Role of Digital Watermark in e-governance and e-commerce

Mrs. S.S.Sherekar†, Dr. V.M.Thakare††, Dr.Sanjeev Jain†††

† SGB Amravati University (M.S.,India)
†† SGB Amravati University (M.S., India)
††† SATI,Vidisha (M.P., India)

Summary
Watermarking techniques, for four media data - video, image, audio, and text are interpreted as DWvideo, DWimage, DWaudio and DWtext respectively in DWM techniques respectively..

In this paper, we focus on important role of digital watermark in electronic governance and electronic commerce applications. Results show that watermarks for video and audio data have to be invisible and robust, and watermarks for text data has to be invisible and fragile, while watermark for image has to be either visible and fragile, or invisible and robust for electronic governance and electronic commerce applications. The watermark is used to protect intellectual property in electronic governance and electronic commerce applications. This facilitates electronic governance and electronic commerce application developers to select adequate digital watermarking techniques for their development.

Key words:
e-governance, e-commerce, digital watermark, fingerprinting, integrity verification

1. E-governance, e-commerce and Watermarks

E-commerce Businesses is communicated with customers and partners through channels. The internet is the newest and best business communication channels. It is fast, reasonably reliable, inexpensive and universally accessible. Doing business online is electronic commerce and there are four main areas in which companies conduct business online today: direct marketing, selling and service: online banking and billing: sharing and distribution of information.

What is the new and urgent need is to secure a high number of critical applications from unauthorized use. Today's e-commerce suffers from security risks. This is the dark side of the e-commerce. Any user can open a direct pipeline to the enterprise's most valuable information assets, presenting a tempting target fraud, malicious hackers and industrial espionage.

E-governance and e-commerce sites have digital content representations of the copyrighted material. However, it is the fact that an unlimited number of perfect copies can be illegally produced, is a serious threat to the rights of content owners. Until recently, encryption[1] has been the primary tool available to protect content owners' rights. Encryption protects content during the transmission of the data from the sender to receiver. However, after receipt and subsequent decryption, the data is no longer protected. One of the solution to this problem is a digital watermarking system[2, 3, 4].

A digital watermark is a piece of information that is hidden directly in media content, in such a way that it is imperceptible to a human observer, but easily detected by a computer.

When digital watermarks are used for intellectual property protection, many e-governance and e-commerce applications are beneficial and they include the online and offline distribution of multimedia content, broadcast services, document verification, ownership identification and so on. This also benefits content creators – artists, authors, and movie studios; content providers – photo stock archives, libraries, and professional photographers; electronic commerce and graphics software vendors; and manufacturers of digital still images, video cameras and digital video discs (DVDs). Numerous electronic business web sites are found in the Internet which contains all types of data, i.e. text, graphics, audio, video etc as well as they are typical e-governance and electronic commerce applications. All of these sites needs intellectual property protection. The type of the web site together with the media data types and types of digital contents decides the type of watermark used in that application for the site security.

2. Requirements of digital watermarks for web contents

It must be noted that one of the basic requirements for web content based digital watermarking is to maintain the quality of the original data not being distorted when a watermark is embedded into it[3, 4]. Besides, there are other requirements that are necessary for specific applications like e-governance and e-commerce. Perceptual transparency and robustness [5] are the most common requirements for such applications. Some other requirements, such as capability to recover data without original data, bit rate of data embedding algorithm, security, unambiguous proof of ownership, etc. are also required for such specific applications[6].

Manuscript received January 5, 2008
Manuscript revised January 20, 2008

2.1 Perceptual transparency: Perceptual transparency means that the embedded watermark is undetectable perceptually. If humans cannot differentiate between the original data and the watermarked data, the watermark is imperceptible. Blind tests are usually conducted to measure the perceptual transparency, where human subjects are presented with data with or without watermark randomly and asked to determine the quality. Perceptual transparency is required for applications in copyright protection, usage tracking and embedded metadata.

2.2 Robustness: The watermarked data is generally processed by some signal processing operations. After operations, the watermarked data is modified or manipulated, the embedded watermark may have been destroyed. The robustness of watermarking ensures that the embedded watermark will not be destroyed after such operations. As a result, third parties are not able to modify the watermarked data to thwart detection of the embedded watermark. A watermarking technique that is not robust is called fragile watermarking. Web applications, such as, data storage and transmission may perform coding operations in order to reduce bit rates. Robustness is important in these applications.

