Digital Watermarking: Current Status and Key Issues

Manjit Thapa
Department of Computer Science, Sri Sai College of Engg. & Tech., Badhani (Pathankot).
e-mail: manjit.thapa@yahoo.co.in

Dr. Sandeep Kumar Sood
Department of Computer Science and Engineering G.N.D.U.R.C, Gurdaspur, India.
e-mail: san1198@gmail.com

Meenakshi Sharma
Department of Computer Science Sri Sai College of Engg. & Tech., Badhani (Pathankot).
e-mail: Sharma.minaxi@gmail.com

Abstract: ***Digital watermarking is used to hide the information inside a signal, which cannot be easily extracted by the third party. Its widely used application is copyright protection of digital information. It is different from the encryption in the sense that it allows the user to access, view and interpret the signal but protect the ownership of the content. One of the current research areas is to protect digital watermark inside the information so that ownership of the information cannot be claimed by third party. Digital watermark can be visible or invisible embedded in a multimedia document for copyright protection. With a lot of information available on various search engines, to protect the ownership of information is a crucial area of research. The watermarking techniques help to achieve artificial intelligence. Digital watermarking is the most effective solution in this area and its use to protect the information is increasingly exponentially day by day.***

Keywords***: Digital Watermarking, Copyright Protection, Discrete Cosine Transform, Discrete Wavelet Transform and Security.***

I. INTRODUCTION

Digital watermarking is a technique that embeds data called watermark into a multimedia object such that watermark can be detected to make an assertion about the objects. It can be categorized as visible or invisible. Example of visible watermarking is the logo visible superimposed on the corner of television channel in a television picture. On the other hand, invisible watermark is hidden in the object, which can be detected by an authorized person. Such watermarks are used for satisfy the author authentication and detecting unauthorized copying. Digital watermarking technique provides copyright protection for digital data. It can be categorized in different ways according to the type of watermark being used such as the watermark may be a visual recognizable logo or sequence random numbers. Another classification is based on domain which the watermark is applied i.e., the spatial domain or the transform domain. The originally watermarking techniques are almost in spatial domain. Spatial domain techniques are affected by image compression and heavy image processing. Transform domain watermarking techniques which is based on the discrete cosine transform (DCT) and discrete wavelet transform (DWT), distinct higher image imperceptibility and are robust to manage. It is presently used in a variety of signal processing applications, such as audio and video compression, removal of noise in audio and the simulation of wireless antenna distribution.

The digital watermarking technique suffers from unintentional and intentional attacks. Unintentional attacks include the common signal processing operations, such as low pass filters, median filters, and analog to digital and digital to analog conversion, resampling, requatization and common geometric distortions, such as rotation, cropping and scaling. Intentional attacks include the collusion (combination of two or more attacker) and forgery.

This paper is organized as follows. In Section II, we introduce the literature review briefly. In Section III, we describe the requirements and applications. In Section IV, we propose future research directions and Section V conclude the paper.

II. LITERATURE REVIEW

In 1997, Kundur and Hatzinakos [1] proposed a fragile watermark technique, which they claimed to be temper-proofing method. Their design integrate delicate watermark in the discrete wavelet domain of the signal by quantizing the corresponding coefficients with user-specified keys. The watermark is a binary signature, which is integrated into key-selected detail sub-band coefficients. This algorithm is built on the quantization method. An integer wavelet transform is introduced to avoid round-off errors during the inverse transform, because round-off may be considered as a tempering attempt. However, it is not used for copyright protection and only check out the tempering with information.

In 1998, Podilchukand Zeng [2] proposed two watermarking techniques for digital images that are based on utilizing visual models. The first technique makes use of a DCT based visual mask and second technique is based on a visual model using four level wavelet decompositions. Their schemes are shown to provide very good results both in terms of image transparency and robustness.

In 1999, Loo and Bary [3] proposed a watermarking algorithm in the complex wavelet domain. They used a model based on communication process that shows the complex wavelet domain has high capacity for integrating information in the host signal. They concluded that complex wavelet domain is a good domain for watermarking. However, it is computationally very expensive.

In 2001, Delp et al. [4] proposed a public watermarking system that embeds a couple of watermarks: a delicate watermark in the spatial domain and a semi-delicate watermark in the frequency domain. They employ the advanced encryption standard to make the watermarking algorithm public and provide high robustness against different operations.

