A Review Paper On WaterMarking: Present Scenario and challenges

Dr. T. N. Sharma*, Ms. Kanika Phutela**, Mr. Manish Bhardwaj***, Mr. Amitesh Kumar****

*(Director, LogicPacePace Technologies Pvt Ltd, Jaipur, Email: tnsharma@rediffmail.com)
** (Assistant Professor, Department of Computer Engineering, Poornima Institute of Engineering and Technology
Email: kanikaphutela@poornima.org)
*** (Assistant Professor, Department of Computer Engineering, Poornima Institute of Engineering and Technology
Email: manishbhardwaj@poornima.org)
**** (Assistant Professor, Department of Computer Engineering, Poornima Institute of Engineering and Technology
Email: amiteshk@poornima.org)

***Abstract*-There has been a remarkable increase in the data exchange over web and the wide-spread use of digital media. As a result, multimedia data transfer also had an improvement. Digital watermarking is popular due to the increase in the requirement of copyright protection for digital contents. The commercial prospective is the another requirement. There are various fields where water marking can be implemented such as in copy control, video authentication, broadcast monitoring, copyright protection ,finger print authentication etc.**

Keywords-information hiding, stegnography, cryptography, watermarking.

I. INTRODUCTION

With the increasing demand of digital multimedia and the digitization of visual data such as images and videos need of digital watermarking has been increased .This advancement has two flips. On one side, it has improved storage, transfer and processing of digitized data; while on the other side, duplication and exploitation of digital contents has also become a serious issue, which enable rapid and error-free movement of any unauthorized digitized data and probably manipulated copy of such information, grow in popularity in the recent years, moreover the security concerns over copyright protection of digitized multimedia data has also been increasingly emphasized. To add owner information as watermark into the visual data as a secondary indication that is not perceivable and is bonded so well with the original data that it is inseparable is one of the most emerging solutions.

Digital watermarking emerged as a promising tool for protection of the multimedia data from copyright violation. Hence “Digital Watermarking is the way for embedding watermark with predefined property rights into images, audios, videos etc implemented by different algorithms available.” This watermarking shows the possession and the user information, which could be any image as the owner’s logo, any serial number for verification or something else as control information. Digital Watermarking is very common in our everyday lives; you see watermarking in currency, government documents, stamps and many other common documents detection of the watermark or communication of the. The main use of watermarking is to provide a level of certainty about the authenticity and or ownership of a document [4].

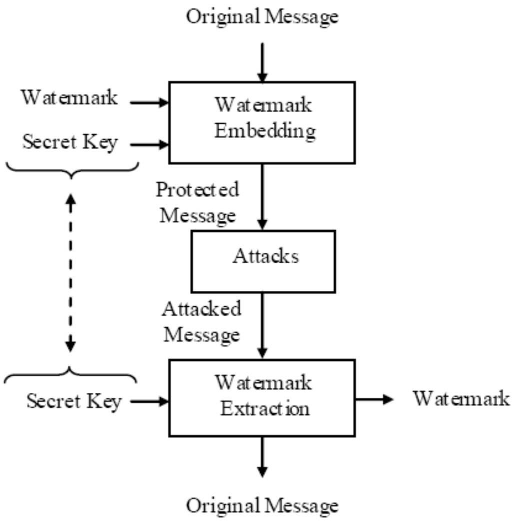

Fig. 1. A generic watermarking scheme [32]

Classification of watermarking techniques depends upon nature of data as text, image, audio or video, working domain (spatial or frequency) domain and human perception (robust or fragile) [6]. For images we can classify watermarking into three ways: (i) Visible watermarking (ii) Invisible fragile watermarking and (iii) Invisible robust watermarking [5], [6].These all can be implemented using hardware or software or both.

II. STEGANOGRAPHY

Steganography is a way that allows secret communication by embedding or hiding the secret information in unsuspected data. Steganography relies on the assumption that the existence of the secret communication is unknown to third parties. Steganographic methods are not robust; the hidden information cannot be tracked after data exploitation.

III. DIGITAL WATERMARKING

A. Requirements

The basic requirements for digital watermarking are as follows:

1) It should be capable to convey as much information as possible, in other words watermark data rate should be higher.

2) Only authorized parties should be able to access the watermark. It should be secret also. This requirement can be fulfilled by employing cryptography in watermarking. 3) A watermark should be robust. This feature helps in copyright protection implementation or conditional access applications.

4) A watermark should be irremovable as well as unnoticeable.

Depending upon media and application type some additional requirements can also be included as follows:

1) When implementing watermark recovery, it may or may not allow using the original or unwatermarked host data.