3. Specific applications of digital watermarks for web contents

In such cases of e-governance and e-commerce, watermarks has several applications[7] including:

3.1 Signatures 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.

3.2 Fingerprinting Watermarks can also be used to identify the content buyers. This may potentially assist in tracing the source of illegal copies.

3.3 Broadcast and publication monitoring As in signaturing, the watermark identifies the owner of the content, but here it is detected by automated systems that monitor television and radio broadcasts.

3.4 Authentication Here, 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 sometimes referred to as a *vapormark*.

3.5 Copy control The watermark contains information about the rules of usage
and copying which the content owner wishes to enforce. Devices which are capable of copying this content can then be required by law or patent license to test for and abide by these watermarks. Furthermore, devices that can play the content might test for the watermarks and compare them with other clues, such as whether the content is on a recordable storage device, to identify illegal copies and refuse to play them. This is the application that is currently envisaged for digital videos and disks.

3.6 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[8] – the hiding of one piece of information within another.

4. Parameters of digital watermarks in web based contents

Web oriented commercial watermarking systems [9, 10, 11] have been proposed to focus on the copyright protection of web contents in the form of digital media data in e-governance and e-commerce. Four parameters are used in the categorization of digital watermark [9]; they are perceptible, imperceptible, robust and fragile. Some of these parameters are mutually exclusive; for example, a watermark cannot be perceptible and also imperceptible. The four parameters can be defined as follows:

4.1 Fragile - Fragile watermarks are easily corrupted by any form of processing procedures. An application used only to indicate modifications of the content needs only a fragile watermark.

4.2 Perceptible - Perceptible watermarking embeds data intended to be visible or audible. There are two important criteria for a good perceptible watermarks. First, it must be difficult for an unauthorized person to remove it. Second is, a good perceptible watermark also has to resist falsification. Since it is relatively easy to embed a pattern or logo into a data, we have to ensure the perceptible watermark was indeed inserted by the claimed user.

4.3 Imperceptible – Imperceptible watermarking embeds data intended to be invisible or inaudible but that can be extracted by a computer.

4.4 Robust - Robust watermarks resist common signal processing procedures, such as cropping, filtering and are useful for ownership assertion purposes. Two major classes of robust watermarking techniques are private and public (or oblivious). A private scheme requires an original or reference content in the watermark detection

procedure; a public scheme does not. Public schemes are attractive for many electronic commerce applications, as it is impractical to use private scheme. An application in which a digital watermark is used to identify proper ownership needs a very robust watermark.

5. General Watermarking Techniques for e-governance and e-commerce

Digital watermarking has many different techniques. Watermarking techniques are usually designed for specific applications and may not be applicable for other applications[12]. Here it is first reviewed a list of possible applications and then identified the requirements for the specific applications like e-governance and e-commerce.
Three basic watermarking procedures are required in digital watermarking[13] and they are watermark insertion, watermark detection and watermark extraction. In general, watermark insertion requires (i) an original data, (ii) a watermark, and (iii) and a private key. The output is the watermarked data as shown in Figure 1. The watermark can be information about ownership, user identity, description of the original data, etc. The watermark insertion procedure is to embed a watermark into the original data. The watermark can be perceptible or imperceptible in the watermarked data depending on the applications. For applications requiring the original data not being distorted, imperceptible watermark is desired. For some other applications, which require displaying the embedded data, a perceptible watermark is preferred.

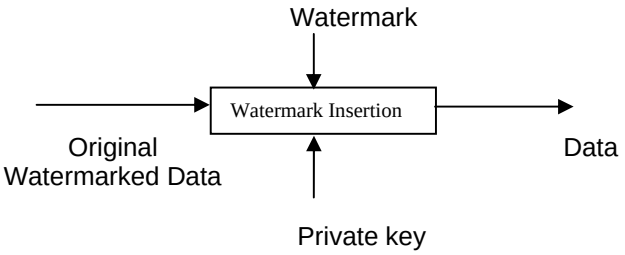


Figure 1. Watermark Insertion.