In 2002, Ali [5] proposed another approach to DWT and DCT to improve the performance of the DWT-based watermarking algorithms. In this method, watermarking is done by embedding the watermark in first and second level of DWT sub-bands of the host image, followed by the application of DCT on the selected DWT sub-bands. The combination of these two transforms improved the watermarking performance considerable in comparison with only watermarking approaches. They showed that the quality of watermark image is very good.

In 2003, Bum et al. [6] introduced two watermarking approaches that are robust to geometric distortions. The first approach is invariant to affine transform attack and is based on normalization. The second approach is based on a re-synchronization scheme that uses log polar map. Both schemes employ a direct sequence code division multiple access approach to integrate a multi-bit watermark in the DFT domain of image. However, their schemes are shown to provide very good result in both approaches.

In 2005, Chen [7] proposed several digital watermarking schemes. They are based on singular value decomposition scheme and had not used DWT, DCT and DFT transforms. They showed that quality of watermarked image is good on their schemes.

In 2006, Wei and Hong [8] proposed a robust digital watermarking scheme for copyright protection of digital images based on sub-sampling. The watermark is a binary image, which is embedded in discrete transform coefficient of the host image and not used in the original image. In this scheme, they had used chaotic map in watermarked image. However the result of watermark image is good and robust than Dong [4].

In 2007, Thang and Patra [9] introduced a novel digital watermarking method, which is based on single key image for extracting different watermarks. In this method, they used independent component analysis technique in watermark embedding and extraction, which is based on public image. With the popularity of internet and availability of large storage devices, storing and transferring a public image is simple and feasible. They showed that robustness of the algorithm against many signal processing operations.

In 2008, Praun et al. [10] presented a robust mesh watermarking algorithm. They generalized spread spectrum techniques based on 2D and 3D surfaces. However, quality of a watermark image is very good.

In 2009, Mei and Li [11] proposed technique with Human Visual System (HVS) characteristics and discrete wavelet transformation (DWT). By using a multi resolution data fusion approach, both image and watermark are transformed into wavelet domain to merge the watermark at the various resolution levels. This method is found to be robust as it embeds the watermark into more salient and strong components of the image. The algorithm is tested against attacks such as JPEG compression, additive noise and two dimensional linear mean filtering. The robustness of the technique is evaluated by normalized correlation coefficient of the extracted and original watermark. The algorithm is robust for the above said attacks. They showed that the algorithm has strong capability of embedding signal and resistant against different attacks.

In 2010, Lamma and Ali [12] suggested two blind, imperceptible and robust video watermarking algorithms that are based on singular value decomposition. Each algorithm integrates the watermark in the transform domain. They used the components of matrices such as U and V. Their schemes are shown to provide very good performance in watermarked video than Chan [6].

In 2011, Lu [13] introduced a new watermarking technique for data hiding in media signal operating in the frequency domain using content based image segmentation. It uses the feature extraction techniques and Voronoi diagram. Voronoi diagram is used to define a group of segment in the host image based on the feature points to be watermarked [14-15]. The segmentation induced by this model is called the Voronoi diagram of the set of the feature points. However, the watermarking scheme can achieve good performance against these signal processing operations.

III. REQUIREMENTS AND APPLICATIONS OF DIGITAL WATERMARKING

In 1998, Cox et al. [16] proposed digital watermarking techniques based on many different applications. Different applications will have different requirements [17-19]. Nevertheless, requirements must be satisfied in several applications area. Some applications of digital watermarking are listed below.

1. Copy Right Protection

Visible watermarking is used for copyright protection which is the most important watermarking application. The owner can protect the audio, image or video data from being used commercially if it is available on internet. The ownership mark should be clearly visible in such cases. Copyright protection demands high level of robustness so that the embedded watermark cannot be removed without data distortion. This watermark is extracted to show as proof if someone claims the ownership of the data.

2. Copy Protection

Copy protection is a particular for digital content because digital copies can be easily made and can be distributed over the internet with no quality degradation. The technical and legal issues that need to be addressed and determined in order to create a working copy protection solution. Those issues are not easy to determine in open system. Copy protection is suitable in closed system. DVD copy protection system has two components as Content Scrambling System (CSS) and MPEG2 video. The extra information have been put in place to provide additional protection for the unscrambled video. Example of analog protection system controls an unscrambled video show on television. In such systems it is possible to use watermarks to indicate the copy status of the digital media (e.g. copy once or never copy).

