A Review of Digital Watermarking

Allan M. Bruce

Department of Engineering, University of Aberdeen

November 2nd 2001

Abstract

This paper reviews a number of aspects of Digital Watermarking. Watermarking can be applied to many digital documents to protect against copyright infringements, including image, text and video formats. Image watermarking is commonly applied in the spatial and transform domains to achieve robust protection. Watermarking also has a role in legal aspects where the method can be used in a court of law as evidence of ownership. Malicious attacks are often used to degrade the watermark allowing copies to be distributed without protection. Several new methods are currently being researched to increase the effectiveness of watermarks. Such methods include the use of artificial intelligence and a second generation of benchmark software to check for robustness of watermarks.

INTRODUCTION

The unauthorised copying of many types of media has been a subject for concern for several years. In the past these copies have been obvious due to depreciation of quality which occurs when using analogue techniques, for example photocopying or recording CD audio to magnetic tape. Nowadays, with the home computer being very popular and widespread, digital copying is easy and 100% facsimiles of images, video, audio and text can be produced quickly and cost effectively. Distribution of these files occurs rapidly due to the internet being available in most homes. The World Wide Web is responsible for a vast increase in pirated media [1] due to its availability and speed of distribution.

Files can be manipulated or modified easily with wide ranges of software and people often claim that these modified files are theirs when in fact they were originally produced by somebody else. To stop these perfect digital copies and modified files being available several methods have been tried and tested [2] and until recently, have failed. Such methods of this include copy protection and file encryption. These old techniques suffer from major drawbacks [3]. Once an encrypted file has been decoded successfully, it can be copied as normal many times for redistribution with no encryption. Copy protection allows a media to be used from its original source but is intended to make unauthorised copies difficult, ideally impossible. Unfortunately these methods have always been cracked in the past and copies continue to be available with the protection removed.

BACKGROUND

It is apparent that copying will always take place therefore a method of identifying the route of copied media could be appealing. It is mainly desirable to detect whether a file is the original and also to whom the original belongs. Publishers are reluctant to distribute material electronically [4] so they would like a method of applying a digital signature to their productions for copyright reasons. “Copyright protection of digital images is defined as the process of proving the intellectual property rights to a court of law against the unauthorised reproduction, processing, transformation or broadcasting of a digital image”[5].

Consider a company producing media for sale, for example 3D models; a customer wishes to identify that the model they have purchased is the original unmodified object from the company. If the model has been modified it may be maliciously to ensure the model fails or does not adhere to the requirements specification therefore meaning another model to be sought from a competitor.

Perhaps an author produces forms of media and wishes them to be copyrighted against unauthorised use or distribution. There must be a method for determining the original author of a file for copyright laws to be enforced in the court of law.

With these requirements, a relatively old technique known as watermarking has been adapted for use in the modern age. It is simply referred to as digital watermarking. Traditional watermarking involved small visible marks in paper to ensure there originality or that they are official. Examples of this can be found in government cheques, official documents and paper money. This method has been modified and updated for digital images and similar techniques are also used for digital video, audio and text. Modern watermarks are no longer visible to the human eye but can be detected using a variety of methods. This review discusses methods of watermarking, types of attack against these and some legal aspects of the new techniques.

DIGITAL WATERMARKING

Digital watermarking is based on the science of steganography [6] or data hiding. Steganography comes from the Greek meaning ‘covered writing’. It is an area of research of communicating in a hidden manner. Steganography and watermarking rely on imperfections of human senses. The eyes and ears are not perfect detectors and cannot detect minor change therefore can be tricked into thinking two images or sounds are identical but actually differ, for examlpe in luminance or frequency shift. The human eye has a limited dynamic range so low quality images can be hidden within other high quality images [4].

There are three main stages in the watermarking process: generation & embedding, attacks and retrieval/detection.

Generation of watermarks is an important stage of the process. Watermarks contain information that must be unique otherwise the owner cannot be uniquely identified. Imagine two companies using identical watermarks, it would be impossible to prove which company the rightful author of a file belonged to. The most common method of generation is to consult a trusted third party and a watermark is generated guaranteeing uniqueness [7]. This third party would typically be a copyright authority or watermark specialist who would store a database of all its known clients. If a product is copied without authorisation and the matter is taken to court then this authority would be consulted to identify the original owner. This is done by extracting the watermark. An example of such a company is Digimarc [8]. Digimarc are a company who specialise in a variety of stages of watermarking. They offer generation of unique signatures and embedding algorithms along with the software to carry them out. One piece of software is the Digimarc Mediabridge^{TM} [15]. This piece of software can take a scanned or photographed image and then read the watermark embedded into it. If the watermark was generated by this software, it contains information which acts as a unique index. This index is looked up on the Digimarc server and points to a web link. This link is opened and appropriate information about the author or image can be displayed and necessary software can be loaded. This is done with no extra involvement or information from the user, it is carried out automatically. The watermark is said to act as a ‘bridge’ between the image and the information, hence the name for the software.

