DIGITAL WATERMARKING TECHNIQUE : A SURVEY

Mr.V.Vijayakumar
ME communication systems
KSR College of Engineering
Tiruchengode, India

Mrs.S.Poongodi M.E., (Ph.D)
Assistant Professor, Department of ECE
KSR College of Engineering
Tiruchengode, India

Dr.B.Kalavathi Ph.D.,
Proff & Head Dept of CSE
K S R Institute for Engg &Tech
Tiruchengode, India

***Abstract*: Everyday, tons of data is embedded on digital media or distributed over the internet. The data so distributed can easily be replicated without error, putting the rights of their owners at risk. Even when encrypted for distribution, data can easily be decrypted and copied. One way to discourage illegal duplication is to insert information known as watermark, into potentially vulnerable data in such a way that it is impossible to separate the watermark from the data. These challenges motivated researchers to carry out intense research in the field of watermarking. Watermarking defines Embedding a digital signal (audio, video or image) with information which cannot be removed easily is called digital watermarking in this paper we discuss various types of watermarking used to secure the data**

I. INTRODUCTION

Information hiding can be mainly divided into three processes cryptography, stenography and watermarks. Cryptography is the process of converting information to an unintelligible form so that only the authorized person with the key can decipher it. As many advances were made in the field of communication it became rather simple to decrypt a cipher text. Hence more sophisticated methods were designed to offer better security than what cryptography could offer. This led to the discovery of stenography and watermarking. Stenography is the process of hiding information over a cover object such that the hidden information cannot be perceived by the user. Thus even the existence of secret information is not known to the attacker. Watermarking is closely related to stenography, but in watermarking the hidden information is usually related to the cover object. Hence it is mainly used for copyright protection and owner authentication.The watermarking system is usually divided into three distinct steps, embedding, attack and detection. In embedding, an algorithm accepts the host and the data to be embedded and produces a watermarked signal. The watermarked signal is then transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. There are many possible attacks. Detection is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was not modified during transmission, then the watermark is still present and it can be extracted. If the signal is copied, then the information is also carried in the copy. The embedding takes place by manipulating the content of the digital data, which means the information is not embedded in the frame around the data, it is

carried with the signal itself. The original image and the desired watermark are embedded using one of the various schemes that are currently available. The obtained watermarked image is passed through a decoder in which usually a reverse process to that employed during the embedding stage is applied to retrieve the watermark. The different techniques differ in the way in which it embeds the watermark on to the cover object.

A secret key is used during the embedding and the extraction process in order to prevent illegal access to the watermark.

A. Requirements

The major requirements of digital watermarking are:

a) *Transparency:*

The embedded watermark should not degrade the original image. If visible distortions are introduced in the image, it creates suspicion and makes life ease for the attacker .It also degrades the commercial value of the image.

b) *Robustness*

This is by far the most important requirement of a watermark. There are various attacks, unintentional (cropping, compression, scaling) and unintentional attacks which are aimed at destroying the watermark. So, the embedded watermark should be such that it is invariant to various such attacks.

c) *Capacity or Data Load*:

This quantity describes the maximum amount of data that can be embedded into the image to ensure proper retrieval of the water during extraction.

II. CLASSIFICATIONS OF WATERMARKING

A. *Visible*

The watermark is visible which can be a text or a logo used to identify the owner.Any text or logo to verify or hide content

$Fw = (1-\alpha) F+ \alpha*W$ [6]

Fw = Watermarked Image

α = constant; $0<=\alpha<=1$,

IF $\alpha=0$ No watermark,

If $\alpha=1$ watermark present

F =original image

W =watermark

B. *Invisible*

The watermark is embedded into the image in such a way that it cannot be perceived by human eye. It is used to protect the image authentication and prevent it from being copied.Invisible watermark can be further divided into three types,

a) *Robust Watermarks*

Invisible watermark cannot be manipulated without disturbing the host signal. This is by far the most important requirement of a watermark. There are various attacks, unintentional (cropping, compression, scaling) and unintentional attacks which are aimed at destroying the watermark. So, the embedded watermark should be such that it is invariant to various such attacks. They are designed to resist any manipulations that may be encountered. All applications where security is the main issue use robust watermarks.

