

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
13 February 2003 (13.02.2003)

PCT

(10) International Publication Number
WO 03/013142 A1

- (51) International Patent Classification: **H04N 7/26, 5/00** (74) Agent: **REES, Alexander, Ellison**; Urquhart-Dykes & Lord, 30 Welbeck Street, London W1G 8ER (GB).
- (21) International Application Number: PCT/GB01/05207
- (22) International Filing Date:
26 November 2001 (26.11.2001)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
0118352.4 27 July 2001 (27.07.2001) GB
- (71) Applicant (for all designated States except US): **AMINO HOLDINGS LIMITED** [GB/GB]; Longstanton House, Woodside, Longstanton, Cambridge (GB).
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): **GILBERT, Martyn** [GB/GB]; 41 St. Michaels, Longstanton, Cambridge CB4 5BZ (GB). **WANG, Keith** [GB/GB]; Amino Communications Limited, Longstanton House, Woodside, Longstanton, Cambridge (GB).
- (81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, 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, MZ, 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.
- (84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, 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, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).
- Published:**
— with international search report
- For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: DIGITAL IMAGE WATERMARKING

A

-1	-2	-1
0	0	0
1	2	1

B

-1	0	1
-2	0	2
-1	0	1

(57) Abstract: A method of digital watermarking in which a digital watermark is embodied into a first image and it is subsequently attempted to identify the digital watermark in a second digital image. The method including the following steps. Measuring intensity gradients at a number of selected points in the first image. Measuring intensity gradients at multiple points in the second image. Comparing the measured intensity gradients in the first and second images and identifying a point in the second image corresponding to each selected point in the first image based on the composition. Calculating the changes between the first and second images from the differences between the locations of the selected points in the first image and the corresponding points in the second image, and correcting for the calculated changes between the first and second images when attempting to identify the watermark in the second image.

WO 03/013142 A1

Digital Image Watermarking

This invention relates to a method and apparatus for watermarking digital images, particularly digital video images.

The advantages of producing images, and particularly video image signals, in digital form are well known. The use of digital signals allows a better quality image to be displayed and reduces the bandwidth required to transmit the signal.

However, despite the obvious advantages of supplying and distributing video images in digital form service providers have been reluctant to offer video services in digital form because of the ease with which unauthorised copies of digital video images can be produced and distributed.

The making and distribution of illicit copies of analogue video is intrinsically limited because the copying of analogue video signals results in degradation. As a result the image produced from a copy of an analogue video signal is of lower quality than the image produced by the original analogue video signal. Also, because analogue video signals must be mechanically recorded onto video tape the numbers of copies which can be made is limited unless a substantial investment in hardware is made.

Neither of these constraints restrict the illicit copying and distribution of digital video signals. Repeated generations of copies of digital video signals can be made without any image degradation and the copies can be easily recorded onto re-writeable CD's. As a result, not only are the video images produced by the illicit copies of just as good a quality as those produced by the original digital video signal but the number of copies which can be produced is greatly increased and the cost of the necessary copying requirement greatly reduced.

It has been attempted to devise technical means to prevent illicit copying of digital video signals. Most such approaches have relied on encrypting the stored or transmitted digital video data so that only authorised users can decrypt the digital video data and view the video image.

Unfortunately such techniques are of limited effectiveness because in order for the video image to be viewed it is necessary for it to be sent to a display device in a displayable or viewable form. The digital video data in this viewable form can be recorded and illicit copies made using any conventional digital video recording methodology and, if desired,

compression techniques even if the encryption of the encrypted digital video signal cannot be broken.

Thus, there is a problem that the illicit copying and reproduction of digital images and particularly digital video images cannot be prevented.

This invention was produced in an attempt to overcome this problem, at least in part.

In a first aspect, this invention provides a method of digital watermarking in which a digital watermark is embedded into a first digital image and it is subsequently attempted to identify the digital watermark in a second digital image, including the steps of:

- measuring intensity gradients at a number of selected points in the first image;
- measuring intensity gradients at multiple points in the second image;
- comparing the measured intensity gradients in the first and second images and identifying a point in the second image corresponding to each selected point in the first image based on the comparison;
- calculating the changes between the first and second images from the differences between the locations of the selected points in the first image and the corresponding points in the second image; and
- correcting for the calculated changes between the first and second images when attempting to identify the watermark in the second image.

