Digital Watermarking – A Multidisciplinary Approach

L. Venkateswarlu[1], Associate Professor and Dr. N V Rao[2], Professor,
[1]CVR College of Engineering, Department of CSE, Ibrahimpatan, R.R. District, A.P., India
Email: venkatlendale@gmail.com,
[2]CVR College of Engineering, Department of CSE, Ibrahimpatan, R.R. District, A.P., India
Email:nvr@ieee.org

Abstract: **For the last six decades, Digital Watermarking, as an art of hiding information in a cover or host image has drawn much attention of researchers from academic institutions and industry. Especially after 1990, a good number of the publications in various Journals and seminars proves the fact that the issue is considered in various disciplines with common goals and applications such as authentication and copyright protection in the era of internet. Many issues such as embedding in transformation domain, attack models, capacity issues, and applications have been addressed mainly because of its multidisciplinary nature. This paper briefly brings out the issue of watermarking in the perspective of different disciplines like Communications, Information Theory, Signal Processing, Human Visual system, Coding Theory, Cryptography, Mathematics and Statistics.**

Index Terms**: Watermarking, Communication theory, Information theory, capacity of watermark**

I. INTRODUCTION

Almost for the last six decades, research and experimental work on digital watermarking has been going on, as evidenced by a good number of publications in international journals and conference proceedings. Majority of the conferences held every year on multimedia, signal processing, communications and other allied themes have been organizing regularly a special track on this watermarking under multimedia security. Academic institutions and research organizations tried to evolve a theory for watermarking with theoretical models and limits. It is observed that a few thousands of papers have been published on various issues on watermarking. Steganography or Information hiding has emerged as a potential research area having ample applications, very relevant in the present era of internet through which digital transmission has been made very easy. These potential applications such as copyright protection for digital media, watermarking, fingerprinting, steganography, and data embedding, authentication of ownership, buyer-seller information etc. are one-way tools for Digital rights management in the internet era. Information hiding, or steganography, has a broad range of applications from copyright protection and transaction tracking, to broadcast monitoring, data integrity, authentication and fingerprinting. Thus, watermarking has become a major and significant research activity in multimedia processing, leading to the standardization of JPEG-2000, MPEG-4, and digital video disks etc.[1].

II. DEVELOPMENT OF WATERMARKING

The development of Watermarking in theory and Practice can be noticed by the following factors.
Even though the concept of electronic watermark was initiated in 1940's, the actual momentum gained in 1990's. Since then the number of papers published on the subject are exponentially growing. By this time a few thousands of papers are made available in journals and conferences. Professional Societies under IEEE have been publishing papers and special issues in their magazines and Transactions such as Communications Magazine, IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, Signal processing Magazine, Multimedia, Security and Privacy, Computer, Proceeding of IEEE, Transactions on Image Processing. Transactions on Instrumentation and measurement, Information Theory etc. Some of these publications regularly carry featured articles on Watermarking. In addition, some issues of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS and of the PROCEEDINGS OF THE IEEE, IEEE Signal Processing were devoted to copyright and privacy protection or Digital Rights Management (DRM). The other publishers/ magazines include ACM, IEICE, Electronic Imaging, EURASIP, and ELSEVIER. International Workshops on Information Hiding have been held regularly since 1996, with special sessions on digital watermarking or Information Hiding for DRM.

 DOI:10.32377/cvrjst0504

2.1 First 50 years of electronic watermarking(1954 – 2004) [4]:

The very first work on watermarking can be traced to the patent by Emil Hembrooke, "Identification of sound and like signals", US Patent 3,004,104 Filed in 1954, issued in 1961. Since then for the first fifty years, a very good and promising trend has been observed especially in the International scene. During the next ten years there had been a momentum significantly in Indian universities in terms of published papers**.** Cox et. al [4] observed an exponential growth since 1995 at an average of 200 published papers per year in many reputed Journals and Magazines mentioned earlier. Organizational support is also visible as Universities and companies like IBM, HP continued a continuous research towards product standardization of watermarking.