2) Watermark embedding may be required in real time also for example, for video fingerprinting. This embedding might require compressed-domain embedding methods.

3) It may be required that watermark should be able to convey some casual information.

In the following, a few of the mentioned requirements and the resulting design issues are highlighted in more detail.

1) Watermark Security and Keys: If security, i.e., secrecy of the embedded information, is required, one or several secret and cryptographically secure keys have to be used for the embedding and extraction process. For example, in many schemes, pseudorandom signals are embedded as watermarks. In this case, the description and the seed of the pseudorandom number generator may be used as key. There are two levels of secrecy. In the first level, an unauthorized user can neither read or decode an embedded watermark nor can he detect if a given set of data contains a watermark. The second level permits unauthorized users to detect if data are watermarked, however, the embedded information cannot be read without having the secret key. Two watermarks can be embedded with these schemes, one with a public key and the other with a secret/private key. Alternatively, a scheme has been proposed which combines one or more public keys with a private key and embeds one combined public/private watermark, rather than several watermarks [7].

While designing an overall copyright protection system, some issues like secret key generation, key distribution and management (by Key Distribution Center), as well as other system integration aspects have to be considered.

2) Robustness: In the design of any watermarking scheme, watermark robustness is typically one of the main issues, since robustness against data distortions introduced through standard data processing and attacks is a major requirement. Standard data processing includes all data manipulation and modification that the data might undergo in the usual distribution chain, such as data editing, printing, enhancement, and format conversion. “Attack” denotes data manipulation with the purpose of impairing, destroying, or removing the embedded watermarks. Although robust watermarking techniques can be designed only when watermark is not public. If watermark detector principle and key are public, and even if only a “black-box “watermark detector is public, the watermark is vulnerable to attacks [8], [9]. Hence, public watermarks, as sometimes proposed in the literature, are not robust unless every receiver uses a different key. This however is difficult in practice and gives rise to collusion attacks.

3) Imperceptibility: One of the main requirements for watermarking is the perceptual transparency. The data combining process should not include any perceptible artifacts into the host data. On the side, for high consistency, it is desirable that the watermark amplitude to be high. Thus, the design of a watermarking method always involves a tradeoff between imperceptibility and robustness. It would be optimal to embed a watermark just below the threshold of perception. However, this threshold is difficult to determine for real-world image, video and audio signals. Several measures to determine objectively perceived distortion and the threshold of perception have been proposed for the mentioned media [10]. However, most of them are still not perfect enough to replace human viewers or listeners who judge the visual or audio fidelity through blind tests. Thus, in the design of watermarking systems, it is usually necessary to do some testing with volunteers. The second problem occurs in combination with post watermarking processing, which might result in an amplification of the embedded watermark and make it perceptible. An example is zooming of watermarked images, which often makes the embedded watermarks visible, or contrast enhancement, which may amplify highly frequent watermark patterns that are otherwise invisible.

4) Watermark Recovery With or Without the Original Data: Watermark recovery is usually more robust if the original, unwatermarked data are available. Further, availability of the original data set in the recovery process allows the detection and inversion of distortions which change the data geometry. This helps, for example, if a watermarked image has been rotated by an attacker. However, access to the original data is not possible in all cases, for example, n applications such as data monitoring or tracking. For other applications, like video watermarking, it may be impractical to use the original data because of the large data volume, even if it is available. It is, however, possible to design watermarking techniques that do not need the original for watermark extraction. Most watermarking techniques perform some kind of modulation in which the original data set is considered a distortion. If this distortion is known or can be modeled in the recovery process, explicitly designed techniques allow its suppression without knowledge of the original. In fact, most recent methods do not require the original for watermark recovery. In some publications, such techniques are called "blind" watermarking techniques [11], [12].

5) Watermark Extraction or Verification of Presence for a Given Watermark: In the literature, two different types of watermarking systems can be found: systems that embed a specific information or pattern and check the existence of the (known) information later on in the watermark recovery—usually using some sort of hypothesis testing—and systems that embed arbitrary information into the host data. The first type, verification of the presence of a known watermark, is sufficient for most copyright-protection applications.

The second type, embedding of arbitrary information, is, for example, useful for image tracking on the Internet with intelligent agents where it might not only be of interest to discover images, but also to classify them. In such cases, the embedded watermark can serve as an image identification number. Another example where arbitrary information has to be embedded are applications for video distribution where, e.g., the serial number of the receiver has to be embedded.

