ISSN No. 0976-5697

Volume 2, No. 3, May-June 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Digital Watermarking : The reliable protection to multimedia content

Ms Anamika Joshi
Sr. Asst. Professor
Shri Vaishnav Institute Of management
Indore (MP), India
E-mail: anajoshi4@gmail.com

Ms Rashmi Tiwari
Asst. Professor
Shri Vaishnav Institute Of management
Indore (MP), India
E-mail:rashmikanungo@yahoo.com

Ms Namrata Jain*
Asst. Professor
Jain Arts, Science & Commerce College
Mandsaur (MP), India
E-mail: namrata_12664@rediff.com

Abstract: The advent of the Internet has resulted in many new opportunities for the creation and delivery of content in digital form. Applications include real time video and audio delivery, digital repositories and libraries, Web publishing and electronic advertising etc. An important issue that arises in these applications is the protection of the rights of all participants. Digital Watermarking is a technology being developed to ensure security and protection of multimedia data. The purpose of digital watermarking is to facilitate data authentication, copyright protection and content integrity verification. Digital watermarking is a relatively new and highly multidisciplinary research field, which combines the work of fields such as digital signal processing with cryptography, communications and information theory, and the theory of visual perception. This paper is intended to disseminate the concept, application and schemes of digital watermarking for multimedia security management. We will be addressing the challenges posed to multimedia security and how watermarking could meet those challenges.

Keywords: Watermarking, data authentication, copyright protection, content integrity verification, cryptography, Digital multimedia security.

I. INTRODAUCTION

Digital information revolution has brought about many advantages and new issues. Unlimited number of replicas of the original content can be made from unprotected digital content. This makes the content creators and content owners more anxious about the copyrights management of their digital contents.

Today, well established cryptographic algorithms can resolve many of these issues. However, cryptography [1] can only protect the digital contents during the transmission of the data from the sender to receiver. Once content is decrypted, there's nothing to prevent an authorized user from illegally replicating digital content. Some other technology is obviously needed to solve this problem. One of the solutions to this problem is a digital watermarking system. [2][3][4][5].

A digital watermarking is a piece of information that is embedded directly in media content, in such a way that it is imperceptible to a human observer, but easily detected by a computer and can later be extracted or detected for a variety of purposes including copy prevention and control.

The watermark should be imperceptibly embedded into the digital multimedia content, and it should be robust enough to survive not only most common signal distortions, but also distortions caused by malicious attacks. Well-established organizations are actively doing research into digital watermarking and developing digital watermarking system and schemes to protect multimedia contents. Researchers are developing general guidelines for effective watermarking algorithm design, improving robustness and reliability, and tailoring to the constantly changing needs of multimedia industries [4][5].

II. APPLICATION AREA

There are a number of different watermarking application scenarios, and they can be classified in a number of different ways. The following classification is based on the type of information conveyed by the watermark [6][7].

Table I: Classes of watermarking applications

Application Class	**Purpose of the embedded watermark**	**Application Scenarios**
Protection of Intellectual Property Rights	Conveys information about content ownership and intellectual property rights	Copyright Protection, Copy Protection, Fingerprinting
Content Verification	Ensures that the original multimedia content has not been altered, and/or helps determine the type and location of alteration	Authentication, Integrity Checking
Information hiding	Represents side-channel used to carry additional Information.	Broadcast Monitoring, System Enhancement

Possible application scenarios of Digital watermarking [8] are:

1. ***Digital Watermarking for Copyright Protection***

The watermark identifies the owner of the content. This information can be used by a potential user to obtain legal rights to copy or publish the content from the contact owner [10].

2. ***Digital Watermarking for Copy Protection***

Watermarks can also be used for copy prevention and control. For example, in a closed system where the multimedia content needs special hardware for copying and/or viewing, a digital watermark can be inserted indicating the number of copies that are permitted. Every time a copy is made the watermark can be modified by the hardware and after a point the hardware would not create further copies of the data. An example of such a system is the Digital Versatile Disc (DVD) [11]. In fact, a copy protection mechanism that includes digital watermarking at its core is currently being considered for standardization and second generation DVD players may well include the ability to read watermarks and act based on their presence or absence.