3. Fingerprinting

Finger printing is similar to giving serial number to any product. Each distributed multimedia copy is embedded with a different watermark. The objective is to convey the information about the legal recipients. A robust watermarking algorithm is required for this application. Watermark is embedded in digital data to trace the source of illegal copies. Information related to customer like serial number or customer identity information is used as watermark. If any illegal copy is found, the source of illegal copy can be found by extracting the watermark.

4. Content Authentication

The aim of this application is related to modification of data. This can be achieved with temper-proofing watermark that have a low robustness to certain modification (e.g. Compression).

5. Broadcast Monitoring

It is used to collect the information about broadcast. This information is used for billing and other purpose. A monitoring is a simple method to observe the human watch broadcast and keep track of everything. This type of broadcast monitoring is expensive and it's liable to error. Self operated monitoring is completely comparative of good. There are two divisions of self operated monitoring system as energetic and submissive. Submissive monitoring systems monitor the condition of being contented about the broadcast and it is difficult to indicate the likeness between the broadcast signals against the database. Energetic monitoring system depends upon extra information and gets the broadcast in one place. The broadcast monitoring solution is able to coexist with equipment for digital and analog signal simultaneously.

A. Security Parameters of Digital Watermarking

In 2003, Bojkovic and Milovanovic [20] introduced a security technique for digital watermarking information. Digital watermarking is gaining importance because of the increased use of internet. Various security schemes for online networks are proposed based on techniques of digitalwatermarking for protecting unauthorized use of digital information.Table 1 gives the comparison of digital watermarking, Table 2 gives the four

classes of watermark and quality of parameters and Table 3 gives the comparison of watermarking schemes [21-22]. Digital watermarking is a useful tool for security applications such as Tracking of printed document source, tamper proofing and assessment, copy control, and finger printing. In essence, one can imperceptibly embed a low-energy signal, called a watermark, containing information such as code or useful public tags in a host multimedia signal to enhance the security feature of the digital information.

TABLE 1. Comparison of Digital Watermarking

Purpose	Visible	Invisible
Validation of intended recipient	---------	M
Non-reputable transmission	---------	M
Deterrence against theft	M	L
Diminish commercial value without utility	M	M
Discourage unauthorized duplication	M	L
Digital notarization and authentication	L	M
Identify source	M	L

A number means (M, N) degree of importance where M represents more and L represents lower

B. Security Tools

In 2001, Seok and Hong [22] introduced digital watermarking technique to provide security in a digital data by making imperceptible modification in original document that can be identified by a machine.It is different from barcode technology as it possess a security characteristics those negate duplication or modification. Even if the unauthorized user detect watermark presence, it is absolutely not possible to remove the watermark in the document as digital watermark varies according to data. Watermark may contain security feature such as document serial number or other information related to data originator such as date of birth. Watermarked documentcan give the information about modifications, counterfeits by comparing the watermarked data to original data [23-24]. The watermark content depends upon the originator or needs to ensure the integrity of the information as well as authentication of the documents. Digital watermarking techniques can be categorized as private and public watermarks.

TABLE 2. Five Classes of Watermarks and Quality Parameters

Watermark	Quality of watermar
Copyright Watermark	○ ○ process is usually private, But public can also be desirable ○ ○ usually more feasible
Fingerprint Watermark	○ Watermark ○ techniques are useful
Broadcast and Copy Control	○ watermark ○ required
Annotation	○ process is usually private, Particular section of community may be worth having ○ important in most cases ○ usually particular ○ contain
Integrity Watermark	○ watermark ○ watermark

TABLE 3.Comparision of Watermarking Schemes

Parameters	Patra et al. [9]	Lu [13]	Chang et al. [7]	Li and Ali [5]	Kim et al. [6]
Cost	H	L	L	H	L
Efficiency	H	H	L	L	H
Attacks	R	JPEG, N	JPEG	N,E,C,R	R,S,T
Method	ICA	SS	SVD	DWT	G
Result	G	G	G	B	B

H – Higher B – Bad ICA – Independent Component and Analysis

L – Lower N - Noise DWT- Discrete Wavelet Transform

G – Good R - Resize SVD- Singular Value Decomposition

1. Private Watermarks

A private or secret watermark may contain information for identifying the licensee or to prove ownership in disputes. Retrieval of secret watermark information requires at least one secret key, known only to the embedder. A private watermark puts heavy demands on a watermarking algorithm regarding robustness, although the demands for capacity are relaxed. Embedded information usually includes licensee-identifying serial numbers or hash values. In general, a serial number is just a pointer or link to externally stored information, such as a customer record.