Another piece of software widely used in the field of watermarking is Stirmark [20]. It is used as a benchmark against attacks. Stirmark applies attacks to a watermarked image in nine different categories [19]. Some JPEG compression is applied in addition to these attacks. If a watermark is still detectable after an attack then a score of 1 is tallied, if not zero is. This is repeated for several images using all attacks and an average mark is obtained. This is the watermark algorithms benchmark score.

There is now also an official project for benchmarking watermarks called Certimark [19].

The embedding process uses an algorithm to incorporate a watermark within a file. These algorithms are widely researched and many have been developed thorough study [1,2,5,7,9-14].

Extraction of the watermark allows the owner to be identified and can also be used to provide information on the intended recipient. This stage is carried out using an algorithm based on the one used to embed the original watermark. Once the watermark has been successfully extracted, it is compared to those in the database and the registered owner can be identified. This stage sounds trivial but the watermark may be damaged by some malicious or accidental means.

Watermarks are often attacked so that the original owner cannot be uniquely identified. To maintain their robustness against attacks, watermarks have been adapted so that successful attack attempts are reduced.

LEGAL ISSUES

One of the main applications of watermarking is for copyright defence. An image, video, text document or audio sample may be embedded with a watermark and registered with a copyright authority. Watermarks are a legally recognised method of proof of ownership and if copyright is infringed then the matter can be presented to the court of law.

There are three types of watermark and their appropriate keys for removal. These are private-key, detection-key and public-key [5,7]. A private-key is available only to the author and can be thought of as a flair or signature to the product, for examlpe points being snapped to grid spacing in 3D objects or certain colours used in images. This type of watermark should not be detectable by anyone other than the original author. Public-key watermarks are those that can be extracted by the public. An example of this type of key is the RSA Algorithm [16] used in cryptography. These are used for verification purposes – perhaps to ensure the seller is the rightful owner. Finally, the detection-key is the method that is recognised in the court of law. This key is available only to the author and a trusted copyright authority and can be used to bring justice to copyright infringement. The key can be used to extract the watermark and this should uniquely identify the author. It is illegal to use copyrighted files for unauthorised distribution or for the watermark to be intentionally removed. Two example cases are discussed by Turnbull et al. [32] where copies of original media were found with the watermark erased. One case was successful as the watermark was intentionally removed however the other was not as it could not be proved that the watermark was removed on purpose.

Another application for watermarking is to trace the route of the certain files during distribution. Multiple watermarks can be embedded in media as long as saturation does not occur [3]. At each server or router in a network, a simple watermark may be embedded in real-time. These watermarks may contain an IP address or DNS name. Once a file is obtained using this method it is possible to trace the route of the file between clients.

The watermark within a file may be modified or removed so that the original owner cannot be uniquely identified. Such methods are known as attacks.

ATTACKS

If a file is generated containing a watermark for copyright reasons, some other party may wish to use it without paying royalties to the owner. Instead, they use techniques known as attacks on the watermark to either remove it or make it difficult to uniquely identify the owner. It is possible to attack the file in transport between client and copyright authority. Here it is best to use heavy encryption methods which take a long time to crack, however an unwatermarked copy may still be obtained eventually. Many types of attack are used and an algorithm for embedding the watermark should be robust against all attacks without affecting the quality of the image. Such attacks are image processing, geometric, compression and conversion.

Image processing is a common method of attack in which the image undergoes some mathematical change, usually blurring or sharpening [17]. Another image processing attack known as cropping is effective when the watermark is not present in the whole image or the whole image is required for detection of the watermark. The most common and successful type of attack is to apply lossy compression [9,18], for examlpe Joint Picture Experts Group (JPEG) or Motion Picture Experts Group (MPEG) methods. The watermarked image is compressed in the hope that losses will cause the watermark to be distorted. JPEG compression for images and MPEG compression for movies is used to reduce colour levels and bandwidth. JPEG uses a hybrid of amplitude modulation and frequency shift keying to compress its images [4]. Most new watermark embedding techniques offer robustness against compression.