3. ***Digital Watermarking for Fingerprinting***

In applications where multimedia content is electronically distributed over a network, the content owner would like to discourage unauthorized duplication and distribution by embedding a distinct watermark (or a fingerprint) in each copy of the data. If, at a later point in time, unauthorized copies of the data are found, then the origin of the copy can be determined by retrieving the fingerprint. In this application the watermark needs to be invisible and must also be invulnerable to deliberate attempts to forge, remove or invalidate.

4. ***Digital Watermarking for Content Authentication***

In this type of application the watermark encodes information required to determine that the content is authentic. It must be designed in such a way that any alteration of the content either destroys the watermark, or creates a mismatch between the content and the watermark that can be easily detected. If the watermark is present, and properly matches the content, the user of the content can be assured that it has not been altered since the watermark was inserted. This type of watermark is referred as a *fragile watermark.* One example of this technology being used for image authentication is the trustworthy digital camera described in [12].

5. ***Digital Watermarking for Broadcast and Publication Monitoring***

In broadcast monitoring, automated system is used to collect information about the content being broadcast, and this information is then used as the bases for billing(for example in advertisement) as well as other purposes. Here, the watermark contains broadcast identification information and it's embedded directly into the multimedia content itself, and the resulting broadcast monitoring solution becomes compatible with broadcast equipment for both digital and analog transmission.

6. Secret communication

The embedded signal is used to transmit secret information from one person to another, without anyone along the way knowing that this information is being sent. This is the classical application of steganography[13] – the hiding of one piece of information within another.

III. Digital Watermarking System

Digital watermarking system [7] consists of two main components: *watermark embedder* and *watermark detector*. The embedder combines the *cover work* C_0, an audio-visual signal in which data will be hidden, and the *payload P,* an input message to be added to the cover work, and creates the *watermarked cover* C_W. This embedding operation takes place in two phases. In the first phase, the watermark encoder takes the payload *P* and maps it into the watermark *W,* which has to be of the same type and dimension as the cover work C_0. For example, if the cover work C_0 is an image, then the watermark encoder would produce an image pattern of the same size as the cover image. This mapping may be done with help of a watermark key *K* which can be used to enforce security. In the second phase, the watermark *W* is added to the cover work C_0 to produce the watermarked cover C_W. It can be described using the following notation:

$$C_W = E_1(C_O,W) \quad \wedge \quad W = E_0(P,K)$$

Watermark detector either extracts the payload *P* from the watermarked cover C_W, or it produces some kind confidence measure indicating how likely it is for a given payload *P* to be present in C_W. The extraction of the payload is done with help of a watermark key *K.* It can be described using the following notation:

$$P = D(C_W,K)$$

Block diagram for generation and detection of watermark

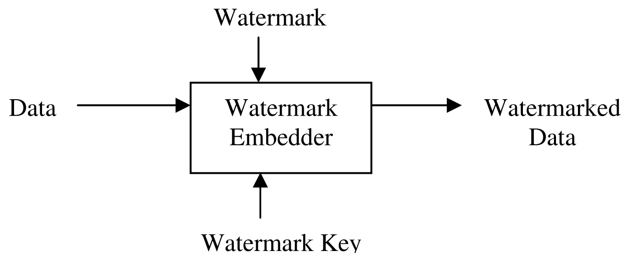

Figure 1 . Watermark Insertion.

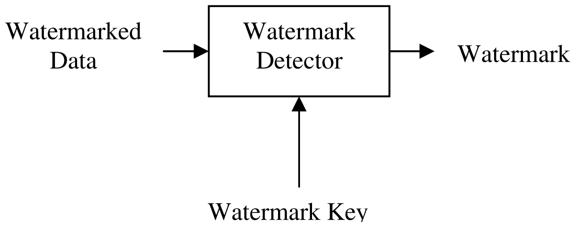

Figure 2. Watermark Detection.

IV . Parameters of Digital watermarking

Digital watermarking techniques may be classified in several ways. Parameters used in the categorization of digital watermark are [14] as given below:

1. Robustness :

A digital watermark is called *fragile* if it fails to be detectable after the slightest modification. Fragile watermarks are commonly used for integrity proof.