In a second aspect this invention provides a method of digital watermarking in which an encoded digital signal is operated on by a decoding means to provide a displayable digital signal and the decoding means incorporates a digital watermark into the displayable digital signal.

Preferred embodiments of the invention will now be described by way of example only with reference to the accompanying diagrammatic figures, in which:

Figure 1A shows a first Sobel operator for use in a first embodiment of the invention; and

Figure 1B shows a second Sobel operator for use in the first embodiment of the invention.

The use of digital watermarks in digital images including digital video images is well known. A digital watermark is formed by data inserted into a digital image identifying the

image producer or issuer, the watermark data being uniquely identifiable and recoverable from the image data or copies thereof and not effecting the appearance of the image produced from the data.

The uses of digital watermarking are, unsurprisingly, similar to the function of paper watermarks of allowing the issuer or generator of the image to be identified.

Digital watermarking of digital images including digital video images can be used to validate the source of images or video and can also be used in various applications such as copy protection, fingerprinting, cost monitoring and data authentication.

In order for digital watermarking to be effective it must be both invisible and secure. Watermarking must be invisible to legitimate viewers of the image or video when this is displayed in the expected or normal manner. Further, the watermark must ideally be invisible or undetectable by unauthorised third parties making illicit copies because if they are able to detect the watermark they will usually be able to remove it or at least corrupt it sufficiently to prevent subsequent recovery and identification of the digital watermark.

The digital watermark should be secure and reliable so the embedded digital watermark can be reliably extracted from the digital image or video or copy thereof and be reliably and unambiguously identified.

Finally, the digital watermark must be robust in order to prevent it being removed either deliberately or unintentionally from the digital image or video.

Unintentional removal of the digital watermark can take place during conventional video processing and editing using techniques such as noise reduction which is commonly applied during video processing before encoding, for example, using MPEG, in order to achieve better compression. Where the presence of a digital watermark is known or suspected illicit copiers may also make deliberate attempts to remove the digital watermark in order either to conceal the fact that a copy is an illicit copy or to prevent identification of the source of the illicit copy. The source being the legitimate copy from which illicit copies have been derived or the part of the supply channel allowing such copying.

In this context removal of the digital watermark is used to refer to the digital watermark being corrupted or damaged to such a degree that it can no longer be reliably identified or information encoded into the digital watermark can no longer be extracted and is not intended to be limited to the total deletion of the digital watermark from the digital image

or video such that the digital image or video is returned to its condition before the digital watermark was applied.

Other forms of video processing which routinely occur and can result in unintentional removal of the digital watermark or which could be deliberately employed by illicit copiers in order to remove a digital watermark include filtering, reformatting and conversion and reconversion between the analog and digital domains.

The most straightforward and reliable digital watermarking techniques are correlation-based algorithms. In correlation techniques a key generated pseudo random pattern is added to either the video data or a transform of the video data as a digital watermark. In order to confirm the presence of the digital watermark the correlation between the video data or the appropriate transform thereof and a pseudo random pattern generated by the same key is calculated and the degree of correlation compared to a threshold. A high level of correlation confirms the presence of the watermark and a low level of correlation indicates the absence of the watermark.

In general, the more energy the digital watermark carries the more robust the watermark will be. Accordingly, a digital watermark should carry as much energy as possible without it being visible so that destruction of the watermark will cause the watermarked image or video image to lose its economic value because of the harm done to the overall appearance of the image.

For clarity and to avoid repetition this description of the invention will refer primarily to the application of the invention to digital video images. However, it should be understood that the invention can be similarly applied to digital watermarking of other forms of digital images and signals.

The two main problems in employing digital watermarks in digital video images are ensuring that the digital watermark can be reliably detected and recovered, that is, ensuring that the digital watermark is robust enough to resist accidental or deliberate removal, and concealing the digital watermark from illicit copiers who wish to remove or corrupt it.

In order to allow a digital watermark to be detected, for example by correlation, it is necessary for the location of the digital watermark in the image to be identified. However, there are a number of problems with determining the location of a digital watermark in an

image with sufficiently precise alignment for correlation or other techniques to identify the digital watermark.