Conversion is another method of attack. Common conversion is colour reduction (using less bits to identify colours therefore not as many are available resulting in the step between colours more noticeable so the watermark will become either visible or disappear depending on its robustness). Another method is digital to analogue conversion and vice versa. Here a digitally stored image may be printed on analogue media and then scanned back into a computer or photocopied. Such attacks are effective after many conversions but quality is greatly reduced from that of the original. Because of conversion to the analogue domain is possible, watermarks must also be resilient to common analogue interference such as Additive White Gaussian Noise (AWGN) [3].

Geometric attacks such as scaling and rotation are also possible but most algorithms are highly robust to these methods. One effective geometric attack is cropping as discussed earlier.

A common method of attack is becoming more successful. Jamming and saturation try not to alter the original watermark but embed further watermarks so that the original can not be extracted reliably. One specific method of this is the Twin Watermark Images Counterfeit Original (TWICO) attack [21].

EMBEDDING

Embedding is the process of applying the watermark to an image, video, text, or sound sample. Common embedding techniques are additive or multiplicative [22]. Several properties of these techniques must be considered in the embedding stage. A good watermark will be robust against attack but will also be imperceptible. A good watermark will remain as it will not be detected therefore attacks on it will not be attempted. Unfortunately, both robustness and imperceptibility are difficult to achieve, i.e. if a watermark is very robust, it will become detectable or if a watermark is indistinguishable then it does not offer good robustness. This is an area for very wide research and many different algorithms have been presented using many techniques. Most of these techniques are based on communications theory. In this review, watermarking of image, video and text are discussed but sound watermarking algorithms are not.

IMAGE WATERMARKING IN THE SPATIAL DOMAIN

Image watermarking is becoming more effective due to its extensive research. Original algorithms were calculated in the spatial domain. In images, not much information can be embedded into flat featureless regions without being detected [4]. Some algorithms attempt to incorporate most of the information into textured or on definite edges but care must be taken to maintain the integrity of the original.

A common method of watermarking was to alter the least significant bit of each pixel in a pseudo-random manner [9]. This offers poor robustness as it very susceptible to noise and also requires the original image for detection of the watermark.

An improvement was presented by Pitas [23] who used a binary mask overlaid on the image. The original binary mask was to be the same size of the image in pixels. The algorithm was based on statistical detection theory and a constant was added to each '1' in the binary mask. Signal processing attacks were successful against this technique. Instead of using a mask the same size as the image, binary patterns forming 2x2 or 3x3 blocks were used instead [24]. These altered methods were much more resilient to low pass and median pass filtering techniques. It was found that a combination of these two methods also proved robust against JPEG compression up to a ratio of 24:1. Further methods in the spatial domain include using 8x8 blocks as zones and the luminance averaged over each zone. Unfortunately these old techniques were not effective against rotation, cropping or scaling known as geometric attacks. One method which improved on these weaknesses was based on amplitude modulation in colour images [25]. The blue channel pixel values were modified in proportion to the luminance of the pixel as shown