b) *Fragile Watermarks*

They are designed with very low robustness. They are used to check the integrity of objects.

c) *Public and Private Watermark*

They are differentiated in accordance with the secrecy requirements for the key used to embed and retrieve watermarks. If the original image is not known during the detection process then it is called a public or a blind watermark and if the original image is known it is called a non-blind watermark or a private watermark.

III. WATERMARKING TECHNIQUES

A. *Spatial Domain Techniques*

Spatial domain watermarking slightly modifies the pixels of one or two randomly selected subsets of an image. Modifications might include flipping the low-order bit of each pixel. However, this technique is not reliable when subjected to normal media operations such as filtering or lossy compression

a) *Least Significant Bit Coding (LSB)*

LSB coding is one of the earliest methods. It can be applied to any form of watermarking. In this methodthe LSB of the carrier signal is substituted with the watermark. The bits are embedded in a sequencewhich acts as the key. In order to retrieve it back this sequence should be known. The watermarkencoder first selects a subset of pixel values on which the watermark has to be embedded. It thenembeds the information on the LSBs of the pixels from this subset. LSB coding is a very simple techniquebut the robustness of the watermark will be too low. With LSB coding almost always the watermarkcannot be retrieved without a noise component.

b) *Predictive Coding Schemes*

Predictive coding scheme was proposed by Matsui and Tanaka in [8] for gray scale images. In thismethod the correlation between adjacent pixels are exploited. A set of pixels where the watermark hasto be embedded is chosen and alternate pixels are replaced by the difference between the adjacentpixels. This can be further improved by adding a constant to all the differences. A cipher key is createdwhich enables the retrieval of the embedded watermark at the receiver. This is much more robust when compared to LSB coding.

c) *Correlation-Based Techniques*

In this method a pseudo random noise with a pattern W(x, y) is added to an image [4] [11], according to the equation I (x, y) I (x, y) k *W(x, y) where,

I(x, y) = Watermarked image.

I(x, y)=Original image

Sk= gain factor

Increasing k increases the robustness of the watermark at the expense of the quality of the watermarked image. At the decoder the correlation between the random noise and the image is found out and if the value exceeds a certain threshold value the watermark is detected else it is not.

d) *Patchwork Techniques*

In patchwork watermarking, the image is divided into two subsets. One feature or an operation is chosen and it is applied to these two subsets in the opposite direction. For instance if one subset is increased by a factor k, the other subset will be

decreased by the same amount. If a[i] is the value of the sample at I in subset 'A' which is increased and b*i+ is the value of the sample in the subset 'B' whose value is decreased, then the difference between the two subsets would intuitively result in

$\Sigma(a[i]-b[i]) = 2N$ for watermarked images $1<=N<=\infty = 0$ otherwise gain factor

B. Frequency-Domain Technologies

Compared to spatial-domain watermark, watermark in frequency domain is more robust and compatible to popular image compression standards. Thus frequency-domain watermarking obtains much more attention. To embed a watermark, a frequency transformation is applied to the host data. Then, modifications are made to the transform coefficients. Possible frequency image transformations include the Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and others. The first efficient watermarking scheme was introduced by Koch et al. In their method, the image is first divided into square blocks of size 8x8 for DCT computation.

A pair of mid-frequency coefficients is chosen for modification from 12 predetermined pairs. Bors and Pitas developed a method that modifies DCT coefficients satisfying a block site selection constraint. After dividing the image into blocks of size 8x8, certain blocks are selected based on a Gaussian network classifier decision. The middle range frequency DCT coefficients are then modified, using either a linear DCT constraint or a circular DCT detection region. A DCT domain watermarking technique based on the frequency masking of DCT blocks was introduced by Swanson. Cox developed the first frequency-domain watermarking scheme. After that a lot of watermarking algorithms in frequency domain have been proposed.