The obvious approach of defining the pixel locations or image coordinates where the digital watermark is embedded in the original digital video image is not effective because conventional video processing and transmission can result in geometric transformation of the received or copied digital video image compared to the original digital video image. Further, it is extremely simple for illicit copiers to carry out geometric transforms of the digital video image in an attempt to remove or conceal digital watermarks and this can easily be done without having any significant impact on the appearance of the digital video image to viewers.

Possible geometric transforms include translation, scaling, rotation, skewing, tilting etc.

In order to allow a digital watermark to be recovered from a digital video image half which has been subjected to geometric transformation it is necessary to determine the net geometric transform which has occurred to the copy of the digital video image compared to the original digital video image. This net geometric transform can then be corrected for when the correlation technique to identify the digital watermark is carried out.

It will usually be most convenient and reliable to correct for the net geometric transform by applying a reverse of the net geometric transform to the digital video image copy to return it to its original form and then to carry out the correlation or other processing to identify the digital video watermark. The present description is based upon the use of this technique. However, in theory it would be equally possible to correct for the net geometric transform by altering the watermark information used for the correlation or other digital watermark identifying process.

It has been suggested that a grid or other arrangement of markers could be added to the digital video image so that the changes in the positions of the markers between the original digital video image and the copy digital video image can be used to determine what geometric transformation has occurred. However, such marker based systems are highly vulnerable to attacks on the markers themselves. In the spatial domain, markers added to a digital video signal are high frequency noise and like other forms of high frequency noise are vulnerable to removal by simple operations such as low pass filtering or digital to analogue followed by analogue to digital conversion.

In the present invention the fundamental characteristics of the digital video image itself are used to determine any changes such as geometric transforms that the digital image has suffered relative to the original image. The fundamental characteristics of the digital video image such as edges, shapes and texture cannot be changed inadvertently during transmission or processing of a video image or deliberately by illicit copiers without rendering the copy video valueless, because without them there is no video image.

In order to carry out alteration detection using the present invention an alteration detection algorithm using image intensity gradients is applied to the video image copy.

The gradients in the digital video image can be measured in a number of ways.

One preferred method is to measure the gradients in the digital video image using Sobel operators, such as those shown in Figures 1A and 1B, to determine the amount of change in intensity, or in other words the gradient, at a particular pixel location in a particular direction. The operator shown in Figure 1A detects vertical gradient G_y and the operator shown in Figure 1B detects horizontal gradient G_x . Sharp horizontal edges have high vertical gradients and low horizontal gradients whilst sharp vertical edges have high horizontal gradients and low vertical gradients. Diagonal edges have high gradients in both directions, while smoother areas have low gradients in both directions.

In a preferred embodiment of the invention the alteration detection is carried out as follows.

The source video image is divided into blocks, for example 32 x 32 pixel blocks. The blocks along the image boundaries are then excluded because some or all of the pixels in these blocks could be lost from the image either by conventional video processing or by deliberate attack. Some or all of the remaining blocks are then chosen. Where only some blocks are chosen they are preferably dispersed across the image in a grid or other predetermined geometric arrangement.

For each of the chosen blocks the gradients of each pixel within the blocks are calculated. The pixel with the greatest overall gradient, which is defined as the sum of the absolute values of G_x and G_y is found and is selected as the salient point within that block.

When the source video image is compared with a copy or target video image a search window in the copy video image is centered on the position in the copy video corresponding to the position of each selected salient point in the source image and a search

made for the pixel within the search window having the best match to the selected salient point. The pixel having the closest gradient values G_x and G_y to the values of the selected salient point within the corresponding search window is identified as being the pixel in the copy video image corresponding to the respective selected salient point in the source video image.

For each salient point this will provide a pair of coordinates $S(X_1, Y_1)$ in the source image and $I(X_2, Y_2)$ in the copy image. This tells us that the salient point (X_1, Y_1) in the source image is now at (X_2, Y_2) in the copy image. This correspondence is referred to as a calibration point. When this salient point matching has been carried out for all of the selected blocks there will be a list of pairs of coordinates forming a list of calibration points, $S(X_n, Y_n)$ and $I(X_n, Y_n)$. By comparing the differences in coordinates in the respective images of the pairs of coordinates making up each calibration point the exact changes or geometric transforms which have occurred between the source video image and the copy video image can be determined.