A digital watermark is called *semi-fragile* if it is intended to de undetectable only after malicious manipulations of the host media in which it is embedded and detectable after non-malicious manipulations. Semi-fragile watermarks commonly are used to detect malicious operations.

A digital watermark is called *robust* if it is intended to be detectable even after significant malicious and non-malicious manipulations on the host media in which it is embedded. Robust watermarks may be used in copy protection applications.

2. **Perceptibility :**

A digital watermark is called *imperceptible* if the original cover data and the watermarked data are perceptually indistinguishable.

A digital watermark is called *perceptible* it its presence in the watermarked data is noticeable.

3. **Capacity :**

Capacity is the optimum amount of data that can be embedded in a given signal. On the basis of length of the embedded message the digital watermarking schemes can be classified into two different classes:

- The message is conceptually zero-bit long and the system is designed in order to detect the presence or the absence of the watermark in the marked object. This kind of watermarking schemes is usually referred to as *zero-bit* watermarking schemes.
- The message is a n-bit-long stream and is modulated in the watermark. These kinds of schemes usually referred to as *multiple-bit* watermarking or *non-zero-bit* watermarking schemes.

V. Digital water marking Techniques

A large number of research papers and articles have been published on digital watermarking over the last decade, where a number of different watermarking approaches have been presented [9, 15, 16, 17, 18, and 19]. Most of those approaches are similar and they only differ in one or a few aspects related to how a watermark gets created, where in the cover work it gets embedded, how it gets embedded, what domain to use for embedding, and how it gets detected. For obvious reason, it is not possible to discuss all contributions made in the field of digital watermarking. Instead, we will classify watermarking solutions according to the defining properties mentioned above. More specifically, the basic alternatives in a design of a digital watermarking system are:

1. **Processing domain selection**: A watermark can be embedded into the cover image in a *spatial domain* [20][21].Alternatively, it can be more advantageous to do it in a *transform domain*, such as discrete Fourier transform domain (DFT) [25][26], discrete cosine transform domain (DCT) [10][22][23], the Fourier-Mellin transform domain, wavelet transform domain [24], or the fractal transform domain [27].
2. **Cover location selection**: Early watermarking techniques were based on using the least significant bit of the image representation as the carrier for watermark. This technique has been improved by *random selection* of cover locations where the watermark information will be embedded. A pseudorandom number generator, initialized by the secret key (the seed), is usually used to determine those locations. This solution basically hides the locations where various bits of watermark information are embedded [10]. An alternative approach protects the watermark information by *spreading* it across cover, so that any cover location contains some part of watermark information [28].
3. **Payload encoding:** Some applications required only one bit of information to show the presence and absence of the watermark. A watermark carrying one bit of information is created as a psedo-random noice drown from uniform distribution.But,most watermarking applications, require more than one bit of information to be embedded. Some solutions allow any multi-bit payload to be directly embedded into an image [10]. Others use *spread spectrum* [29] or *error correcting codes* to transform a payload into an appropriate watermark before embedding it into data.
4. **Watermark embedding method selection:** A watermark can simply be *added* to the cover image. The addition may be image independent or image dependent. The additional techniques differ on how they exploit frequency sensitivity, luminance sensitivity and masking capabilities of the human visual system (HVS) [16]. An alternative watermark embedding method is based on *quantization* [30]. Their method called quantization index modulation (QIM) is based on the set of N- dimensional quantizers. The quantizers are designed such that the reconstruction values from one quantizer have a good separation from the reconstruction points of every other quantizer. The message to be transmitted is used as an index for quantizer selection. The selected quantizer is then used to embed the information by quantizing the image data in either special or DCT domain. Quantization watermarks suffer from low robustness, but have a high information capacity due to rejection of host interference.
5. **Watermark detection**: In general, watermark detection is directly derived from watermark embedding.

VI. Evaluation of Watermarking system

Once a watermarking system has been designed and implemented, it is important to be able to objectively evaluate its performance. This evaluation should be done in such a way to be able to compare results against other watermarking systems designed for the same or similar purpose [31][32].