2.2 Generic Information –Hiding Problem:

In general steganography or Information Hiding problem can be stated as a process in which a message is to be embedded in a host data set, and the resulting data may face data processing operations known as attacks. These attacks always try for the removal of information hidden. Watermarking is regarded as a subset of Steganography, where the information to be hidden in the cover is related to the cover. Hidden information is called Watermark. A text, image or an audio clip , logo can be taken as a watermark. The essential features of any watermark are stated below.

Fidelity: The degree of degradation in perception or loss of visual quality due to the insertion of watermark.

Robustness: The level of immunity against all forms of attacks to remove the traces of watermark (intentional and non-intentional manipulations).

Payload: This is otherwise known as capacity of watermark, an indication of how much can be added as the watermark to the cover under constraints.

Security: Watermark should be secure enough, depending on the application.

III. Watermarking as truly interdisciplinary:

By carefully observing the research and experiments carried out in the field of digital watermarking, one can obviously notice that it is truly interdisciplinary.

The disciplines that emerge in the study of watermarking are:

Information Theory and Communications Theory Image and signal processing, compression, Transforms with cryptography, Game Theory, Coding Theory, Detection and Estimation Theory,
Cryptography and Protocol Design, Visual perception theory, Mathematics and Statistics.

Perhaps a key reason for the rapid work and enthusiasm in this field is the fact that digital watermarking is inherently a multi-disciplinary topic that builds on developments in diverse subjects but for a common objective.

3.1 Watermarking and communications:

Even a general examination of any watermarking scheme reveals the idea that there is a significant similarity between the watermarking and communications. Just let us see how a communication system works. Specified information is introduced into a communication channel, which is also known as communication medium. The transmitted information is received at the destination by the receiver. But the main goal of communications is to receive the transmitted information with high reliability, without much distortion. Similarly watermark is additional information embedded in a multimedia like an image (communication Channel) and transmitted. It is to be extracted at the receiver end without any quality degradation. Both need robustness and reliability. The case of attacks on watermarked media is viewed as communications in a hostile environment such as transmission errors and noise. Thus in simple terms, this common model considers watermarking as a form of communications, in which the original medium is a communication channel and watermark is a modulated signal that contains the message. This analogy has been shown in Fig:1.

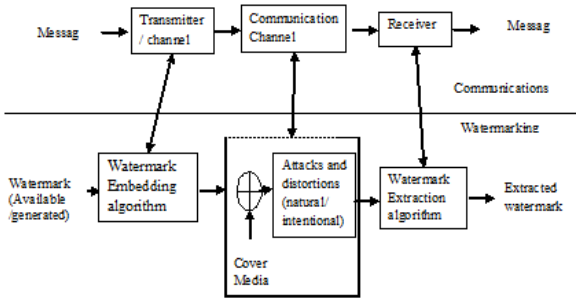

Fig 1: Analogy between communications and water marking

A few models have been developed in the study of theoretic analysis of watermarking. Signal Processing and communication concepts were used initially. In the Digital Rights Management, watermarking of digital media is considered as a potential application for copyright Protection. So Fidelity of the cover is a factor for the evaluation of any algorithm for embedding. So Fidelity, robustness and capacity are the serious requirements of any watermark.

Spread Spectrum methods:

The initial models of watermark considered spread spectrum techniques for watermarking algorithms. Watermark spreads over the image for robustness. In communications, Spread spectrum systems are considered as they transmit very little power within any single frequency. They have excellent interference and anti-jamming properties. These properties are quite suitable for WM applications. Many research papers are published on Spread spectrum Image watermarking.

In spread spectrum methods, the message is scattered across the image making it difficult for image manipulations like cropping, rotation and other basic image manipulation techniques to remove or manipulate the hidden watermark. This is also somewhat resistant to statistical analysis of steganographic images because it gives it the impression of noise in an image. Here mention is to be made about Patchwork from IBM which is a tool to scatter hidden information based on statistical distribution of intensity values in the given image.

It is not out of context to remember the inventors of Spread Spectrum communications. Hedy Lamarr, then the international beauty icon, along with co-inventor George Anthiel, developed a "Secret Communications System" to help combat the Nazis in World War II. By manipulating radio frequencies at irregular intervals between transmission and reception, the invention formed an unbreakable code to prevent classified messages from being intercepted by enemy personnel. On August 11, 1942, U.S. Patent 2,292,387 was granted to them.