2. Public Watermarks

A public watermark is retrieved by the receiver (licensee) of copyrighted material. It usually contains copyright or licensing information, such as the identifier of the copyright holder, the creator of the material, or a link (URL) through which to fetch more related information. It may contain a serial number that uniquely identifies material to registration entities. Retrieving a public watermark requires no information but model data itself with a specific key, unique among the material generated by one or various creators or copyright holders. A public watermark puts heavy demands on a watermarking algorithm regarding capacity [25]. Because a public watermark provides additional copyright-related information for receivers and doesn't aim to prove ownership or identify licensees, the requirements regarding robustness are relaxed.

IV. FUTURE DIRECTION

One of the current research areas is to protect digital watermark inside the information so that ownership of that information cannot be claimed by third parties. The future of digital watermarking relies on setting standards and creating applications so that creators of digital content can easily implement it. Digital watermarking can be used in variety of application such as copying protection, pirate tracing, content aunthication and communication. Digital watermarking techniques are used for copyright protection in digital data. The digital information is increasingly exponentially day by day on the web. The watermark should be obtained by legal process, which can be used for transmission and storage. It should be reestablished using common signal processing, such as signal enhancement, geometric operations and noise filtering. It should have various types of characteristics such as manipulations, intentional and accidental simultaneously. Exactly delicate watermark should be allowed alteration in contents.
The watermark should be joined with digital data that cannot be discriminated. Moreover, it should be feasible. The actual data should not be settled due to integration of watermark. It should not possible to remove a digital watermark without intimation demoting the watermarking content. The copyright information as a demand cannot be changed without authorized person. Security watermark can be discovered by original creator. It is debatable that how much information would be integrated in the watermark. It is indispensable to improve the quality of being reliable watermark systems to protect intellectual property and copyrights. Attacks on watermarks would be contemplated in current development of watermarking tools. Areas for development include watermark detection, recovery, and authentication and access control. Substitute use the original cover information to select one watermark, out of a set of available watermarks, which creates the least amount of demolish, and causes the least interference with the original cover. The issues would be related to integrated multi-bit payloads and evaluation of watermarking systems. There are so many applications that can get benefit by applying digital watermarking technology. Protection of intellectual property is very important nowadays because digital multimedia content can be copied and distributed quickly, easily, inexpensively, and with high quality. In this way, digital watermarking techniques for copy right protection would have become increasingly robustness.

V. CONCLUSION

Digital watermarking is one of emerging area of research. We presented a technical discussion on digital watermarking information such as audio, video and image. Digital watermarking can be utilized for aunthication of data, copyright protection and communication process. It is the most common technique for the security of digital information. It is used in security tools, security features and other security parameters. Researchers have proposed various security schemes to protect the ownership of digital information. However, it is hard to satisfy all demands simultaneously. Therefore, standard benchmarks are required to evaluate and compare the performance of different watermarking systems.

REFRENCES

[1] D. Kundur and D. Hatzinakos, "Digital Watermarking Using Multiresolution Wavelet Decomposition", International Conference on Acoustics, Speech and Signal Processing Proceedings, pp. 2969-2972, 1997.
[2] P. Zeng and C. Jin, "Image Adaptive Watermarking Using Visual Models", IEEE Journal on Selected Areas in Communications, vol. 16, pp. 525-539, 1998.
[3] W. Loo and X. Kingsbury, "Digital Watermarking using Complex Wavelets", International Conference on Image Processing, vol. 3, pp. 29-32, 1999.

