International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 3, 2013. ISSN: 2348-6600
Reference ID: IJCS-018 PAGE NO: 091-098

Survey on Joint Photographic Experts Group [JPEG] Watermarking

M.Veni [#1], Dr.P.Eswaran [*2]

[#1], M. Phil scholar, Department of Computer Science and Engineering,
Alagappa University, Karaikudi.
India.

[*2] Assistant professor, Department of Computer Science and Engineering,
Alagappa University, Karaikudi.
India.

Abstract— ***The expansion of the Internet has frequently increased the availability of digital data such as audio, images and videos to the public. Digital watermarking is a technology being developed to ensure and facilitate data authentication, security and copyright protection of digital media. Watermarking, which belong to the information hiding field, has seen a lot of research interest recently. There is a lot of work begin conducted in different branches in this field. Steganography is used for secret communication, whereas watermarking is used for content protection, copyright management, content authentication and tamper detection. We classify the techniques based on different domains in which data is embedded.***
Keywords -Watermarking, internet, authentication.

I. INTRODUCTION

Digital watermarking is a technique which embeds additional information called digital signature or watermark into the digital content in order to secure it[1]. A watermark is a hidden signal added to images that can be detected or extracted later to make some affirmation about the host image. The major point of digital watermarking is to find the balance among the aspects such as robustness to various attacks, security and invisibility. The invisibleness of watermarking technique is based on the intensity of embedding watermark. Better invisibleness is achieved for less intensity watermark. So we must select the optimum intensity to embed watermark. In general there is a little tradeoff between the embedding strength (the watermark robustness) and quality (the watermark invisibility). Increased robustness requires a stronger embedding, which in turn increases the visual degradation of the images[3].

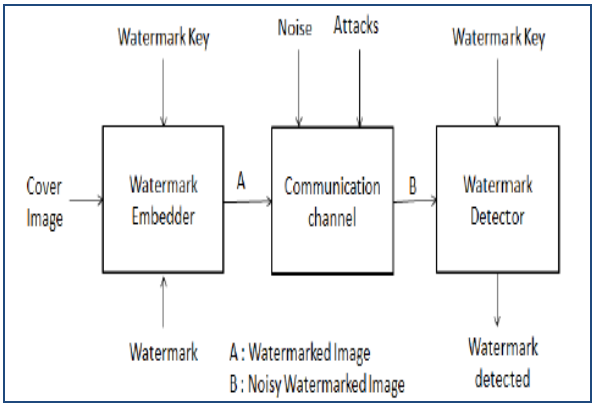

Figure 1 Digital WaterMarking

II. TERMINOLOGY

- Visible watermarks

Visible watermarks are visual patterns that are inserted into images or video, like in paper watermarks. It can be used to mark preview images available in image'

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 3, 2013. ISSN: 2348-6600
Reference ID: IJCS-018 PAGE NO: 091-098

databases or on the web to prevent commercial use. It is also possible to add audible marks into soundtrack of a video. Nevertheless, we will focus on imperceptible watermarks since visible watermarks remain difficult to protect and alter the original media[3].

- Fingerprinting and Labeling

Both terms denote special applications of watermarking, where information such as the creator or recipient of the data is embedded. This information can be a code that corresponds to the person. In labeling, it can be any information of interest.

- Bitstream watermarking

It is often used for compressed data streams such as video.

- Embedded signatures

This term, which comes from cryptography, was often used instead of watermarking. Nowadays, it leads to confusion since the cryptographic signatures serve for authentification purposes by detecting any alteration of the data and to authenticate the sender. With watermarking techniques, authentification can be applied to different kind of media and it requires an additional feature, that is to say, robustness. Watermarks have to resist to alterations and modifications.

- Fragile watermarks

These watermarks have a limited robustness. They are applied for detection of modification of the data, rather than conveying unerasable information.