The size of the blocks of the source image, the number of the possible blocks used and the size of the search windows can be varied. Usually the search window should be larger than the blocks in order to minimize the possibility of the changes moving the salient point outside the window.

The simplest and most common change which is likely to be undergone by the digital video image is translation and scaling. Further, this translation and scaling is usually likely to be uniform so that the whole image is translated by the same factor A where $A=(A_x, A_y)$ and scaled horizontally and vertically by respective scaling factors B_x and B_y .

In this simplest case all of the list of correlation points should fit into a straight line such that the following equations are satisfied:

$$I(X_n)=A_x+B_xS(X_n)$$

$$I(Y_n)=A_y+B_yS(Y_n)$$

The values of A , B_x and B_y can be obtained easily by applying linear regression using the coordinate pairs in the correlation list. Once the values of A , B_x and B_y are known

the copied image can be translated back to its original position and scaled back to its original scale. The embedded watermark can then be recovered.

Other changes in the image can also be deduced, identified and reversed by a similar comparison of the list of calibration points coordinate pairs and suitable techniques to allow particular changes between the source image and the copy image can be easily produced by the skilled person. Accordingly, these will not be discussed in detail here.

The simple example given above assumes that changes to the image will be uniform. It is possible that changes to the image could be non-uniform so that different parts of image are altered by different forms of alteration or by alternations having different sets of parameters. In order to correct for non-uniform translation and scaling changes the above calculation of translation and scaling parameters must be carried out separately for different parts of the image so that suitable parameters can be obtained to allow the changes to be reversed for each part of the image which has undergone a different change. Similar calculations for different parts of the image must be carried out for other forms of nonuniform change.

The use of pixel gradients to allow image changes to be identified provides considerable advantages over the use of pixel intensities. Firstly, pixel gradients are more likely to be unique over a local area than pixel intensities. Also pixel intensity data is vulnerable to attacks such as slight grey level shifting, which will not affect gradient data. For 8-bit images for example, pixel intensities range from 0 to 255, while each gradient G_x or G_y in each direction can range from below -1000 to over +1000. Thus, the combination of G_x and G_y of a pixel has a much large range of possible values than the pixel intensity so that it is more likely to be unique over a local area. Further, in practice images more commonly include groups of pixels having the same or very similar intensities than groups of pixels having the same or very similar gradients.

One exception is extremely uniform edges and these are very rare in real world images. In order to deal with the rare event that an extremely uniform edge is present in the video image, the change detection process can exclude blocks including such uniform edges from consideration so that such blocks are not used to identify and select salient points.

Preferably the change detection process compares the overall gradient of the salient point identified and selected within each block to a threshold and excludes those blocks in

which the overall gradient is below the threshold from further consideration. This eliminates large smooth areas from consideration.

The use of pixel intensity gradient rather pixel intensity directly makes the process immune to grey level shifts which do not much affect intensity gradients.

In practice, if a video image is degraded or corrupted sufficiently that the pixel intensity gradient information cannot be recovered the appearance of the image to viewers will have been so greatly harmed that the copy will have no economic value.

This comparison of intensity gradients according to the invention allows the changes between an original digital video image and a copy digital video image to be identified and corrected for so that an embedded watermark can be recovered even after filtering, reformatting or conversion between the digital and analogue domains and vice versa. This applies to all forms of change including scaling, repositioning or skewing.

In a particularly advantageous embodiment of the invention the digital watermark embeds a pseudo random code or other data sequence into the mid-frequency components of the transform of the main of the digital video image and is recovered from a digital video image using a correlation technique.

Preferably the watermark should be embedded into the luminance data part of the digital video image instead of the chrominance data part.

The embedding of the digital watermark into the luminance part of the digital video image signal instead of the chrominance part provides the advantage that because the luminance part of the video image is the most visible part the degradation in the quality of the copy digital video image which will occur if the digital video image is corrupted or changed sufficiently to remove the digital watermark is maximised.