IV. Techniques used for watermarking

A. DCT-based watermarking

In DCT-based watermarking technique first of all image is first divided into blocks of 8 ×8 pixels. After transformation and quantization, the DCT coefficients are selected who have mid-frequency range based on a Gaussian network classifier. Now embedding is performed followed by modifications using linear DCT constraints. This algorithm is limited to JPEG compression.

B. Embedding and Extraction

This technique uses the irrelevant portion of the fractional component of pixel intensity value of the cover image. This is encoded to generate watermark. Watermark in the unimportant part helps in maintaining the consistency of the cover image.

Imperceptibility is achieved. If watermark can consist of large capacity than it will be an added benefit. This large capacity watermarking will be useful in watermarking applications and security products.

C. Secure Spread Spectrum Watermarking

A digital watermarking can also be used in audio, video, image and multimedia data. Generally we think that any watermark should be kept in perceptually major components of a signal if it is to be vigorous to ordinary signal distortion and malevolent attack. But this modification can lead to significant degradation of quality of signal.

Solution of this problem is to add a watermark into spectral components of data using some techniques like spread spectrum communications, hiding a band

Signal that is narrow in a channel. Removal of watermark is difficult for an attacker even if multiple attackers work together. It is also consistent to ordinary signals and distortions like digital-to-analog and analog-to-digital Conversion, dithering, compression, re-sampling, quantization, rotation, cropping, translation and scaling. This algorithm can work upon image audio and video with some modifications. When the retrieval process is implemented owner is identified and counterfeiting is made impossible.

D. Spread Spectrum

Limitations imposed due to least significant bit substitution can be removed by spreading the watermark transversely the cover image by using greater bits than the required bits. This way of hiding data ensures the robustness of watermark. This spread spectrum technique allows the frequency bands matching before embedding. Spread spectrum preserves privacy using a secret key for controlling pseudo noise generator. Pseudorandom sequence can be used as the spreading sequences. Pseudo noise can be generated using matlab function.

E. Wavelet Based Watermarking

To convert into discrete wavelet domain multi resolution data combination technique is used. Image and watermark are used for transformation. For the embedding purpose watermark is added with each wavelet decomposition level of host image. At the time of detection an average from wavelet decomposition is taken. It is strong enough to fight with compression, noise and filtering operations.

V. CONCLUSION

This paper discuses various techniques for watermarking. New approaches are expected to come out and may merge existing approaches. For example, a watermark can be separated into two parts: one for copyright protection and the other for customer fingerprinting. One watermark may be embedded in DCT domain while other in DWT. various scene change algorithms may be suggested. Further texture features could be extracted. However many challenges are still there. Robustness is a parameter that has to be well thought of. Some aggressive video processing’s may modify the watermark signal. Certain factored checks have to be described for an intended application. Some major challenges are the collusion attack and real time watermarking as proposed in the literature. The performance of many image watermarking algorithms is being improved by the perceptual measures. It is challenging to exploit the perceptual features of the video in real time.

VI. REFERENCES

[1]Mansi Hasija1 ,Alka Jindal2 “Contrast of Watermarking Techniques in different domains” IJCSI International Journal of Computer Science Issues, Vol.8, Issue 3, No. 2,ISSN (Online): 1694-0814 ,May 2011.

[2]Hsin-Lung Wu & Jen-Chun Chang &Te-Chih Chou & Lai, Wei-Ming “A New Scheme for Data Hiding on Halftone Images” Fifth International Conference on Genetic and Evolutionary Computing, IEEE, 2011

[3]Dilip Kumar Sharma, Vinay Kumar Pathak and G.P. Sahu “Digital watermarking for secure e-government framework”

[4]Hsiang-Cheh Huang, Feng-Cheng Chang, Wai-Chi Fang “Reversible Data Hiding with Histogram-Based Difference Expansion for QR Code Applications” IEEE 2011.

[5]J. Pan, H. C. Huang, and L. C. Jain. Intelligent WatermarkingTechniques.*World Scientific*, 2004.

[6] S. Jayaraman, S. Esakkirajan, and T. Veerakumar.*Digital ImageProcessing*. McGraw-Hill, 2009

[7]“Fast public-key watermarking of compressed video,” in*Proc. IEEE Int. Conf. on Image Processing 1997 (ICIP ’97)*,vol. 1, Santa Barbara, CA, Oct. 1997, pp. 528–531.

[8] I. J. Cox and J.-P. Linnartz, “Some general methods for tampering with watermarks,” *IEEE J. Select.Areas Commun. (SpecialIssue on Copyright and Privacy Protection)*, vol. 16, pp.587–593, May 1998

[9]“Watermark estimation through detector observations,” in*Proc. IEEE Benelux Signal Processing Symposium ’98*, Leuven,Belgium, Mar. 1998.