III. TECHNIQUES

Watermarking is the method to hide the secret information into the digital media using some strong and appropriate algorithm. Algorithm plays a vital role in watermarking as, if the used watermarking technique is efficient and strong then the watermark being embedded using that technique cannot be easily detected. The attacker can only destroy or detect the secret information if he know the algorithm otherwise it is critical to know the watermark. There are various algorithms present in the today scenario that are used to hide the information. Those algorithms come into two domains, Spatial and Frequency domain [5].

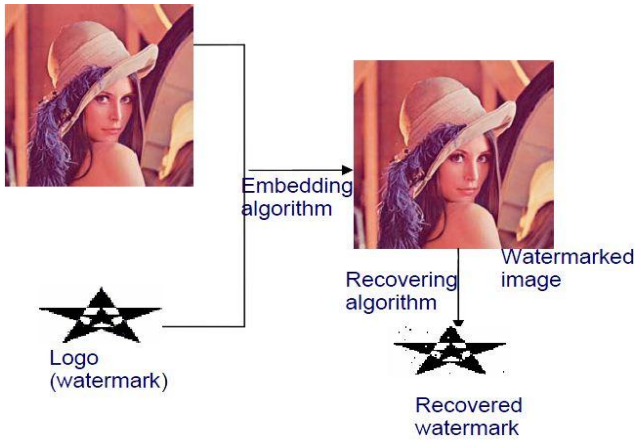

Figure 2 Process of Water marking

Spatial domain: Spatial domain digital watermarking algorithms directly load the raw data into the original image. Spatial watermarking can also be applied using color separation. In this way, the watermark appears in only one of the color bands. This renders the watermark visibly subtle such that it is difficult to detect under regular viewing. Spatial domain is manipulating or changing an image representing an object in space to enhance the image for a given application. Techniques are based on direct manipulation of pixels in an image .

Additive Watermarking: The most straightforward method for embedding the watermark in spatial domain is to add pseudo random noise pattern to the intensity of image pixels. The noise signal is usually integers like (-1, 0, 1) or sometimes floating point numbers. To ensure that the watermark can be detected, the noise is generated by a key, such that the correlation between the numbers of different keys will be very low.

Least Significant Bit: Old popular technique embeds the watermark in the LSB of pixels. This method is easy to implement and does not generate serious distortion to the image; however, it is not very robust against attacks[7]. The embedding of the watermark is

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 3, 2013. ISSN: 2348-6600
Reference ID: IJCS-018 PAGE NO: 091-098

performed choosing a subset of image pixels and substituting the least significant bit of each of the chosen pixels with watermark bits. The watermark may be spread throughout the image or may be in the select locations of the image. But these primitive techniques are vulnerable to attacks and the watermark can be easily destroyed. Such an approach is very sensitive to noise and common signal processing and cannot be used in practical applications.

SSM Modulation Based Technique: Spread-spectrum techniques are methods in which energy generated at one or more discrete frequencies is deliberately spread or distributed in time. SSM based watermarking algorithms embed information by linearly combining the host image with a small pseudo noise signal that is modulated by the embedded watermark.

Texture mapping coding Technique*:* This method is useful in only those images which have some texture part in it. This method hides the watermark in the texture part of the image. This algorithm is only suitable for those areas with large number of arbitrary texture images (disadvantage), and cannot be done automatically. This method hides data within the continuous random texture patterns of a picture.

Patchwork Algorithm: Patchwork is a data hiding technique developed by Bender et alii and published on IBM Systems model. Patchwork imperceptibly inserts a watermark with a particular statistic using a Gaussian distribution. A pseudo randomly selection of two patches is carried out where the first one is A and the second is B. Patch A image data is brightened where as that of patch B is darkened (for purposes of this illustration this is magnified).

Frequency domain: Compared to spatial-domain methods, frequency-domain methods are more widely applied. The aim is to embed the watermarks
in the spectral coefficients of the image. The most commonly used transforms are the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), the reason for watermarking in the frequency domain is that the characteristics of the human visual system
HVS captured by spectural components.