Most frequency-domain algorithms make use of the spread spectrum communication technique. By using a bandwidth larger than required to transmit the signal, we can keep the SNR at each frequency band small enough, even the total power transmitted is very large. When information on several bands is lost, the transmitted signal can still being recovered by the rest ones. The spread spectrum watermarking schemes are the use of spread spectrum communication in digital watermarking. Similar to that in communication, spread spectrum watermarking schemes embed watermarks in the whole host image. The watermark is distributed among the whole frequency band. To destroy the watermark, one has to add noise with sufficiently large amplitude, which will heavily degrade the quality of watermarked image and be considered as an unsuccessful attack.

C. *Wavelet-domain Domain Technologies*

The new JPEG2000 standard has adopted a new technique, the wavelet transform. Though this standard has not been widely used yet, any new watermarking algorithm that intends to survive in the future should get along with it. Here come the watermarking schemes based on wavelet transform. The difference between different wavelet domain methods depends on the way the watermark is weighted. The reason for this is to reduce the presence of visual artifacts.

The DWT (Discrete Wavelet Transform) separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components.The process can then be repeated to computes multiple "scale" wavelet decomposition, as in the 2 scale wavelet transforms shown in figure

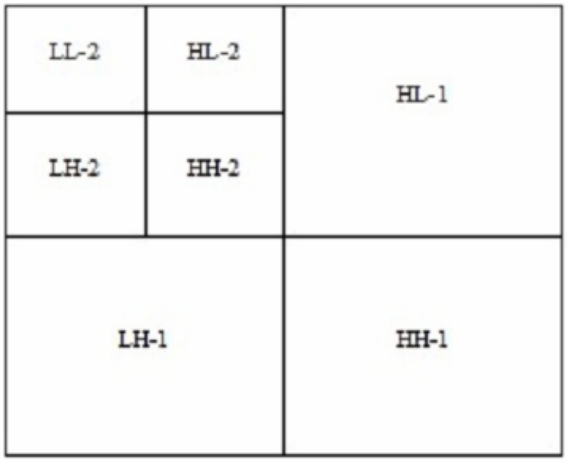

Figure: 2- scale wavelet transform

One of the many advantages over the wavelet transform is that that it is believed to more accurately model aspects of the HVS as compared to the FFT or DCT, Higher compression ratio Avoid blocking artifacts Allows good localization both in time and spatial frequency domain. Transformation of the whole image introduces inherent scalingThis allows us to use higher energy watermarks in regions that the HVS is known to be less sensitive to, such as the high resolution detail bands {LH, HL, HH) Embedding.

IV. QUANTIZATION TECHNIQUE

Fernando Pérez-González, Carlos Mosquera, Mauro Barni and Andrea Abrardo proposed a novel quantization-based data-hiding method, called Rational Dither Modulation (RDM) [1][12], is presented. This method retains most of the simplicity of the conventional dither modulation (DM) scheme, which is largely vulnerable to amplitude scaling and modifies it in such a way that the result becomes invariant to gain attacks. RDM is based on using again-invariant adaptive quantization step-size at both embedder and decoder. This causes the watermarked signal to be asymptotically stationary. Mathematical tools are used to determine the stationary probability density function, which is later used to assess the performance of RDM in Gaussian channels. RDM is compared with improved spread-spectrum methods, showing that the former can achieve much higher rates for the same bit error probability. Finally, a broader class of methods, that extends gain-in variance to quantization index modulation (QIM) methods, is also presented. The current RDM proposal has proven its merits in a highly theoretical context, which is largely independent of the host nature; needless to say, a considerable amount of work is necessary to tune RDM to the demands of practical applications. For instance, our assumption of a stationary host is far from holding with real signals. A partial relief would be to pseudorandomly permuting the host samples to create a “pseudo-stationary” signal, but in turn, this may affect RDM’s resilience to slow-varying gains. Other open implementation issues that need be taken into consideration include the use of varying embedding strengths, practical effects of the embedding PAR, the selection of the quantization step, and the initialization of the function Besides the practical implementation of RDM with multimedia signals, ongoing research covers the design of the function controlling the step size, with the possible inclusion of weighted norms, the combination of RDM with distortion compensation and channel coding, and the adaptation of RDM to deal with faster gain variations.