Communications with side information:

In [3], Cox *et al.* introduce the paradigm of watermarking as a coded communication system with side information at the embedder. Based on this paradigm, and by considering a statistical model for attacks, some detection rules are proposed for detecting the presence of watermarks in images. Capacity or load of a watermark is the amount of information a cover can hold within the constraints mentioned above. So in order to improve capacity, watermarking is modeled as a form of communication with side information. In this, the cover is considered as side information and is available to transmitter or receiver or to both. It is to be noted that, in this model, cover is not considered as a noise.

In these applications of watermarking information is hidden within a host data set and is to be reliably communicated to a receiver. The cover or host data set is corrupted in a covert way, and is not easily detectable by a casual analysis. There may be attacks to destroy this stegno information. For this end, additional distortion to the data set is introduced. Side information usually in the form of cryptographic keys / information about the cover signal may be available to the information hider or to the decoder or to both.

The Parallel Between Communication and Information Hiding Systems [1,6]:

Communication Perspective	*Information Hiding*
Encoder-Decoder	Embedder-Detector or extraction of Watermark
Side information	Host or Cover image
Channel noise	Attacks to removal or manipulations
Power constraints	Perceptual distortion Limits
Signal to noise ratio (SNR)	Embedding distortion To attack distortion (WNR)

A communication analogy for watermarking has helped to answer the fundamental questions**:** a) Where should most of the watermark energy be placed so that it is robust to perceptual coding; b) How much information can reliably be hidden. Watermarking is greatly benefited from the richness of the communication paradigm[1]. This has given an ample opportunity for communication engineers to view deeply into the theory and applications of digital watermarking

3.2 Information Theory: [1,6]

Information theory has been a valuable tool in studying watermarking problems. Publications include a definition of watermarking capacity or computation of payload for watermarking hosts, watermarking security, etc.. Many mathematical models and tools form the basis of Information theoretic studies of watermarks are carried out on the basis of mathematical models. From Communications point of view, watermarking has been considered as a way of communication, in which the cover image is viewed as a communications channel to send messages. So traditional Information theory is used to formulate and solve watermarking capacity issues. Here capacity of watermark is to estimate how much can be embedded. Shannon's Formula is the basis of these Information Theoretic studies on Capacity of watermarks. Information hiding can be seen as an application of "dirty paper" coding, in multi-user communications [2]. Thus, the role of information theory in Watermarking is so fundamental that it becomes the basis in characterizing the fundamental limits of watermarking systems and in guiding the development of optimal

 DOI:10.32377/cvrjst0504

watermark embedding algorithms and optimal attacks [1]. As already stated, Watermarking can be viewed as a communication problem with side information. This side information may be in the form of the host signal and/or a cryptographic key and is available at the encoder and the decoder. This problem is mathematically defined by distortion constraints, by statistical models for the host signal, and by the information available in the game among the information hider, the attacker, and the decoder. In particular, information theory explains why the performance of watermark decoders that do not have access to the host signal may surprisingly be as good as the performance of decoders that know the host signal [1].

Watermarking security analysis based on information theory :[5]

From an information theory point of view, Watermarking security is quantified via the equivocation and mutual information between Secret and public parameters as per the design of watermarking. Information theory tools are used to estimate the measure of information leakage for a variety of scenarios and also the tradeoff between different requirements of watermarking: robustness, imperceptibility and security. This analysis in the watermarking in transformation domain has been carried out to improve the visual quality of watermarked image and robustness of watermark. [5]

3.3 Human Perception:

Another approach similar to information theory is based on human perception . Perceptual models take into consideration the human audio-visual system. In some watermarking techniques both information theoretic and perceptuality criteria has been proposed, in which perceptually significant features are selected for watermark insertion. The just noticeable difference criterion is usually used for this purpose. The algorithms in transformation domain are tried in this context.