By definition, watermarking is a technique for embedding a watermark into a cover work imperceptibly and robustly. Therefore a quality of a new watermarking system can be measured by evaluating those two properties and comparing results against an equivalent set of measures obtained by evaluating other watermarking systems.

Watermark imperceptibility can be evaluated either using subjective evaluation techniques involving human observers, or using some kind of distortion or distance metrics. Watermark robustness can be evaluated using standardized benchmark tests. Those tests are designed to create various distortions to the watermarked cover under tests, so that it is possible to measure watermark detection rate under those conditions.

VII. WATERMARKING ISSUES

The important issues that arise in the study of digital watermarking techniques are:

- *Capacity:* what is the optimum amount of data that can be embedded in a given signal? What is the optimum way to embed and then later extract this information?
- *Robustness:* How do we embed and retrieve data such that it would survive malicious or accidental attempts at removal?
- *Transparency:* How do we embed data such that it does not perceptually degrade the underlying content?
- *Security:* How do we determine that the information embedded has not been tampered, forged or even removed?

Indeed, these questions have been the focus of intense study in the past few years and some remarkable progress has already been made. However, there are still more questions than answers in this rapidly evolving research area. Perhaps a key reason for this is the fact that digital watermarking is inherently a multi-disciplinary topic that builds on developments in diverse subjects. The areas that contribute to the development of digital watermarking include at the very least the following:

- Information and Communication Theory
- Decision and Detection Theory
- Signal Processing
- Cryptography and Cryptographic Protocols

Each of these areas deals with a particular aspect of the digital watermarking problem.

VIII. CONCLUSION

Digital watermarking provides more solutions and promises for multimedia security. It has been accepted as a complementary technology to multimedia encryption, providing some additional level of protection. There are many ranges of applications that could be benefited from applying digital watermarking. Protection of intellectual property is very important nowadays because digital multimedia content can be copied and distributed quickly, easily, inexpensively, and with high quality. And watermarking could be used for this purpose. Other applications, such as copy protection, fingerprinting, content authentication and broadcast monitoring could also be benefited. The solutions are more likely to remain application dependent and trade-offs between the conflicting requirements of low distortion, high capacity, complexity, and robustness still have to be made. Before trustworthiness can be evaluated, possible attacks for specific applications have to be studied at the development stage. With so many challenges and potential, we expect that digital watermarking will continue to be an active research area.

IX. REFERENCES

[1] Ajaya Goel, O.P. Sahu, Rupesh Gupta, Sheifali Gupta. “Improved Digital Watermarking Techniques and Data Embedding In Multimedia” International Journal on Computer Science and Engineering Vol. 02, No. 02, 2010, 164 – 68.

[2] I.J. Cox, M. L. Miller and J.A. Bloom “Watermarking applications and their properties” Int. conf. on Information Technology, Las Vegas, 2000.

[3] M. D. Swanson, M. Kobayashi, and A. Tawfik, "Multimedia Data-Embedding and Watermarking Technologies," Proceedings of the IEEE, vol.86, no. 6, June 1998, pp. 1064-1087.

[4] F. A. P. Petitcolas, R. J. Anderson and M.G. Kuhn, “Information Hiding – A survey, “ Proceedings of the IEEE, Special Issue on Protection of Multimedia Contents, vol. 87, no. 7, 1999,pp. 1062 – 1078.

[5] B.M. Macq and J.J. Quisquter. “ Cryptology for digital broadcasting”. Proceeding of the IEEE, volume 83, pages 944-957, june 1995.

[6] Moulin, P.; O'Sullivan, J.A.; “Information-theoretic analysis of information hiding”, IEEE Transactions on Information Theory, Volume: 49 Issue: 3 , March 2003, Page(s): 563 -593.

[7] Edin Muharemagic and Borko Furht “Multimedia Security: Watermarking Techniques”. www.cse.fau.edu/~borko

[8] M. Arnold, M. Schmucker, and S. D. Wolthusen, "Techniques and Applications of Digital Watermarking and Content Protection", Artech House, 2003.

[9] R. G. van Schyndel, A. Z. Tirkel and C. F. Osbome, "A Digital Watermark," Proceedings of IEEE International Conference on Image Processing, vol.2, pp. 86-90, Austin, Nov. 1994.