[10]M. Kutter and F. Petitcolas, “A fair benchmark for imagewatermarking systems,” in *Proc. SPIE IS&T/SPIE’s 11th Annu.Symp., Electronic Imaging ’99: Security and Watermarking ofMultimedia Contents*, vol. 3657, Jan. 1999.

[11]R. J. Anderson and F. Petitcolas, “On the limits of steganography,”*IEEE J. Select. Areas Commun. (Special Issue on Copyright and Privacy Protection)*, vol. 16, pp. 474–481, May 1998.

[12]M. Barni, F. Bartolini, V. Cappellini, and A. Piva, “A DCTdomainsystem for robust image watermarking,” *Signal Processing(Special Issue on Watermarking)*, vol. 66, no. 3, pp.357–372, May 1998

[13]Peter Meerwald, “ Digital image watermarking in thewavelet Transform domain “ P.Hdthesiss.

[14]Houng- Jyh Mike Wang, Po-Chyi Su and C.-C. Jay Kuo,“Wavelet-based digital image watermarking” OPTICSEXPRESS, 7 December 1998 / Vol. 3, No. 12,PP 491-496

[15]Arvind Kumar Parthasarathy and SubhashKak “AnImproved Method of Content Based Image Watermarking “IEEE Transaction on broadcasting, Vol. 53, No. 2, June 2007, PP 468-479.

[16] Xiang-Gen Xia, Charles G. Boncelet and Gonzalo“Wavelet Transform based watermark for digital Images”, R.Arce : OPTICS EXPRESS, 7 December 1998 / Vol. 3, No. 12,PP 497-511

[17]MahaSharkas, Dahlia ElShafie, and NadderHamdy ,”ADual Digital-Image Watermarking Technique”, Transaction on Engineering, computing and technology, Vol 5, April 2005ISSN 1305-5313

[18]Rafael C. Gonzalez, R.E.Woods, Steven:, “Digital imageprocessing using MATLAB:”

[19]Vallabha V Hampiholi, “ Multiresolution WatermarkBased on Wavelet Transform for Digital images”

[20]www.amara.com/current/wavelet.html “ An introduction about Wavelets- Amara Graps “

[21]Ibrahim Nasir, Ying Weng, Jianmin Jiang, “A NewRobust Watermarking Scheme for Color Image in SpatialDomain”

[22]VikasSaxena, J.P Gupta, ” Collusion Attack ResistantWatermarking Scheme for Colored Images using DCTIAENG International Journal of Computer Science, 34:2,IJCS_34_2_02: Publication: 17 November 2007

[23]M. Kuttera and F. A. P. Petitcolas, “ A fair benchmarkfor image watermarking systems

[24]P.Deepika , S.RajeshPh.D , Dr.V. SrinivasaRaoPh.D" Watermark- Based Multimedia Content Authentication"(IJAEST) INTERNATIONAL JOURNAL OF ADVANCED ENGINEERING SCIENCES ANDTECHNOLOGIES VolNo. 7, Issue No. 1, 048 – 053,Publication 2011
[25]FRANK HARTUNG,MARTIN KUTTER "Multimedia Watermarking Techniques"PROCEEDINGS OF THE IEEE, VOL. 87, NO. 7, JULY 1999
[26]NedeljkoCvejic, TapioSeppänen" Increasing Robustness of LSB Audio Steganography Using a NovelEmbedding Method"Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04) 2004 IEEE.
[27]Ismail Avcıbas"Steganalysis Using Image Quality Metrics"IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 12, NO. 2, FEBRUARY 2003
[28]Kumari Vandna, Kirti Khatkar"Improve Security And Capacity of Watermark Image Truly Imperceptible"International Journal of Graphics & Image Processing |Vol 1|issue 2|November 2011
[29]Ioannis Pitas, Senior Member,IEEE"Region-based image watermarking" IEEE Transaction On Image Processing, Vol.10, No.11, November 2001
[30]DhruvArya "A Survey of Frequency and Wavelet Domain Digital Watermarking Techniques" International Journal of Scientific & Engineering Research, Volume 1, Issue 2, November-2010
[31] XIE Qing, XIE Jianquan, XIAO Yunhua "A High Capacity Information Hiding Algorithm In Color Image" IEEE ,2010
[32] Mustafa Osman Ali and Rameshwar Rao
"Digital Image Watermarking Basics, and Hardware Implementation"