3.4 Capacity of watermark and Game Theory:[1,9]

Hiding capacity is evaluated for upper-bound of the rates of reliable transmission. It also objectively quantifies the fundamental tradeoff among three quantities: information-hiding rates that can be practically achievable, levels of distortion that can be tolerated for the information hider and the attacker. The hiding capacity or the pay load of watermark is modeled as the result of a game between the information hider and the attacker. The optimal attack strategy is the solution of a particular rate-distortion problem, and the optimal hiding strategy is the solution to a channel-coding problem. The hiding capacity is derived by extending the Gel'fand–Pinsker theory of communication with side information at the encoder. Many extensions to this study are made such as the presence of distortion constraints, side information at the decoder, and unknown communication channel **[1].**

O'Sullivan *et al* [9] first formulated the watermarking scenario as a game played between an information hider and an attacker. The mutual information between the input and output of the attack channel was taken as the cost function of the game. The attacker tries to minimize this cost while the hider tries to maximize it. The upper bound on this mutual information is the data hiding capacity. The main result of the work is the insight that the best attack approach is equivalent to the most efficient data compression possible subject to a distortion constraint, and the optimal information hiding strategy corresponds to optimal channel coding in which the attacker determines the channel characteristics [9].

In these techniques the entire watermarking process is considered to be a game and optimal joint data hiding and attack strategies are derived. The watermark and attacker are both assumed to be at "peak" performance. Expressions for the possible data hiding rate are derived and analyzed to gain perspective as to the potential of the technology.

Modeling of attacks or distortions:

Watermarking researchers have modeled all possible distortions between the stages of embedding and detection, and drawn metrics for quality measures. These attacks include not only noise (Natural) but also intentional attacks such as modifications, geometric transforms and compression.

Mutual Information Theory (MI):

It is a basic concept taken from information theory. It is a measure of the statistical dependence or correlation between two given random variables. It is a measure of common information between them. So It is appropriately used to see the correlation between cover images: original and watermarked. And also watermark: original and extracted.

In Watermarking research, watermark detection using Mutual Information detector has been used effectively, and it has been proved to be efficient as it incorporates higher order statistics of non-Gaussian image distribution. In addition Geometric invariants such as translation, rotation and scaling are improved. [8]

Watermark extraction becomes even impossible at times when attacks or distortions are powerful.

This residual information is named as the scar and it is used to confirm the existence of an attacked watermark. However, it is possible only when the mutual information between the embedded message and

the attacked copies is above a certain threshold. Scar is made use of by measuring the correlation between the attacked watermark and the original one. The watermarking scar can be measured using mutual information between the embedded watermark and the marked/attacked copies.[7]

3.5 Statistics in Watermarking:

Natural images have statistics and any modifications to original or natural brings an observable change in their statistics. This factor is made use of in detecting a watermark in a cover image [10]. Experimental Investigation has been made to study if stego images containing embedded information are statistically natural and it is found that the hidden images disturb the fundamental statistical features of original image. This study is used to detect watermarks in images. It is shown that, within multi-scale, multi-orientation image decompositions such as wavelets, first- and higher-order magnitude and phase statistics are relatively consistent across a broad range of images, but are disturbed by the presence of embedded hidden messages. Thus higher order statistics is used to detect hidden steganographic messages in digital images [11].

Assessing the quality of images is a key step in the determination of fidelity of watermarking, and is an essential requirement for acceptance . Objective assessment is done through statistical measures like MSE (Mean square Error), RMSE (Root Mean square Error), SNR, PSNR, Structural Index etc.

3.6 Signal Processing and Mathematical Transformations in watermarking algorithms:

There was initial work in the use of basic digital signal processing (DSP) strategies for data hiding. In fact many papers have been published in IEEE transactions of Image Processing on image watermarking, a publication of Signal Processing Society of IEEE. An image can be viewed as a signal and watermark is considered as a message signal transmitted through a cover signal.