Discrete cosine transforms (DCT): DCT like a Fourier Transform, it represents data in terms of frequency space rather than an amplitude space. This is useful because that corresponds more to the way humans perceive light, so that the part that are not perceived can be identified and thrown away. DCT based watermarking techniques are robust compared to spatial domain techniques. Such algorithms are robust against simple image processing operations like low pass filtering, brightness and contrast adjustment, blurring etc. However, they are difficult to implement and are computationally more expensive. At the same time they are weak against geometric attacks like rotation, scaling, cropping etc. DCT domain watermarking can be classified into Global DCT watermarking and Block based DCT watermarking

Discrete wavelet transforms (DWT): Wavelet Transform is a modern technique frequently used in digital image processing, compression, watermarking etc. The transforms are based on small waves, called wavelet, of varying frequency
and limited duration. The wavelet transform decomposes the image into three spatial directions, i.e. horizontal, vertical and diagonal[30].

Algorithm	Advantages	Disadvantage
LSB	Easy to implement and understand Low degradation of image quality	It lacks basic robustness. Vulnerable to noise Vulnerable to cropping, scaling.
Correlation	Gain factor can be increased resulting in increased robustness	Image quality gets decreased due to very high increase in gain factor

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 3, 2013. ISSN: 2348-6600
Reference ID: IJCS-018 PAGE NO: 091-098

Patchwork	High level of robustness against most type of attacks	It can hide only a very small amount of information.
Texture Mapping coding	This method hide data within the continuous random texture patterns of a picture	This algorithm is only suitable for those areas with large number of arbitrary texture
DCT	The watermark is embedded into the coefficients of the middle frequency, so the visibility of image will not get affected and the watermark will not be removed by any kind of attack.	Block wise DCT destroys the invariance properties of the system. Certain higher frequency components tend to be suppressed during the Quantization step.

IV. SURVEY ON JPEG IMAGES IN WATER MARKING

- **SPATIAL DOMAIN BASED WATERMARKING SCHEMES**

LSB BASED SCHEMES

In their paper, Macq and Quisquater briefly discussed the issue of watermarking digital images as part of a general survey on cryptography and digital television. The authors provided a description of a procedure to insert a watermark into the least significant bits of pixels located in the vicinity of image contours[14]. Since it relies on modifications of the least significant bits, the watermark is easily destroyed. Further, their method is restricted to images, in that it seeks to insert the watermark into image regions that lie on the edge of contours.

- **PATCH WORK BASED SCHEMES**

Another, well known spatial domain based scheme is patchwork-based technique given by Bender et al. They described two watermarking schemes. The first is a statistical method called *patchwork*. Patchwork randomly chooses pairs of image points, and increases the brightness at one point by one unit while correspondingly decreasing the brightness of another point. The second method is called "texture block coding" wherein a region of random texture pattern found in the image is copied to an area of the image with similar texture. Autocorrelation is then used to recover each texture region. The most significant problem with this scheme is that it is only appropriate for images that possess large areas of random texture. The scheme could not be used on images of text.

- **CORRELATION BASED WATERMARKING SCHEMES**

The most straightforward way to add a watermark to an image in the spatial domain is to add a pseudorandom noise pattern to the luminance values of its pixels.

- **CORRELATION BASED SCHEMES WITH 1 PN SEQUENCE**

A well known technique for watermark embedding is to exploit the correlation properties of additive pseudo-random noise patterns as applied to an image[20].

Many watermarking methods have been proposed in the literature. Schyndel, Tirkel, and Osborne generated a watermark using a m-sequence generator. The watermark was either embedded or added to the least significant bit of the original image to produce the watermarked image. The watermark was extracted from a suspected image by taking the least significant bits at the proper locations. Detection was performed by a cross-correlation of the original and extracted watermark. Schyndel *et al*. showed that the resulting image contained an invisible watermark with simple extraction procedures. The watermark, however, was not robust to additive noise.