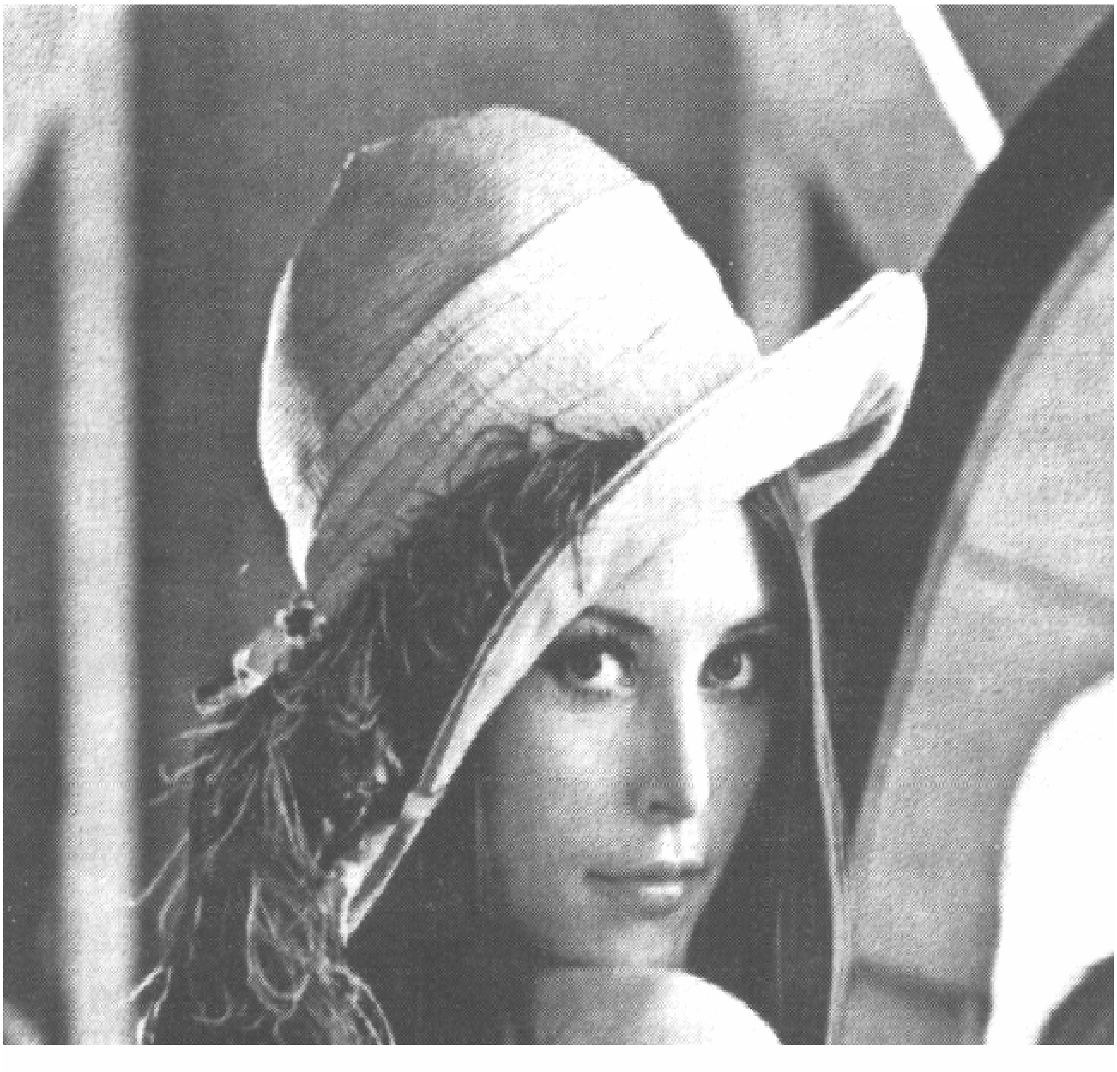

Figure 1, Lena strongly watermarked using bi-directional coding[4]

$$B_{i,j}* = B_{i,j} + (2s - 1)qL_{i,j}$$

Where B is the original value and B* is modified value, L is luminance, s is bit to be embedded and q is signature strength. The signature strength is adjusted for the robustness of the watermark, a high value gives a visible watermark and low values give low resistance watermarks. This algorithm was proved to be resilient against geometrical attacks, signal processing and JPEG compression. These techniques were developed for uni-directional coding. The image is split into blocks and the mean of each pixel in the block is obtained. Each block is given a binary value '0' or '1' which makes up a code used to store information. If the block denotes a 1 then the mean of the block is added to each pixel within the block. This proved to be a good reliable method but was adapted further for improved robustness. This advanced algorithm, named bi-directional coding was identical to uni-directional coding but included an extra stage. In this stage, if a block denoted a binary '0' the mean product was subtracted from each pixel. Figure 1, on the previous page, shows an example of bi-directional coding using a weak watermark therefore imperceptible. Figure 2, below shows an image with the same algorithm but