In Signal Processing, many transformations are used for analysis. Fourier, Trigonometric and Wavelet are very prominent among them. For robustness of watermarking, frequency or transformation domain has been suggested. Many transformations have been experimented for embedding watermark. In the literature, more than 20 transforms are used for watermark fusion: DCT, DST,DFT, SVD, Arnold, DWT (Bi- orthogonal, packet decomposition, stationary wavelet, second generation wavelet, dual tree wavelets, curvelets, ridgelets, chirplets, noiselets, shearlets), Hadamard transformation, KL transformations, Walsh 2D transformation, Z transformation, Genetic transformation, Binomial transformation, Slant transformation, Affain Transforms, Back projection and tensor transformation, Bandlet transformation, Radon transformation, Counterlet transformation). In addition, dual transformation domains are used for better robustness. They are DWT + DCT, DWT+SVD, DWT+DCT+SVD.

Among them DWT and its variants like bi orthogonal wavelets are more promising. Signal processing concepts can be aptly used in the theory of Watermarking. It is to be noted that Signal Processing society of IEEE publishes *Transactions of Image Processing*, which is considered as the leading research journal on Image Processing. This publication also has a regular feature on Multimedia security that contains research articles on watermarking.

3.7 Image Processing Techniques:

Much research work in watermarking was done in the media of digital images. Majority of papers published are pertaining to Image watermarking. The human Perception is limited by not differentiating the embedded image in an image. This was better used in watermarking algorithms development and experimentation. Embedding watermark in a cover image can be considered as fusion of images. Image Compression is an attack that can diminish the quality and hence the criterion of watermarking is that it is resistant to compression.

The above current scenario clearly explains the role of Signal Processing, Image Processing, Mathematical Transformations in the study of Watermarking.

SCOPE FOR FURTHER RESEARCH

Any research should lead to a useful tool for the society. Digital watermarking as viewed from multi disciplinary perspective provides ample opportunities for wider research and applications based on sound theoretic principles of communications and information theory. Hence the following are expected from the future research.

1. Watermarking research should converge towards a standard tool for authentication.
2. A hardware realization is required for automatic finger printing for multimedia security and authentication.

 DOI:10.32377/cvrjst0504

REFERENCES

[1] Pierre Moulin, The role of information theory in watermarking and its application to image watermarking , Signal Processing, Volume 81, Issue 6, June 2001, pp.1121–1139.

[2] M. H. M. Costa, "Writing on dirty paper," *IEEE Trans. Inf. Theory*, vol. 29, no. 3, pp. 439–441, May 1983.

[3] I. J. Cox, M. L. Miller, and A. L. McKellips, "Watermarking as communications with side information," *Proc. IEEE*, vol. 87, no. 7, pp. 1127–1141, Jul. 1999.

[4] J. Cox, M. L. Miller , The First 50 years of electronic watermarking. Journal of Applied Signal Processing , 2002, 2,pp. 126-132., 2002.

[5] Fazli, A.R. **,** Watermarking security analysis based on information theory**,** Signal and Image Processing Applications (ICSIPA), 2011 IEEE International Conference on , Kuala Lumpur ,16-18 Nov. 2011 ,Page(s):599 – 603.

[6] Adrian Sequeira and Deepa Kundur, Communication and Information Theory in Watermarking: A Survey, *Proc. SPIE* 4518, Multimedia Systems and Applications IV, 216 (November 12, 2001).

[7] Sofiane Braci, Abdelkader Miraoui, Claude Delpha and R´emy Boyer , Watermarking Scar as an Ultimate copy protection:, 2009 Euro-American Workshop on Information Optics IOP Publishing, Journal of Physics: Conference Series **206** (2010).

[8] Ting Luo, Mutual Information based Watermarking Detection in Wavelet Domain for copyright Protection, Trusted Infrastructure Technologies Conference, 2008. APTC '08. Third Asia-Pacific, 14-17 Oct. 2008 , Hubei, pp. 113 – 119.

[9] J. A. O'Sullivan, P. Moulin, and J. M. Ettinger, "Information theoretic analysis of steganography," in *Proc.IEEE International Symposium on Information Theory*, pp. 297, August 1998.

[10] Alvaro Martin et. al.,Is Image Steganography Natural , Technical report, HP Laboratories, March 7, 2004.

[11] Siwei Lyu, Information Forensics and Security IEEE Transactions on Vol:1, Issue:1, March 2006, pp.111 - 119 .