Cox *et al*. noted that in order for a watermark to be robust to attack, it must be placed in perceptually significant areas of the image. The watermark was based on 1000 random samples of a N(0,1) distribution. These samples were added to the 1000 largest DCT coefficients of the original image, and the inverse DCT was taken to retrieve t watermarked image. For detection, the watermark was extracted from the DCT of a suspected image. Extraction was based on knowledge of the original signal and the exact frequency locations of the

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 3, 2013. ISSN: 2348-6600
Reference ID: IJCS-018 PAGE NO: 091-098

watermark. The correlation coefficient was computed and set to a threshold. If the correlation was large enough, the watermark was detected. Their method was robust to image scaling, JPEG coding, dithering, cropping, an rescanning[26].

Xia, Boncelet, and Arce proposed a watermarking scheme based on the Discrete Wavelet Transform (DWT). The watermark, modeled as Gaussian noise, was added to the middle and high frequency bands of the image. The decoding process involved taking the DWT of a potentially marked image. Sections of the watermark were extracted and correlated with sections of the original watermark. If the cross-correlation was above a threshold, then the watermark was detected. Otherwise, the image was decomposed into finer and finer bands until the entire, extracted watermark was correlated with the entire, original watermark. This technique proved to be more robust than the DCT method. When embedded zero-tree wavelet compression and halftoning were performed on the watermarked images. Improvements on the above schemes were possible by utilizing properties of the Human Visual System. Bartolini *et al.* first generated a watermarked image from DCT coefficients. Then spatial masking was performed on the new image to hide the watermark.

Kundur and Hatzinakos embedded the watermark in the wavelet domain. The strength of the watermark was determined by the contrast sensitivity of the original image. Both techniques showed resistance to common signal processing operations.

Delaigle *et al* proposed a unique watermarking scheme based on the Human Visual System. Binary m-sequences were generated and then modulated on a random carrier. This image served as the watermark, and then it was masked based upon the contrast between the original signal and the modulated image. The masked watermark was added to the original image to form the watermarked image. Their technique was robust to additive noise, JPEG coding, and rescanning.

Craver *et al* noted that certain watermarking techniques were susceptible to counterfeit attacks. They showed that the method proposed by Cox et al. can be attacked by creating a fake original image and fake watermark that is indistinguishable from the true original image and watermark. To prevent this scenario, they modified the Cox *et al.*The algorithm by making the watermark dependent on the original image. This new scheme was less susceptible to counterfeiting and still maintained robustness.

Bas, Chassery, and Davoine introduced a watermarking system using fractal codes. A collage map was composed from 8x8 blocks of the original image and from the image's DCT. The watermark was added to the collage map to produce a marked image. The results showed that fractal coding in the DCT domain performed better than coding in the spatial domain. The DCT-based watermarking technique was robust to JPEG compression, while spatial fractal coding produced block artifacts after compression.

RESULTS AND DISCUSSION

The following comparison table depends upon the factor of Watermarking and also calculates the cost, complexity.

Factors	Spatial Domain	Frequency domain
Computation cost	Low	High
Robustness	Fragile	More robust
Perceptual quality	High control	Low control
Computational complexity	Low	High
Computational time	Less	More
Capacity	High	Low
Examples of application	Mainly authentication	Copy rights

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 3, 2013. ISSN: 2348-6600
Reference ID: IJCS-018 PAGE NO: 091-098

Examples of Watermarking

(a) Original Lena image (b) Watermarked Lena image

CONCLUSION

In this paper we surveyed the current literature on digital mage watermarking. We had a look at some current methods of watermarking, including additive and substitutive techniques in the frequency or spatial domains. The next generation of watermarking techniques will focus on the content of the data. An image will not be watermarked but every part of the image will contain the embedded information. The existing tools for image segmentation, active contour searching and differential treatments motivate this approach. Watermarking techniques are still a very recent domain of research. The solutions proposed in term of security, still face the problem of robustness. Contrary to cryptographic techniques, which are widely used and efficient since years, the use of watermarks to protect copyrights seems to be difficult to manage. Nevertheless, both domains focus on different topics. Watermarking must solve a problem of transparent broadcasting of protected data.