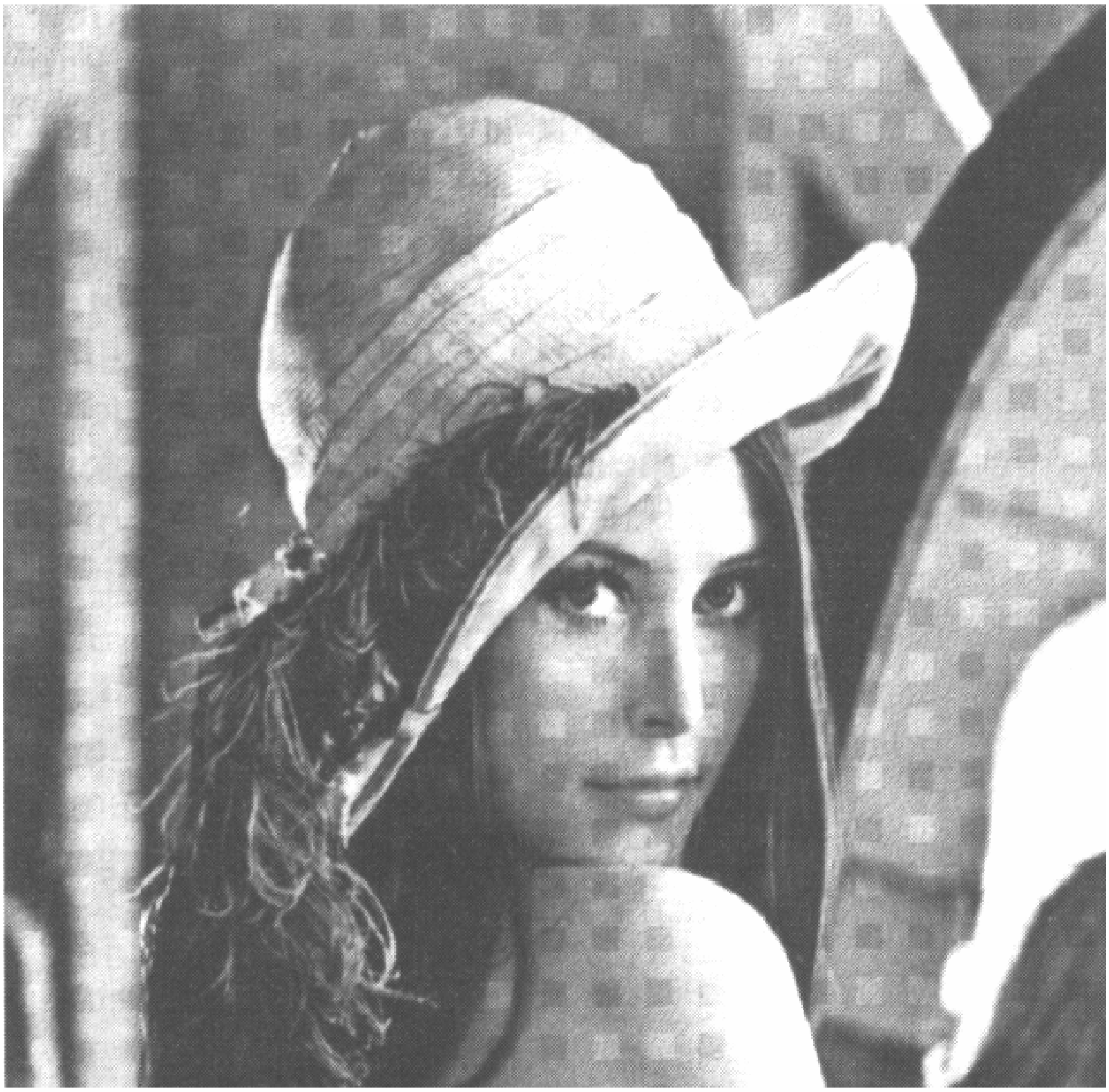

Figure 2, Lena strongly watermarked using bi-directional coding[4] using a stronger embedded watermark, this increases robustness but at the cost of image quality. There is a disadvantage to using this technique if embedding different information into the same image. If somebody obtains several copies of the image with the different watermarks, then they can compare the differences and read most, if not all, of the image. Caronni [27] got around this by randomising the block sizes and positions. This offered a simple yet highly robust approach to watermarking in the spatial domain.

These methods incorporate weaknesses in the human vision system. Wang and Bovik [26] discuss methods that rely on the human vision having highest spatial resolution at the foveation point (the point of fixation), therefore can remove high frequency information in the peripheral regions. This can be combined with common techniques to embed a more robust watermark in these areas.

Another exploitation of the human vision system is to embed information into high frequency regions of images as the human eye has a limited dynamic range and is most responsive to low frequencies [18]. This technique is robust against many attacks but a simple low pass filter or lossy compression could destroy the watermark.

A more robust algorithm may be adapted by analysing the image in the transform domain.

IMAGE WATERMARKING IN THE TRANSFORM DOMAIN

Most of these methods are based on the Discrete Cosine Transform (DCT) or the Fast Fourier Transform (FFT) although many others have been attempted and proven to be successful. Bors and Pitas [28] proposed an algorithm that used 8x8 blocks. The algorithm is split into two main sections. Parameters are first used to find block locations. Secondly, parameters for constraint are imposed on the DCT coefficients.

Zhao and Koch [29] use a similar technique but instead of calculating which blocks to use for transformation, blocks are selected at random and then quantised. This method is susceptible to geometric distortion.