[4] C. I. Podilchuk, and E. J. Delp, "Digital watermarking: Algorithms and Applications", IEEE Signal Processing Magazine, pp. 33-46, 2001.
[5] L. Rajab, T. Khatib and A. Haj, "Combined DWT-DCT Digital Image Watermarking", Journal of Computer Science, vol. 3, pp. 740-749, 2002.
[6] B. Kim, J. G. Choiand D. Min, "Robust Digital Watermarking Method Against Geometric Attacks", Real Time Imaging Processing, vol. 9, pp. 139-149, 2003.
[7] C. C. Chang and P. Tsai, "SVD-based Digital Image Watermarking Scheme", Pattern Recognition Letters, vol. 26, pp. 1577-1586, 2005.
[8] W. Hong and M. Hang, "Robust Digital Watermarking Scheme for Copy Right Protection",
IEEE Trans. Signal Process, vo.l2, pp. 1- 8, 2006.
[9] T. V. Nguyen and J. C. Patra, "A Simple ICA based Digital Image Watermarking Scheme", Digital Signal Processing, vol. 18, pp. 762-776, 2007.
[10] H. Tina, W. Lu, R. prawn and Y. Ming, "A Fragile Watermarking Scheme for 3D meshes", MM-SEC'05, ACM, pp. 117-123, 2008.
[11]M. Jiansheng and L. Sukang, "A Digital Watermarking Algorithm Based on DCT and DWT", International Symposium on Web Information System and Application (WISA), PP. 104- 107, 2009.
[12] A.H. Ali, M. Ahmad, Digital audio watermarking based on the discrete wavelets transform and singular value decomposition, Eur. J. Sci. Res. vol. 39 no. 1, pp. 6-21, 2010.
[13] W. Lu, H. Lu and F. L. Chung, "Feature Based Watermarking Using Watermark Template Match",Applied Mathematics and Computation, vol. 177, no. 1, pp. 886-893, 2011.
[14] A. Kumar and V. Santhi, "A Review on Geometric Invariant Digital Image Watermarking Techniques", International Journal of Computer Applications, ISSN-09 vol. 12, no14, pp. 31-36.
[15] Y. Lu, K. Uehira, and K. Yanaka,"Practical Evaluation of Illumination Watermarking Technique Using Orthogonal Transforms", Journal of Display Technology, vol. 6, no. 9, pp. 351-358, 2010.
[16] I. J. Cox, J. Kilian, F. T. Leighton and T Shamoon, "Robust Watermark for Multimedia", Proc. of the 1st Information Hiding Workshop, New York, LNCS, vol. 1300, pp.183-206, 1997.
[17] M. Barni and B. Bovid, "Digital Watermarking for Copyright Protection: A Communication Perspective", IEEE Communication Magazine, vol. 39, no. 8, pp. 90-91, 2001.
[18] A. Kumar and V. Santhi, "A Review on Geometric Invariant Digital Image Watermarking Techniques", International Journal of Computer Applications, vol. 12, no. 14, pp.31-36, 2010.
[19] F. Petitcolas, R. Anderson and M. Kuhn, "Attacks on Copyright Marking Systems in Information Hiding", LNCS, Berlin, vol. 1524, pp. 218-238, 1998.
[20] Z. Bojkovic and D. Milovanovic, "Multimedia Contents Security :Watermarking Diversity and Secure Protocols", 6th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Service, TELSIKS, vol. 1, no. 3, pp. 377-383, 2003.
[21] I. J. Cox and J. P. Linnartz, "Some General Methods for Tampering With Watermark", IEEE Journal on Selected Areas in Communications, vol. 16, pp. 587-593, 1996.
[22] S.J. Lee, S. H. Jung, "A Survey of Watermarking Techniques Applied to Multimedia", IEEE Transactions on Industrial Electronics, vol. 12 pp. 272-277, 2001.
[23] Y. Trank and W. Frank," Robust Image Watermarking in The Spatial Domain", Signal Processing, vol. 13, no 14, pp. 385-403, 1997.
[24] E. Koch and J. Zhao, "Robust Labels into Images for Copyright Protection", International Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies, Vienna, pp. 1064-1087, 1985.
[25] P. K. Dhar and M.I. Khan, "A New DCT-based Watermarking Method for Copyright Protection of Digital Audio", International Journal of Computer Science & Information Technology (IJCSIT), vol. 2, no. 5, pp. 91- 97, 2010.