Brian Chenand Gregory W. Wornell , proposed a new method to avoid the problem of embedding one signal (e.g., a digital watermark), within another “host” signal to form a third, “composite” signal.

The embedding is designed to achieve efficient tradeoffs among the three conflicting goals of maximizing information-embedding rate, minimizing

distortion between the host signal and composite signal, and maximizing the robustness of the embedding, introduce new classes of embedding methods, termed quantization index modulation (QIM) and distortion-compensated QIM (DC-QIM), and develop convenient realizations in the form of what we refer to as dither modulation. Using deterministic models to evaluate digital watermarking methods, we show that QIM is "provably good" against arbitrary bounded and fully informed attacks, which arise in several copyright applications, and in particular, it achieves provably better rate distortion–robustness tradeoffs than currently popular spread-spectrum and low-bit(s) modulation methods of probabilistic models, DC-QIM is optimal (capacity-achieving) and regular QIM is near-optimal. These include both additive white Gaussian noise (AWGN) channels, which may be good models for hybrid transmission applications such as digital audio broadcasting, and mean-square-error-constrained attack channels that model private-key watermarking applications.

V. SPREAD SPECTRUM SCHEMES

Spread Spectrum schemes represent an early type of embedding method. It adds a sequence of pseudo-random signals into the host signals to form the watermarked data. According to how the watermark is added into the host contents, the spread spectrum schemes can be further subdivided into the additive and multiplicative spread spectrum (ASS and MSS) schemes. The signals are usually embedded into the perceptually important components of the host image to achieve a balance of perceptual quality and robustness. At the detector, the original image should be available to cancel the watermarked image to extract the embedded signals. The extracted signals are then correlated with a predefined pattern for validation. The detection that requires the original data is called private detection.

For many prospective applications, this requirement is sometimes quite astringent. Later, Piva andZeng designed [10][11] the blind detection techniques which require no presence of the original hosts. The blind detection employs the statistical inference to differentiate between the unwatermarked and the watermarked contents. In these blind schemes, the original work is taken as the noise interfering with the watermarking detection. The host interference should not be a problem if it is available at the detector or decoder. For many prospective applications, this is not the case.

This situation can be further improved by designing a better embedded or an optimum detector or decoder. The first approach utilizes the host information at the embedded, whereas the second, it improves the performance of spread spectrum watermarking schemes by exploiting the probability distribution function (pdf) of the host signals at the detector or decoder.

A. *Side-informed embedded*

Cox model as the watermarking as communication with side information, and proposed to utilize the host information in the embedding process. The idea was that instead of treating the cover data as noise added to the embedded signals, it could be taken as side information to improve both the fidelity and the detection rate by means of an appropriate perceptual mask and the knowledge of the detector. First Approach: perceptual models.

Using a global embedding strength results in the perceptible local distortion. Thus many authors proposed to locally bound the maximum embedding strength by the Human Perceptual Systems (HPS) to

achieve the maximum allowable perceptual distortion and robustness Podilchuk and Zeng utilized the Watson's perceptual model to embed the perceptually-shaped signals into the host contents.