ACKNOWLEDGMENT

I also thank my parents and my friends for their constant encouragement and support at all phases in my life. I also thank the Almighty for showering His blessings throughout to develop this paper.

REFERENCES

[1] Manpreet kaur, Sonia Jindal, Sunny behal, ―A Study of Digital image watermarking‖, Volume2, Issue 2, Feb 2012.

[2] Evelyn Brannock, Michael Weeks, Robert Harrison, Computer Science Department Georgia State University ―Watermarking with Wavelets: Simplicity Leads to Robustness‖, Southeast on, IEEE, pages 587 – 592, 3-6 April 2008.

[3] Vidyasagar M. Potdar, Song Han, Elizabeth Chang, ―A Survey of Digital Image Watermarking Techniques‖, 2005 3rd IEEE International conference on Industrial Informatics (INDIN).

[4] Jiang Xuehua, ―Digital Watermarking and Its Application in Image Copyright Protection‖, 2010 International Conference on Intelligent Computation Technology and Automation.

[5] Ensaf Hussein, Mohamed A. Belal, ―Digital Watermarking Techniques, Applications and Attacks Applied to Digital Media: A Survey‖, IJERT, ISSN: 2278-0118, Vol. 1 Issue 7, September-2012.

[6] C.-T. Li and F.M. Yang., ―One-dimensional Neighborhood Forming Strategy for Fragile Watermarking‖. In Journal of Electronic Imaging, vol. 12, no. 2, pp. 284-291, 2003.

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 3, 2013. ISSN: 2348-6600
Reference ID: IJCS-018 PAGE NO: 091-098

[7] [6] Rakesh Ahuja, S S Bedi, Himanshu Agarwal, ―A Survey of Digital Watermarking Scheme‖, MIT International Journal of Computer Science and Information Technology, Vol.2, No. 1, Jan. 2012, pp.(52-59).

[8] R. Radhakrishnan and N. Memon, "On the security of the SARI image authentication system," in *Proc. IEEE International Conference on Image Processing (ICIP 01)*, Thessaloniki, Greece, October 2001.

[9] C.-Y. Lin and S.-F. Chang, "SARI: Self-authentication-and recovery image watermarking system," in *Proc. 9th ACM International Conference on Multimedia*, Ottawa, Canada, 30 September–5 October 2001.

[10] Xie, L., Boncelet, G., Acre, G.R., "Wavelet transform basedwatermarking for digital images", in Optics Express, vol. 3, no. 12,Dec 1998.

[11] Boneh, D.; Shaw, J.; "Collusion-secure fingerprinting for digital data," IEEE

Transactions on Information Theory, Volume: 44 Issue: 5 , Sept. 1998, Pages: 1897 -1905

[12] Burgett, S.; Koch, E.; Zhao, J.; "Copyright labeling of digitized image data", IEEE Communications Magazine, Volume: 36 Issue: 3 , March 1998, Pages:94-100

[13] Chen, B.; Sundberg, C.-E.W.; "Digital audio broadcasting in the FM band by means of contiguous band insertion and pre-canceling techniques," IEEE Transactions on Communications, Volume: 48 Issue: 10 , Oct. 2000, Pages: 1634 - 1637

[14] Chen, B.; Wornell, G.W.; "An information-theoretic approach to the design of robust digital watermarking systems," Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing, March 1999. Volume: 4 , Pages: 2061 -2064

[15] Chen, B.; Wornell, G.W.; "Quantization index modulation: a class of provably good methods for digital watermarking and information embedding," IEEE Transactions on Information Theory, Volume: 47, Issue: 4, May 2001, Pages: 1423 -1443.

[16] Chou, J.; Pradhan, S.S.; El Ghaoui, L.; Ramchandran, K.; "Watermarking based on duality with distributed source coding and robust optimization principles," Proceedings of International Conference on Image Processing, Volume: 1, Sept. 2000, Pages: 585 -588.