Ruanaidh *et al.* [4] discuss an algorithm in the transform domain where "a simple form of modulation for placing bits on an image is outlined. Secondly, a technique for determining the number of bits to be placed at given locations in the image is described"

They use an adaptation of the JPEG algorithm and is explained in the following steps:

1. First, the image is divided into appropriately sized blocks
2. The mean of the block is then subtracted from each pixel within the block
3. Each pixel in the block is then normalised within the range of -127 to 127
4. The transform of each block is then calculated
5. Next, selected coefficients of the transformation are modulated, for examlpe using bi-directional coding
6. Finally, the inverse transform is computed, denormalised and the mean of the block is added to each pixel. This block then replaces the original from the image.

Detection can be done by carrying out steps 1 through 4 on the original unwatermarked image.

This algorithm provides a very robust watermark and can be implemented quickly if using the Fast Fourier Transform.

VIDEO WATERMARKING

There is a vast area of research into watermarking when applied to video. Here, many of the techniques from image watermarking can be applied but several constraints require development of the basic algorithms. Videos are generally large and therefore can be time consuming to apply watermarks. Because of this a watermark algorithms must be rapidly calculated for video applications. Some watermarks may be required to be embedded in real-time to allow broadcast or multicast transmission of streaming video. Sky use a method of encryption in real-time to broadcast their television service [30]. Limited bandwidth defines another design constraint of the algorithm used to embed video watermarks. A video occupies a certain bandwidth and it is desirable this is not increased after embedding a watermark. Finally, many videos are often stored in compressed format that relies on processing only changed images from frame to frame, for examlpe MPEG. Due to this, if a watermark is embedded, care must be taken to ensure it does not become too visible.

There are many algorithms used for differing video formats. The most common modern method of compression is the MPEG-2 algorithm used in coding DVD-video(Digital Versatile Disc). Figure 3 below shows a block diagram of the embedding of a watermark into DVD MPEG-2 video. This method of compression relies on block motion compensation (BMC) and after BMC uses DCT compression to describe the residual error[x]. In the diagram EC is used to mean Entropy Coding and Q for quantisation. A superscript -1 denotes the inverse of these.

There are 3 main areas in the embedding process to satisfy the constraints mentioned earlier:

A. To ensure that the bandwidth of the final watermarked video is not greatly increased, the watermark is only embedded into non-zero DCT coefficients. This maintains the high level of compression within MPEG-2 video.
B. As mentioned MPEG compression uses a method of only updating changed images in video clips. It incorporates within this, a level of predictive compression. To maintain high image quality and avoid watermarks from previous frames creating visible distortion, a drift compensation signal is introduced.
C. To enable the compression to remain high and maintain available bandwidth, a check is introduced to compare the watermarked frame with the unwatermarked one. If the watermarked frame occupies

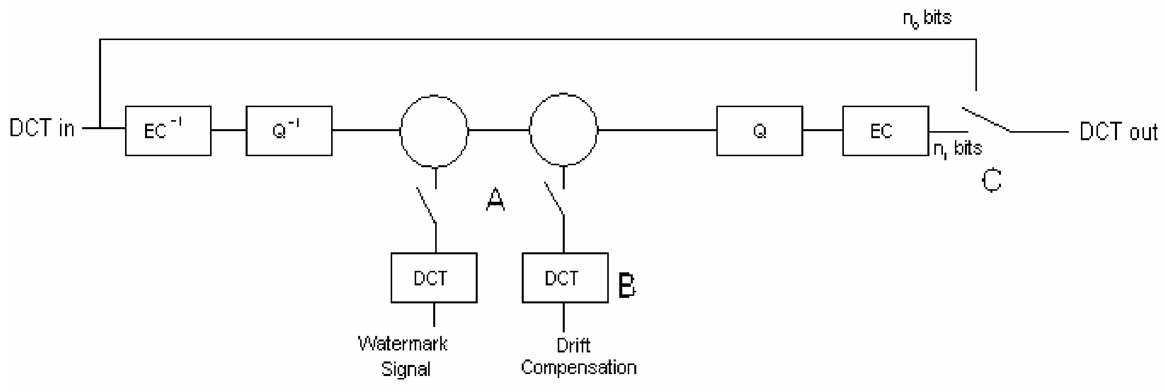

Fig. 3. Block Diagram Showing the Embedding of a Watermark in MPEG-2 video [3]

more bits in the bitstream it is disregarded and the unwatermarked frame is used instead.

DVD-video has remained a very secure for of storing digital media due to its high level of encryption and watermarking may be used as a backup. Some DVDs have been cracked in the past because one company accidentally produced a DVD which stored the encryption key on the disc in a readable form. This was exploited by hackers who then produced software to remove the encryption from DVDs. Nowadays, DVDs now use a different key but it only a matter of time before another hacker 'cracks' the code.