In general, the more energy the watermark carries, that is the greater the difference between the digital video signal with and without the watermark, the more robust the watermark will be. Accordingly, it is advantageous for the watermark to carry as much energy as possible without it becoming visible.

The maximum amount of energy that can be carried by an embedded digital watermark without affecting the perceived video image and becoming visible is increased if the digital watermark is embedded into higher frequency areas of the digital video signal.

This is because the human visual system is more sensitive to noise, which is how the digital watermark is perceived, in low frequency or smooth parts of the digital image than in high frequency or detailed parts of the video image. Thus, a higher energy digital watermark can be embedded into high frequency or detailed parts of the digital video image without the digital watermark being visible. As a result of this higher energy the digital watermark is more robust to attacks such as noise filtering.

Digital watermarks embedded in the spatial domain are low power high frequency noise added to the video image signal and as a result are vulnerable to attacks by processing techniques such as noise reduction or low pass filtering. By embedding the digital watermark into the video image signal in a transform domain the digital watermark can be made more robust and harder to remove. A preferred transform is the discrete wavelet transform or DWT. As an alternative, the discrete cosine transform or DCT can be used.

These transforms are convenient because the DCT is the standard transform used in MPEG2 digital image coding and the DWT is the standard transform used in MPEG4 coding.

The DWT transform is preferred because this gives a better match to the performance of the human visual system.

The DWT decomposition bands to be used for digital watermarking are partitioned into blocks of suitable size to allow the required amount of the digital watermark data to be embedded, for example the bands can be partitioned into 32 by 32 or 64 by 64 blocks. These relatively large blocks together with appropriately selected correlation thresholds provide a relatively robust digital watermarking system in which the digital watermark can be reliably extracted by correlation.

In general the 8 by 8 blocks used in standard in MPEG coding cannot be used for watermarking because the 8 by 8 blocks are too small for reliable correlation calculation.

In practice it has been found that attack on a digital watermark embedded in the first stage DWT decomposition bands have a relatively limited adverse effect on the reconstructed or copied video image. This is because the first stage or stage 1 wavelet decomposition bands correspond to the highest frequency parts of the digital image representing the finest details of horizontal, vertical and diagonal edges in the video image. Tampering with or removal of these coefficients will cause some loss of detail in the video image but will often not make the image unwatchable or unacceptable.

Accordingly, it is preferred to embed the digital watermark into the second stage or stage 2 wavelet decomposition bands and it has been found that changes to these coefficients in order to remove an embedded digital watermark has a more significant impact on the quality of the digital video image.

As explained above, the maximum energy which can be carried by the digital watermark is limited by the requirement that the digital watermark should not have any visible effect on the displayed video image. It is preferred that the watermarking procedure controls the energy held in the digital watermark to be as high as possible without affecting the digital video image in response to the characteristics of the part of the video image in which the watermark is to be embedded, taking into account the features of the human visual system. It is preferred to carry out this process by measuring the variance of the part of the video image where the digital watermark is to be embedded and to control the weight or energy of the digital watermark based on this variance.

The digital watermark itself is preferably a pseudo random code embedded into multiple parts of the image and recoverable or identifiable by correlation as discussed above.

Preferably the image is divided into a number of areas corresponding to the number of bits in the digital watermark so that a separate binary digit of the digital watermark can be embedded into and recovered from each of these parts of the image.

As explained above, the digital watermark according to the invention is sufficiently robust to survive digital to analogue and analogue to digital conversion. Accordingly the watermark can be extracted from analogue copies of the digital original, provided they are digitised first.

The pseudo random code of the digital watermark can be used to deter copyright infringement by encoding the origin or distribution channel of the digital image into the digital watermark in a second embodiment of the invention.

In the past the main commercial value of digital watermarking has been to authenticate digital images or video images by allowing their original source to be confirmed. Where the making of illicit copies is concerned this may be of use in the legal enforcement of copyright by proving that digital images are illicit copies, since the digital watermark allows the identity of the originator of the image to be proved this will show the digital image to be an illicit copy if the originator has not given permission for the copying. However, it is very

rarely the case that proving that an alleged infringing copy is a copy of the original is a matter of substance. It is generally extremely easy to show that the illicit copy is a copy of the original by comparing them directly, particularly because the economic value of the illicit copies is usually based on them being as similar as possible to the original.