The Watson's model, initially designed for image compression, includes three Major perceptual functions namely frequency, luminance and contrast masking. Tuned with this model, the image quality is much improved, especially at the smooth regions of the images that are more sensitive to the image manipulations. Since the embedding strength can be locally bounded to achieve a distortion of one Just Noticeable Difference (JND) level, a higher robustness can also be achieved a acceptable image quality. The idea of employing perceptual models is further extended to the video watermarking. In the authors presented a perceptual model in the DFT domain. In addition to the masking criterion, the model also discriminates the different perceptual effects of edge and texture.

The model investigated in exploits the temporal and the frequency masking to guarantee that the embedded watermark is inaudible and robust. Similar ideas of using perceptual models to improve both the perceptual quality and the robustness. Second approach: side-informed techniques with the knowledge of the structure of the detector (a kind of reverse engineering to compute the desired embedding signals.) Based on Cox's frame work aside-informed embedder is designed according to a specified criterion, such as maximizing the correlation coefficient or maximizing the robustness.

Since both the correlation coefficient and the robustness are related to the host contents, the embedded signals thus depend on the host contents. In order to achieve the best perceptual quality at a fixed robustness, Miller et al. presented an iterative embedding algorithm that builds the watermark by adding perceptually shaped components until the desired robustness is achieved. Similar ideas are also formulated however; these side-informed schemes do not handle the important issue of how to insert the watermark to minimize the error rate at a fixed distortion level. Improved Spread Spectrum (ISS) scheme proposed also exploits the knowledge of host contents by projecting them into the watermark, and this projected host interference is then compensated in the embedding process. The authors claimed that the performance measured in probabilities of errors could be improved by tens of magnitudes. This is not strange since ISS is quantization scheme with only two quantizers. The second approach succeeds is removing (or partially removing) the host interference and thus improves the system's performance.

Comparison of the above two approaches: The embedder of the first approach does not require the knowledge of the detector's structure, whereas the second instance, Miller's maximum robustness assumes that the detection statistic is the correlation coefficient. For ISS, the detector is a simple linear correlator. The second approach excels the first performance since it offers a property of host interference rejection. For instance, ISS can have a complete rejection of the host interference. It also due to the host interference property and it is difficult to implement the perceptual analysis for the second approach since the embedded signal relies on the summary of the host features.

Informed detector: The detector has to be informed the host pdf (and the embedding strengths for some cases, i.e., optimum detectors.) Hernande designed an optimum detector for ASS watermarking

in the Discrete Cosine Transform (DCT) domain. Their detector exploits the fact that the host's low- and mid-frequency DCT coefficients can be better model by Generalized Gaussian Distributions (GGD).Briassouli exploited the fact that Cauchy pdf also gives a better approximation of the low- and mid-frequency DCT coefficients, and designed a locally optimum Cauchy nonlinear detector. According to their comparison of results, it is hard to say whether Cauchy model yields a better performance than GGD model.In truth, GGD models are much more popular modeling than DCT coefficients. For MSS, Oostveenand Barni modeled the magnitudes of Discrete Fourier Transform (DFT) coefficients through a Weibull pdf and investigated the optimum detection in the DFT domain. For multiplicative watermarking in the DCT domain, Cheng derived the structure of its optimum detector. In this paper, Cheng also derived a class of generalized correlators. Unlike the previous Universally Most Powerful (UMP) detectors, this class of detectors is derived from the Locally Optimal (LO) or Locally Most Powerful (LMP) tests. Recently, an optimum decoder for information hiding in the Laplacian Discrete Wavelet Transform (DWT) data was proposed. All the above optimum detectors are derived under the hypothesis that no attack is mounted on the host contents.

