invention there is provided a permanently sealed container having a flexible outer wall defining a partially evacuated internal chamber having a resiliently deformable member located therein.

It is preferred that the resiliently deformable member is foam.

Preferably the sealed container includes a fluid.

Preferably the resilient force of the deformable member in combination with the force applied by the pressure of fluid within the container is in equilibrium with atmospheric pressure applied to the flexible outer wall.

It is preferred that the flexible outer wall has an inner surface which surrounds and contacts the outer surface of the resiliently deformable member.

It is preferred that the combined pressure of the fluid within the container and the resiliently deformable member is sufficient to maintain the flexible outer wall in contact around the resiliently deformable member substantially without compressing the resiliently deformable member.

It is preferred that the flexible outer wall is in the form of a skin or membrane which is formed over the surface of the resiliently deformable member.

Preferably the sealed container includes a valve for entry or exit of fluid from the internal chamber.

It is preferred that the combined pressure of fluid within the chamber and the inherent resilience of the resiliently deformable prevents noticeable deformation of the resiliently deformable member by atmospheric pressure applied to the outer surface of the flexible outer wall.

It is preferred that the interior chamber includes a fluid in the form of air having a pressure to partially inflate the flexible outer wall.

It is preferred that the partial inflation of the flexible outer wall is sufficient to make the flexible outer wall cling to the outer surface of the resiliently deformable member.

According to the aspect of the invention outlined above compressive devices such as cushions may be made.

According to one example it is desirable sometimes to create a sealed container that can be made to a degree of flexibility.

An inflated beach ball for example feels hard to compress because the air pressure inside rapidly increases as it is squeezed.

If the beach ball is partially inflated it is still hard to squeeze beyond a point and only hard to expand as normal foam softness this tends to create a partial vacuum in the ball. In is obtained by air escaping from the foam.

The principle of this devices is to place two opposing forces so that when one is compressed the other seeks to expand.

As shown in Figure 1 a block A if moved to either side is pulled by the opposing spring to the centre.

In the example of a beach ball filled with foam a partial vacuum created inside makes it possible to compress the beach ball as it does not meet the resistance of air pressure immediately until the pressure builds above the outside air.

The ball thus feels somewhat soft as the foam compresses with resistance increasing as the foam tends to bounce back and the air pressure rises.

When the force is released the ball resumes its former shape defined by an equilibrium state of the foam and the partial vacuum and the sponge's resilience.

It is possible to adjust the softness of the device in many ways. For example it is possible to alter the vacuum inside or use different kinds of miniatures of sponge like or elastic material.

In an example of this use breast implants and other prosthetic devices would be able to be constructed with a more natural softness in this way.

In other examples one could adjust the characteristics of a car shock absorber by using two opposing forces in this way, perhaps a partial vacuum and a spring.

According to one variation of the present invention the resiliently deformable member is in the form of a spring or a plurality of rubber balls.

According to one aspect of the present invention there is provided a device for shock absorbing comprising a container having a deformable outer wall, a resiliently deformable means located within the container and compressible or expandable with or against the outer wall, the container also including a fluid having a predetermined pressure adapted to resist compression of the resiliently deformable member.

According to a related aspect of the present invention a method of encrypting data is provided.

Although there are numerous methods of encrypting data, invariably by calculating numerous possible permeatations of encrypted data it is possible to decrypt the encrypted data.

The present invention aims to provide an encryption method which is difficult if not impossible to decrypt without the use of the encryption method.

The present invention provides a method of encrypting data which in its preferred form utilises methods for compressing data.

According to the present invention there is provided a method of encrypting data, including the steps of representing the data as image data, processing the image data to produce a number representing the image data, processing the number to produce a mathematical expression which is equivalent to the number, whereby the mathematical expression is able to be converted back to the number and the number can be converted to the image data for encryption.

Preferably the method includes the step of converting the number into an algebraic expression $A^B + C^D + D^E + ..R = N$, where A, B, C, D, E, R are variables which may be real numbers, integers or other types of numbers.

The method includes the step of encoding each variable in the algebraic expression.

Preferably the method includes a plurality of encryption steps.

Preferably the method includes one or more additional steps of converting the algebraic expression into different algebraic expressions.

According to the preferred embodiment of this aspect of the present invention data compression techniques can be utilised in encryption devices. According to a preferred embodiment of the present invention any image or data can be encoded. To do so one reduces the data by various techniques which are outlined above and in prior patent application no. PP9781.

An example $A^B + C^D + D^E + F^G$ can represent a number which itself represents data.

It is then possible to apply an encoding step to the above formula.

Thus it is possible to write this expression as a ABCDEFG and apply various encodings, even those available already to these numbers and replace them in the formula. For example it would be possible to jumble the operands of the formula in some prearranged way or add false variables, etc. The fundamental principal behind the above technique is that the original message be it pure data or image data, can be represented as image data in an array of pixels.

Using the compression techniques described previously it is possible to represent the image data as a single number N.