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

[11] Bell, A.E.; “The dynamic digital disk”, Spectrum, IEEE, Volume: 36 Issue: 10 , Oct. 1999, Page(s): 28 - 35.

[12] Friedman, G.L., “The Trustworthy Digital Camera: Restoring Credibility to the Photographic Image,” IEEE Transaction on Consumer Electronics, Vol. 39, No. 4, November 1993, pp.905-910.

[13] R.J. Anderson and F. Peticolas, “On the Limit of Steganography,” IEEE J. Select.Areas Comm., vol. 16, May 1998, pp. 474-481.

[14] Digital watermarking – wikipedia the free encyclopedia.

[15] I.J. Cox, M.L.Miller, and J.A.Bloom, “Digital Watermarking”, Morgan Kaufmann, 2001.

[16] Hartung, F.; Kutter, M.; “Multimedia watermarking techniques”, Proceedings of the IEEE , Volume: 87 Issue: 7 , July 1999, Page(s): 1079 -1107.

[17] S. Katzenseisser and F.A.P Petitcolas, “Information Hiding Techniques for Steganography and Digital Watermarking”, Artech House, Boston – London 2000.

[18] Podilchuk, C.I.; Delp, E.J.; “Digital watermarking: algorithms and applications” Signal Processing Magazine, IEEE , Volume: 18 Issue: 4 , July 2001, Page(s): 33 – 46.

[19] 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, Page(s): 1108 -1126.

Bender W., Gruhl D., and Morimoto N., "Techniques for Data Hiding," Technical Report, MIT Media Lab, 1994

[20] Cox I., Kilian J., Leighton T., and Shamoon T.,"Secure spread-Spectrum watermarking for Multimedia," Technical Report 95-10, NEC Research Institute, 1995.

[21] M. Barni, F. Bartolini, V. Cappellini, and A. Piva,

"A DCT-domain System for Robust Image Watermarking," Signal Processing (Special Issue on Watermarking), vol.66, no. 3, 1998, pp.357- 372.

[22] Afzel Noore ,West Virginia University, Morgantown, WV, USA, "An Improved Digital Watermarking Technique for Protecting JPEG Images " Proceedings of IEEE conference ,ICCE 2003, 17-19 June 2003.

[23] D. Kundur, and D. Hatzinakos, "A Robust Digital Image watermarking Method using Wavelet-Based Fusion," Proceedings of the IEEE International Conference on Image Processing, Oct. 26-29, 1997, Santa Barbara, CA, vol. 1, pp. 544-547.

[24] Ramkumar, M.; Akansu, A.N.; Alatan, A.A.; "A robust data hiding scheme for images using DFT", Image Processing, 1999. ICIP 99. Proceedings. 1999 International Conference on , Volume: 2 , 24-28 Oct. 1999 Page(s): 211 -215 vol.2.

[25] Papadopoulos, H.C.; Sundberg, C.-E.W.; "Simultaneous broadcasting of analog FM and digital audio signals by means of precanceling Techniques",1998. ICC 98. Conference Record.1998 IEEE International Conference on Communications, Volume: 2 , 7-11 June 1998, Page(s): 728 -732 vol.2.

[26] Dugelay, J.-L.; Roche, S.; "Fractal transform based large digital watermark embedding and robust full blind extraction" Multimedia Computing and Systems, 1999. IEEE International Conference on , Volume: 2 , 7-11 June 1999 Page(s): 1003 -1004 vol.2

[27] Cox, I.J.; Kilian, J.; Leighton, F.T.; Shamoon, T.; "Secure spread spectrum watermarking for multimedia", IEEE Transactions on Image Processing, Volume: 6 Issue: 12 , Dec. 1997, Page(s): 1673 -1687.

[28] Hartung, F.; Girod, B; "Digital Watermarking of MPEG-2 Coded Video in the Bitstream domain,"**,** Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing, Vol. 4, Munich, Germany, Apr. 1997, pp 2621-2624

[29] 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, Page(s): 1423 -1443

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

[31] Petitcolas, F.A.P.; "Watermarking schemes evaluation", Signal Processing Magazine, IEEE, Volume: 17 Issue: 5 , Sept. 2000, Page(s): 58 -64.