The second embodiment of the invention provides a watermarking scheme in which an encrypted digital video image signal is received by a consumer decrypting device, for example a set top box, which inserts a digital watermark into the decrypted video signal sent for display.

Accordingly, if the video signal sent for display is illicitly copied, the digital watermarking can be recovered from the illicit copies and the consumer decrypting device, and thus the consumer producing the illicit copies or allowing their decrypted video signal to be used to produce the encrypted copies can be identified.

Preferably the digital watermarking scheme is a two stage digital watermarking process in which a first video watermark is applied by the distributor or content provider transmitting the encrypted digital video signal and a second digital watermark is inserted by the customer equipment.

A particularly useful application of the second embodiment of the invention is for use in the field of distributing pay per view or subscription only video, as follows.

The digital video signal has a first digital watermark embedded into it by the video supplier identifying the video supplier. The video supplier encodes the digital video signal, for example using MPEG, and transmits it to subscribers, for example through a fibreoptic cable digital network. The supplier digital watermark may be embedded into the signal before encoding.

The encoded digital video signal is received by an authorised subscriber having a subscriber set top box. The set top box decodes the encoded digital signal using a subscriber smart card which also carries a unique subscriber identity code.

The set top box decodes the received encoded video signal to produce a decoded viewable video signal and simultaneously embeds into the viewable decoded video signal a digital watermark including the unique subscriber identity code.

If the subscriber makes or allows to be made illicit copies of the decoded viewable digital video signal, the digital watermark carrying the unique subscriber identity code can be recovered from these copies.

This is of great commercial significance in preventing illicit copying because identification of the source of the illicit copies allows action to be taken to stop the copying. Such action could include revoking the subscribers status and possible further legal action. This will prevent the subscriber making further illicit copies of other material and will provide a deterrent effect.

It will be appreciated that although the example of the second embodiment of the invention refers to the unique subscriber identity being encoded into the second watermark it is only necessary that the unique subscriber identity be deduceable from the second watermark.

In the described example of the second embodiment of the invention the digital image is a digital video image. This is expected to be the most commercially valuable application of the invention. However, the invention can be applied to digital watermarking of other forms of signal such as still images.

In the described example of the second embodiment of the invention the transmitted digital video signal is encoded. It is not essential that the transmitted signal be encoded, some other form of copy protection requiring that the received signal be processed by the set top box could be used such as transmitting the digital video signal in a deliberately degraded form requiring processing by the set top box to reproduce the original digital video image. The transmitted digital video signal may also or alternatively be encrypted.

The described example of the second embodiment of the invention refers to the use of a consumer set top box to carry out decoding with the unique consumer identity being stored in and read from a subscriber smart card. The second embodiment of the invention is equally applicable to other forms of signal processing equipment and other techniques for providing a unique subscriber identity to be embedded into the second digital watermark. The unique code embedded into the second digital watermark could be unique to the data processing device used to provide the viewable digital video signal rather than the subscriber if preferred.

In the described example of the second embodiment of the invention the encoded video signal includes a digital watermark identifying the provider so that the displayable video signal includes two digital watermarks identifying the provider and the subscriber. This is preferred but not essential, the displayable video signal may include only the digital watermark identifying the subscriber.

The above embodiments are described by way of example only and the person skilled in the art will appreciate that the details can be changed and other techniques used within the scope of the present invention.

Claims:

1. A method of digital watermarking in which a digital watermark is embedded into a first digital image and it is subsequently attempted to identify the digital watermark in a second digital image, including the steps of:
measuring intensity gradients at a number of selected points in the first image;
measuring intensity gradients at multiple points in the second image;
comparing the measured intensity gradients in the first and second images and
identifying a point in the second image corresponding to each selected point in the first image based on the comparison;
calculating the changes between the first and second images from the differences between the locations of the selected points in the first image and the corresponding points in the second image; and
correcting for the calculated changes between the first and second images when attempting to identify the watermark in the second image.
2. A method according to claim 1, in which the digital watermark is embedded into the first digital image in the transform domain.
3. A method according to claim 2, in which the watermark is embedded in the discrete wavelet transform domain.
4. A method according to claim 3, in which the watermark is embedded in the second stage of wavelet decomposition.
5. A method according to any one of claims 2 to 4 in which the watermark is embedded into the mid-frequency components of the transform domain.
6. A method according to any preceding claim, in which the first digital image is divided into a plurality of areas and one bit of the digital watermark is embedded into each area.