TEXT WATERMARKING

The final method of embedding watermarks discussed in this review will be in the application of text watermarking.

Some important documents are very valuable in their original form and require to be watermarked, for examlpe wills, cheques, contracts and title deeds. As with image watermarking it is possible to embed an imperceptible watermark to uniquely identify the author. Methods of doing this rely on the format of storage.

Text can be stored in many different ways and unfortunately some of these cannot be watermarked, for examlpe ASCII encoding contains no perceptual headroom [3] and therefore cannot be watermarked in its raw format. Formats that may be include any that are stored in a formatted manner, for examlpe postsrcipt and portable document format (pdf), indeed this document has been watermarked so that the author can be identified. In these files the watermark again makes use of imperfections in the human vision system. Each character is too small to contain a watermark therefore an alternative yet simple method provides an extremely robust watermark. This technique modulates inter-line spacing and the spacing between words [31]. Small differences, as small as one four hundredth of an inch, is enough to withstand photocopying up to ten times. A more obvious but commonly used method is to vary fonts or font sizes within the document to allow for a higher level of robustness against attack. Different algorithms are used to format the spacing this way for a given watermark but uniqueness is easily achieved.

Many applications incorporate a watermark feature to apply a signature to text, indeed this document has been watermarked using Adobes' Acrobat software. Application of a watermark is simple using this package. A profile needs to be setup which contains information about the author, then using a drop-down menu the document can be signed.

It is possible to bypass this type of digital signature by using Optical Character Recognition (OCR) software using a quality scanner but this process is slow, expensive, inaccurate and often requires manual supervision.

UPCOMING METHODS

All methods of watermark embedding have advantages and disadvantages but the most common drawback is the lack of successful detection after attacks.

Yu *et al.* [2] have developed a new technique of detection. In there tests, a modified Kutters Algorithm was used. Kutter also exploits imperfections in the human eye and its inability to recognise small variance in colour. This algorithm is successful to most common types of attack but the detection process can be difficult. To increase the success rate of detecting the watermark, Yu *et al.* decided to use Artificial Neural Networks (ANNs). Many images are embedded with a particular watermark and then attacked by many different techniques. Once a large number of these attacked watermarked images are available, they are used as a training set for an ANN, which 'learns' what the various attacked watermarks look like. A new unseen attacked image may then be input to the ANN and it should be able to detect more watermarks which conventional methods failed to do. Initial tests have proved to be good and detection is approximately four times better with some common attacks.

CONCLUSION

In this paper, many aspects of watermarking have been reviewed. Applications for watermarking include the ability to trace a document transferred via the internet or to store information about the author and intended recipients. The most important application of watermarks, however, is for protection against copyright violation. Registered authorities accept watermarking as a proof of ownership and this can be used in the court of law.

Image watermarking is the most researched area and can be split into two main categories by the mathematical techniques used to embed information. In the spatial domain, an adaptation of bi-directional coding was found to be very simple yet offered a robust watermark. Bi-directional coding is also utilised in various methods of watermarking in the transform domain.

Watermark algorithms used for video streams are generally similar but embedding methods vary. This depends on which format the file is stored in. Drift compensation is used in compressed video files, for example MPEG-2. This method is used to ensure image quality remains. Watermarked frames are discarded if the bandwidth is greater than the unwatermarked version.

Modulation of inter-line and inter-word spacing was found to be a common technique used to embed watermarks into text documents. This was achieved easily using Adobe Acrobat.

Watermarked information can be destroyed by attacks. Many different attacks on watermarks are used and the most common successful attack is lossy compression, especially JPEG conversion in images. Sirmark is used to benchmark the robustness of a watermark algorithm although S. Voloshynovskiy *et al.* [32] have very recently proposed a second generation watermark benchmark.

Other recent developments in this field include the use of artificial intelligence to detect attacked watermarks.

With these improvements, watermarking is becoming an increasingly reliable method of storing important information and protection of digital documents.

REFERENCES

[1] H.J. Wang, P.-C. Su and C.-C. Jay Kuo, Wavelet-based digital image watermarking, Optics Express (Dec 1998) pp491-496.

[2] P.-T. Yu, H.-H. Tsai, J.-S. Lin, Digital watermarking based on neural networks for colour images, Signal Processing (Mar 2001) pp663-671.

[3] J.K. Su, F. Hartung and B. Girod. Digital watermarking of text, image and video documents, Computers & Graphics (Dec 1998) pp687-695

[4] J.J.K O-Ruanaidh, W.J. Dowling, F.M Boland, Watermarking digital images for copyright protection, IEE Proceedings in Vision, Image and Signal Processing (Aug 1996) pp250-256.