VI. APPLICATIONS

Copyright Protection: This is by far the most prominent application of watermarks. With tons of images being exchanged over insecure networks every day, copyright protection becomes a very important issue. Watermarking an image will prevent redistribution of copyrighted images. Authentication: Sometimes the ownership of the contents has to be verified. This can be done by embedding a watermark and providing the owner with a private key which gives him an access to the message. ID cards, ATM cards, credit cards are all examples of documents which require authentication. [2]

Broadcast Monitoring: As the name suggests broadcast monitoring is used to verify the programs broadcasted on TV or radio. It especially helps the advertising companies to see if their advertisements appeared for the right duration or not. [3]

Content Labeling: Watermarks can be used to give more information about the cover object. This process is named content labeling. Tamper Detection: Fragile watermarks can be used to detect tampering in an image. If the fragile watermark is degraded in any way then we can say that the image or document in question has been tampered.

Digital Fingerprinting: This is a process used to detect the owner of the content. Every fingerprint will be unique to the owner. [3]

Content protection: In this process the content stamped with a visible watermark that is very difficult to remove so that it can be publicly and freely distributed [2] watermark.

VII. CONCLUSIONS

In this paper, we have introduced some important basic concepts in digital watermarking, including its foundation, properties, requirements and applications, After that, common watermarking techniques are reviewed; schemes in spatial domain, frequency domain and wavelet domain are introduced with analysis of pros and cons, in terms of imperceptibility, robustness, implementation complexity etc., for each domain. Compare the above discussion the wavelet domain give better result over spatial and frequency domain

REFERENCES

[1] Fernando Pérez-González, Carlos Mosquera, Mauro Barni, and Andrea Abrardo "Rational Dither Modulation: A High-Rate Data-Hiding Method Invariant to Gain Attacks "IEEE transactions on signal processing, vol. 53, no. 10, October 2005.

[2] R. Popa, "An analysis of steganographic techniques", The Politehnica University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering, Website: http://ad.informatik.uni-freiburg.de/mitarbeiter/will/dlib_bookmarks/digital-watermarking/popa/popa.pdf, 1998.

[3] P. Vidyasagar, S. Han and E. Chang. "A survey of digital image watermarking techniques", 3rd IEEE International Conference on Industrial Informatics (INDIN 2005), edited by T. Dillon, X. Yu. And E. Chang, pp. 495-502, Perth, Western Australia, 2005.

[4] J. Dugelay and S. Roche, "A Survey of Current Watermarking Techniques" in Information Techniques for Steganography and Digital Watermarking, S.C. Katzenbeisser et al, Eds. Northwood, MA: Artec House, pp. 121-145, Dec. 1999.

[5] I. J. Cox, et al, "Digital watermarking and steganography" (Second Edition), Morgan Kaufmann, 2008.

[6] K. R. Rao and P. Yip, "Discrete Cosine Transform: Properties, Algorithms, Advantages, Applications", Academic Press, Massachusetts, 1990.

[7] Brian Chenand Gregory W. Wornell "Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding" IEEE transactions on signal processing 2001.

[8] T. C. Lin and C. M. Lin, "Wavelet based copyright protection scheme for digital images based on local features", Information Sciences: an International Journal, Vol. 179, Sept. 2009.

[9] Jidong zhong and shangteng huang "An enhanced multiplicative spread spectrum watermarking scheme" IEEE transations on circuits and systems for viedo technology, vol 16, no.12, December 2006.

[10] Amir Valizadeh, and Z. Jane Wang,An "Improved Multiplicative Spread Spectrum Embedding Scheme for Data Hiding" IEEE transactions on information forensics and security, vol. 7, no. 4, august 2012.

[11] I.J. Cox, M.L. Miller, J.M.G. Linnartz and T. Kalker, "A Review of Watermarking Principles and Practices" in Digital Signal Processing for Multimedia Systems, K.K. Parhi and T. Nishitani, New York, Marcel Dekker, New York, pp. 461-482, 1999.s

[12] Nima Khademi Kalantari and Seyed Mohammad Ahadi "A Logarithmic Quantization Index Modulation for Perceptually Better Data Hiding" IEEE transactions on image processing, vol. 19, no. 6, June 2010.