7. A method according to any preceding claim, in which the digital watermark is a pseudo random data sequence.
8. A method according to any preceding claim, in which the watermark is identified in the second image using a correlation process.
9. A method according to any preceding claim, in which the selected points in the first image are selected by defining a number of regions of the first image; measuring the overall gradient in two orthogonal directions at each point in each region; and selecting the point having the highest overall gradient.
10. A method according to claim 9, in which the overall gradient of the points is compared to a threshold and the points are not selected if their overall gradient is below the threshold.
11. A method according to claim 9 or claim 10, in which points in the second image corresponding to the selected points are identified by defining a window in the second image centred on the location of each selected point in the first image; measuring the gradient in two orthogonal directions at each point in each window; and identifying the point in each window having measured gradients closest to those of the respective selected point as corresponding to said selected point.
12. A method according to any preceding claim, in which each point is a pixel.
13. A method of digital watermarking in which an encoded digital signal is operated on by a decoding means to provide a displayable digital signal and the decoding means incorporates a digital watermark into the displayable digital signal.
14. A method according to claim 13 in which the displayable signal is a digital image

signal.

15. A method according to any claim 13 or claim 14 in which the digital watermark identifies a user using the decoding means.
16. A method according to any one of claims 13 to 15 in which the digital watermark identifies the decoding means.
17. A method according to any one of claims 13 to 16 in which the encoded digital signal is encrypted and the decoding means carries out a decryption operation.
18. A method according to claim 17 in which the decoding means carries out a decoding operation using a smart card and the smart card provides a unique identity code which is used by the decoding means to generate the digital watermark.
19. A method according to claim 18 in which the identity code identifies the user.
20. A method according to any one of claims 13 to 19 in which the encoded digital signal incorporates a further digital watermark identifying the digital signal provider and this further digital watermark remains in the displayable digital signal.
21. A method according to any preceding claim in which the image is a video image.
22. Apparatus adapted to carry out the method of any preceding claim.

FIG.1A

-1	-2	-1
0	0	0
1	2	1

FIG.1B

-1	0	1
-2	0	2
-1	0	1

INTERNATIONAL SEARCH REPORT

Internal Application No

PCT/EP 01/05207

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 H04N7/26 H04N5/00

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)

IPC 7 H04N G06T

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 practical, search terms used)

EPO-Internal, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	SUN Q ET AL: "RECOVERING MODIFIED WATERMARKED IMAGE WITH REFERENCE TO ORIGINAL IMAGE" PROCEEDINGS OF THE SPIE, SPIE, BELLINGHAM, VA, US, vol. 3657, January 1999 (1999-01), pages 415-424, XP000961849	1-3,8,9, 11,12
A	the whole document	7,10
X	JOHNSON N F ET AL: "RECOVERY OF WATERMARKS FROM DISTORTED IMAGES" INFORMATION HIDING. INTERNATIONAL WORKSHOP PROCEEDINGS, XX, XX, no. 1768, September 1999 (1999-09), pages 318-332, XP008002242	1-4,7-11
	the whole document	

	-/--	



Further documents are listed in the continuation of box C.



Patent family members are listed in 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 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 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