Once the number N is compressed and the numbers A B C D E F G in some encoded form are transmitted to a destination, even if it was possible for someone to work out that there were numbers A B C D E F G it would be virtually impossible to work out the relationships between these numbers in order to find the number N and thus the image that it represents in a pixel array. This is because the numbers transmitted can be combined to produce so many different numbers and there is no clue as to what number is actually being looked for. Even if the number was accidentally decrypted its significance would not be evident because only the encryptor would know that it represents an image in a pixel array.

The above encryption technique could be used for numerous applications including bank files, classified transmission and any other traditional encryption application.

CLAIMS

1. A method of compressing data including the steps of providing a first package of data, ordering the package of data into a plurality of groups of data comprising a plurality of characters, performing a mathematical operation on each plurality of groups to produce a plurality of patterns of characters, identifying predetermined patterns of characters from the plurality of patterns of characters, storing the location of each predetermined pattern of characters in memory, performing a further mathematical operation on the plurality of patterns of characters to produce a further plurality of patterns of characters, identifying further predetermined patterns of characters from the further plurality of patterns of characters, storing the location of each further predetermined pattern of characters in memory, processing each mathematical operation performed with the location of stored predetermined patterns and further predetermined patterns and producing a second package of data of a reduced number of characters which second package of data includes the number and type of mathematical operations performed, the location of stored predetermined patterns and further predetermined patterns and after which mathematical operation they occurred, whereby the first package of data is retrievable from the second package of data.

2. The method as claimed in claim 1 wherein the first package of data is ordered into a plurality of groups of data comprising a plurality of numbers.

3. The method as claimed in claim 2 including the step of representing each predetermined pattern by a symbol of reduced number of characters.

4. The method as claimed in any one of the preceding claims including the step of removing each predetermined

pattern of numbers from the plurality of patterns of numbers and storing each predetermined pattern of numbers as a symbol with an associated address and associated number representing the number of mathematical operations that occurred prior to the predetermined pattern of numbers being removed.

5. The method as claimed in any one of claims 1 to 3 including the step of inserting a symbol representing a particular predetermined pattern in a group of data having a predetermined pattern of characters.

6. The apparatus as claimed in any one of the preceding claims wherein predetermined patterns of numbers are produced after each mathematical operation are stored in a look-up table whereby they can be retrieved in reverse order of entry into the look-up table.

7. The method as claimed in claim 6 wherein the mathematical operation includes the step of subtracting a predetermined number from each group of characters.

8. The method as claimed in claim 7 wherein the mathematical operation includes the step of comparing each group of numbers with a predetermined number and producing a number that is the difference.

9. The method as claimed in claim 8, wherein the further mathematical operation includes the step of sorting each group of numbers after predetermined patterns of numbers have been stored, the sorting being in accordance with predetermined criterion.

10. The method as claimed in any one of the preceding claims wherein the further mathematical operation includes shuffling groups of characters in accordance with a predetermined transformation.

11. The method as claimed in claim 1 wherein the mathematical operation includes a transformation step

whereby characters at predetermined positions are grouped together.

12. A method of encrypting data including the step of providing a package of data, performing a mathematical operation on the package of data to create groups of data comprising a plurality of patterns of characters, identifying predetermined patterns of characters from the plurality of patterns of characters, storing in memory the mathematical operation performed and the location of each predetermined pattern of characters, repeating the steps a predetermined number of times to produce an encrypted package of data.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU 99/00913

A.	**CLASSIFICATION OF SUBJECT MATTER**
Int Cl[6]:	H03M 7/30, H04N 7/30,7/32, H04L 9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
WHOLE IPC

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WPAT, IMAGE AND COMMUNICATION, COMPRESSION OR DECOMPRESSION,CODING OR DECODING, ENCRYPTION OR DECRYPTION, MATHEMATICAL OR ALGORITHM.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	BRUCE SCHNEIER "Applied Cryptography; Protocols, Algorithms, and Source Code in C" John Wiley and Sons Inc. US, 1994 (see in particular Part 3, pages 187-410).	12
P,X	US 5923376 (PULLEN et al.) 13 July 1999 (see the whole document)	1
P,A	The whole document.	2-11

[X] Further documents are listed in the continuation of Box C

[X] See patent family annex

* Special categories of cited documents:

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

"E" Earlier application or patent 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 when the document is taken alone

"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

Date of the actual completion of the international search	Date of mailing of the international search report
19 November 1999	-7 DEC 1999

Name and mailing address of the ISA/AU
AUSTRALIAN PATENT OFFICE
PO BOX 200
WODEN ACT 2606
AUSTRALIA
Facsimile No.: (02) 6285 3929

Authorized officer
ANDREA HADLEY
Telephone No.: (02) 6283 2222

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU 99/00913

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,A	US 5872597 (YAMAKAGE et al.)16 February 1999	1
A	EP 0806807 A2 (DAEWOO ELECTRONICS CO.,LTD)12 November 1997 (see the whole document)	1
A	US 5678043 (NG et al.) 14 October 1997 Column 3, line 6 - Column 16.	1-12
A	US 5499294 (FRIEDMAN) 12 March 1996 Column 4, line 19 - Column 8, line 25.	12

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/AU 99/00913

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian 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		Patent Family Member			
US	5923376	US	5867221	WO	9737495
EP	0806807	FI	961940	GB	2312993
		US	5874872		
US	5678043	US	5603022		