[5] J. O-Ruanaidh *et al.,* Cryptographic copyright protection for digital images based on watermarking techniques, Theoretical Computer Science (Sep 1999) pp 117-142.

[6] L.M. Marnel, C.G Boncelet, Jr and C.T Retter, Spread spectrum image steganography, IEEE Transactions on Image Processing (Aug 1999) pp 1075-1083.

[7] C. Fornaro and A.Sanna, Public key watermarking for authentication of CSG models, Computer-Aided Design (Oct 2000) pp 727-735.

[8] Digimarc Software, http://www.digimarc.com, Oct 2001

[9] M. Barni *et al.*, Copyright protection of digital images by embedded unpercievable marks, Image and Vision Computing (Aug 1998) pp897-906.

[10] J.R. Hernandez, J.M Rodriguez, F. Perez-Gonzalez, Improving the performance of spatial watermarking of images using channel coding, Signal Processing (Jul 2000) pp 1261-1279.

[11] S. Pereira, S. Voloshynoskiy and T. Pun, Optimal transform domain watermark embedding via linear programming, Signal Processing (Jul 2001) pp1251-1260.

[12] F. Perez-Gonzalez, J.R. Hernandez and F. Balado, Approaching the capacity limit in image watermarking: a perspective on coding techniques for data hiding applications, Signal Processing (Jul 2001) pp 1215-1238.

[13] R. Baitello *et al.*, From watermark detection to watermark decoding: a PPM approach, Signal Processing (Jul 2001) pp 1261-1271.

[14] M. Borni *et al.*, A DCT-domain system for robust image watermarking, Signal Processing (May 1998) pp 357-372.

[15] S. Decker, Engineering considerations in commercial watermarking, IEEE Communications Magazine (Aug 2001) pp 128-133.

[16] B. Schneier, Applied cryptography 2nd edition, Wiley 1995.

[17] J.R. Hernandez *et al.*, Information retrieval in digital watermarking, IEEE Communications Magazine (Aug 2001) pp 110-116.

[18] C.-T. Hsu and J.-L. Wu, Hidden digital watermarks in images, IEEE Transactions on Image processing (Jan 1999) pp 58-68.

[19] S. Voloshynovskiy, S. Pereira and T. Pun, Attacks on digital watermarks: classification, estimation-based attacks, and benchmarks, IEEE Communications Magazine (Aug 2001) pp 118-126.

[20] F.A.P Petitcolas and M.G. Kuhn, Stirmark Software, http://www.cl.cam.ac.uk/~fapp2/watermarking/stirmark/, Oct 2001

[21] S. Craver *et al.*, http://www.cs.arizona.edu/~collberg/Teaching/620/1999/Handouts/hual2.ps.gz Oct 2001

[22] M. Barni *et al.*, Watermark embedding: hiding a signal within a cover image, IEEE Communications Magazine (Aug 2001) pp 102-108.

[23] I. Pitas, A method for signature casting on digital images, IEEE Int. Conf. on Image Processing (1994) pp 86-90.

[24] N. Nikolaidis and I. Pitas, Copyright protection of images using robust digital signatures, IEEE Int. Conf. on Acoustics, Speech and Signal Processing (1996) pp 2168-2171.

[25] M. Kutter, F. Jordan, and F.Bossen, Digital signature of color images using amplitude modulation, Proc SPIE, Software and Retrieval for Image and Video Databases (Feb 1997) pp 518-526.

[26] Z. Wang and A.C. Bovik, Embedded foveation image coding, IEEE Transactions on Image Processing (Oct 2001) pp 1397-1410.

[27] G. Caronni, Assuring ownership rights for digital images, Reliable IT Systems VIS95, Viewreg Publishing Company, Germany (1995).

[28] A. Bors ad I. Pitas, Image watermarking using DCT domain constraints, IEEE Int. Conf. on Image Processing (Sep 1996) pp 231-234.

[29] J. Zhao and E. Koch, Embedding robust labels into images for copyright protection, Proc. Int. Congression on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies, Vienna (Aug 1995) pp 242-251.

[30] M. Barni *et al.*, Digital watermarking for copyright protection: a communication perspective (Editorial), IEEE Communication Magazine (Aug 2001) pp 90-91.

[31] Brassil *et al.*, Electronic marking and identification techniques to discourage document copying, Proceedings of INFOCOM 94.

[32] S. Voloshynovskiy *et al.*, Attack modelling: towards a second generation watermarking benchmark. Signal Processing (Jun 2001) pp 1177-1214