21 June 2002

Date of mailing of the international search report

28.06.2002

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Marie-Julie, J-M

INTERNATIONAL SEARCH REPORT

Internal Application No
PCT/JP 01/05207

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	LOO P ET AL: "Motion estimation based registration of geometrically distorted images for watermark recovery" SECURITY AND WATERMARKING OF MULTIMEDIA CONTENTS III, SAN JOSE, CA, USA, 22-25 JAN. 2001, vol. 4314, pages 606-617, XP008001970 Proceedings of the SPIE - The International Society for Optical Engineering, 2001, SPIE-Int. Soc. Opt. Eng, USA ISSN: 0277-786X	1-3,7
A	the whole document	4-6
A	FR 2 789 783 A (CANON KK) 18 August 2000 (2000-08-18) page 12, line 15 -page 14, line 26 page 16, line 5 - line 17 page 18, line 22 -page 22, line 22	1-12
A	CELIK M U ET AL: "Analysis of feature-based geometry invariant watermarking" SECURITY AND WATERMARKING OF MULTIMEDIA CONTENTS III, SAN JOSE, CA, USA, 22-25 JAN. 2001, vol. 4314, pages 261-268, XP008001969 Proceedings of the SPIE - The International Society for Optical Engineering, 2001, SPIE-Int. Soc. Opt. Eng, USA ISSN: 0277-786X	1-12
A	the whole document	
A	KAEWKAMNERD N ET AL: "Wavelet based watermarking detection using multiresolution image registration" 2000 TENCON PROCEEDINGS. INTELLIGENT SYSTEMS AND TECHNOLOGIES FOR THE NEW MILLENNIUM (CAT. NO.00CH37119), 2000 TENCON PROCEEDINGS. INTELLIGENT SYSTEMS AND TECHNOLOGIES FOR THE NEW MILLENNIUM, KUALA LUMPUR, MALAYSIA, 24-27 SEPT. 2000, pages 171-175 vol.2, XP001066364 2000, Piscataway, NJ, USA, IEEE, USA ISBN: 0-7803-6355-8 the whole document	1-7,12
	----- -/--	

INTERNATIONAL SEARCH REPORT

Intern: I Application No

PCT/GB 01/05207

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	LOO P ET AL: "Digital watermarking with complex wavelets" IEE SEMINAR ON SECURE IMAGES AND IMAGE AUTHENTICATION (REF. NO.00/039), IEE SEMINAR ON SECURE IMAGES AND IMAGE AUTHENTICATION, LONDON, UK, 10 APRIL 2000, pages 10/1-7, XP001066365 2000, London, UK, IEE, UK the whole document ---	1-7,12
A	SCHMID C ET AL: "LOCAL GRAYVALUE INVARIANTS FOR IMAGE RETRIEVAL" IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, IEEE INC. NEW YORK, US, vol. 19, no. 5, 1 May 1997 (1997-05-01), pages 530-535, XP000693746 ISSN: 0162-8828 the whole document ---	1
X	WO 00 13136 A (DIGITAL VIDEO EXPRESS L P ;MERCIER GUILLAUME (US); LUO HUI (US); B) 9 March 2000 (2000-03-09) page 1, line 30 -page 2, line 5 page 34, line 24 -page 35, line 15 ---	13-22
A	EP 1 005 229 A (HEWLETT PACKARD CO) 31 May 2000 (2000-05-31) abstract ---	13,14
A	EP 0 975 165 A (SONY CORP) 26 January 2000 (2000-01-26) paragraph '0021! paragraph '0023! paragraph '0032! -----	13,17,18

INTERNATIONAL SEARCH REPORT

International application No.
CT/GB 01/05207

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:
3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☒ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest.
- ☒ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. Claims: 1-12

A method of embedding a digital watermark into a digital first image and identifying the digital watermark in a second image by using reference points in the first and second image.

2. Claims: 13-22

A decoding means operating on a encoded digital signal to provide a displayable digital signal and decoding means incorporates a digital watermark into the displayable digital signal.

INTERNATIONAL SEARCH REPORT

Intern	Application No
PCT, ^{us}	01/05207

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
FR 2789783	A	18-08-2000	FR 2789783 A1	18-08-2000
WO 0013136	A	09-03-2000	AU 6131899 A	21-03-2000
			WO 0013136 A1	09-03-2000
EP 1005229	A	31-05-2000	CN 1255021 A	31-05-2000
			EP 1005229 A2	31-05-2000
			JP 2000165889 A	16-06-2000
EP 0975165	A	26-01-2000	EP 1126705 A2	22-08-2001
			EP 0975165 A2	26-01-2000
			CN 1115150 A	17-01-1996
			DE 69523220 D1	22-11-2001
			DE 69523220 T2	13-06-2002
			EP 0691787 A1	10-01-1996
			JP 8077706 A	22-03-1996
			US 5796828 A	18-08-1998