[17]Wolfgang, R.B.; Podilchuk, C.I.; Delp, E.J.; "Perceptual watermarks for digital images and video," Proceedings of the IEEE, Volume: 87, Issue: 7, July 1999, Pages: 1108-1126.

[18] Min Wu; Bede Liu; "Data hiding in image and video .I. Fundamental issues and solutions," IEEE Transactions on Image Processing, Vol. 12, Number 6, June 2003, Pages: 685- 695

[19] Min Wu; Yu, H.; Bede Liu; "Data hiding in image and video .II. Designs and applications," IEEE Transactions on Image Processing, Vol. 12, Number 6, June 2003, Pages: 696- 705.

[20]Hartung, F.; Kutter, M.; "Multimedia watermarking techniques," Proceedings of the IEEE , Volume: 87, Issue: 7 , 1999, Pages: 1079 -1107

[21] Katzenseisser, S.; Petitcolas, F.A.P; "Information Hiding Techniques forSteganography and Digital Watermarking," Artech House, Boston – London, 2000.

[22] Kirovski, D.; Malvar, H.; "Robust spread-spectrum audio watermarking,"Proceedings of 2001 IEEE International Conference on Acoustics, Speech, and Signal Processing, Volume: 3, May 2001, Pages: 1345 -1348

[23] Koch, E.; Zhao, J.; "Towards Robust and Hidden Image Copyright Labeling," in IEEE

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 3, 2013. ISSN: 2348-6600
Reference ID: IJCS-018 PAGE NO: 091-098

Workshop on Nonlinear Signal and Image Processing, 1995.

[24] Kutter, M; Petitcolas, F.A.P.; "A Fair Benchmark for Image Watermarking Systems," Security and Watermarking of Multimedia Contents, SPIE-3657:226-239, 1999.

[25] Langelaar, G.C.; Setyawan, I.; Lagendijk, R.L.; "Watermarking digital image and video data. A state-of-the-art overview," IEEE Signal Processing Magazine,Volume: 17, Issue: 5, Sept. 2000, Pages: 20-46

[26] Mintzer, F.; Braudaway, G.; "If one watermark is good, are more better?,"Proceedings Int. Conf. Acoustics, Speech, Signal Processing, Volume 4, Phoenix,AZ, March 1999.

din Muharemagic and Borko Furht,

[27]"Survey Of Watermarking Techniques AndApplications", Department of Computer science and Engineering, Florida Atlantic University.

[28] Andreja Samˇcovi´c, J´an Tur´an, "Attacks on Digital Wavelet Image watermarks", Journal of Electrical Engineering.

[29] Peining Taoa and Ahmet M. Eskicioglub, "A robust multiple watermarking scheme in the Discrete Wavelet Transform domain", The Graduate Center, The City University of New York.

[30] Baisa L. Gunjal, "An Overview Of Transform Domain Robust Digital Image Watermarking Algorithms", Department of Computer Engineering, Amrutvahini College of Engineering.

[31] Igor Djurovic, Srdjan Stankovic, and Ioannis Pitas," Digital watermarking in the fractional Fourier transformation domain", Journal of Network and Computer Applications (2001), page 167 – 173.

[32] Vaishali.S.Jabade, Dr.Sachin R.Gengaje "Literature Review of Wavelet based Digital Image Watermarking Techniques", International Journal of Computer Applications, Vol.31, No.1, October2011.

[33] P. Meerwald, A. Uhl, "A Survey of Wavelet-DomainWatermarking Algorithms", EI San Jose, CA, USA, 2001.

[34] Mohamed A. Suhail and Mohammad S. Obaidat, "Digital Watermarking-Based DCT and JPEG Model", IEEE Transactions OnInstrumentation and Measurement, Vol. 52, NO. 5, p.1640-1647, October 2003.

[35] Mahendra Kumar et. al., "Implementation of Different Non-Recursive FIR Band-pass filters using Fractional Fourier Transform" in proceedings of 4 th IEEE International Conference on Computational Intelligence and Communication Networks (CICN-2012), Mathura, 3-5 Nov. 2012.