Watermark extraction and watermark detection as shown in Figure 2 and Figure 3 are used to retrieve the embedded watermark from the watermarked data. For watermark extraction, a public key is used together with the watermarked data to retrieve the embedded watermark. For watermark detection, a public key and a specified ID - watermark are used together with the watermarked data to determine whether the watermark is correct.

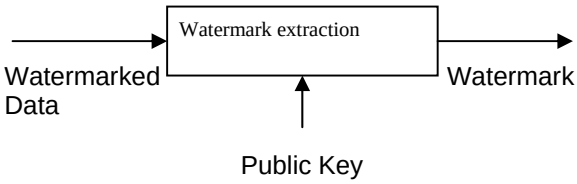


Figure 2. Watermark Extraction.

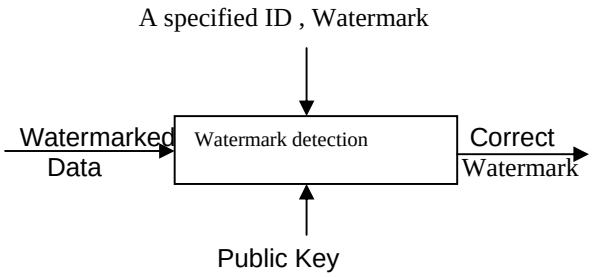


Figure 3. Watermark Detection.

There are two domains for watermarking technology-spatial domain and transform domain[14,15,16]. Watermarking in e-governance and e-commerce is the process of embedding data (or controlled distortion) into a multimedia element such as image, audio and video. This embedded information, or the watermark, can later be extracted from the multimedia and used for security purposes. In such multimedia applications, the watermark should be invisible to the human observer. A watermarking algorithm consists of the watermark structure, an embedding algorithm and an extraction or detection algorithm. Watermarks can be embedded into multimedia directly (e.g., the time domain) or after the multimedia element has been transformed (e.g., the discrete cosine transform). Performance issues include robustness to attack (attempts to remove the watermark), capacity (how bits can be hidden in the multimedia) and how transparent is the watermark under normal viewing or listening conditions.
There are various methods in transform domain based on spared spectrum sequence in Fourier or DCT domain coefficient.
In spatial domain , methods can be mainly classified as LSB based, blocked based, statistical and feature point based.

6. Efficient design best suited for e-governance and e-commerce

In this section the efficient design, algorithm or method which will be best suited for current technologies and current trends like e-governance and e-commerce is proposed.

Typical uses of watermarks include identification of the origin of content, tracing illegally distributed copies, and disabling unauthorized access to content. A mature robust watermarking technology should be resistant to many types of attacks and normal A/V processes such as noise, "filtering, resampling, cropping, data compression etc. Fig shows the efficient design to test originality of the image for e-commerce and e-governance.

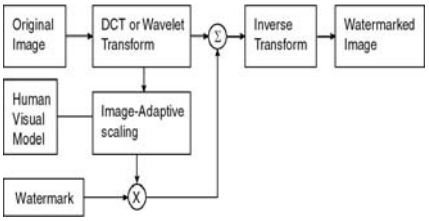


Fig : Efficient design to test originality of the image for e-commerce and e-governance

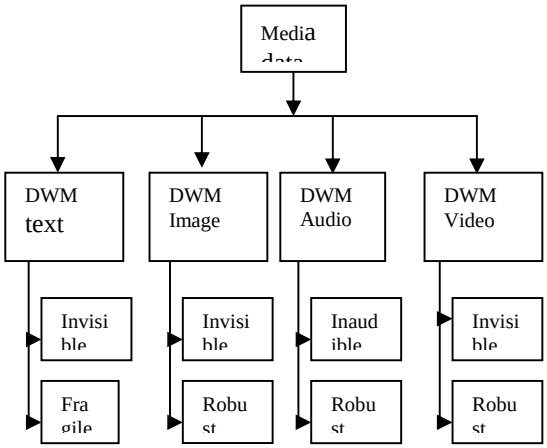
7. Experimental results

Developers who are willing to use digital watermarking can easily identify appropriate techniques and commercial systems that best fit for e-governance and e-commerce applications. Digital watermark (DWM) is introduced for a particular media data. For instance, a watermark for image data can be invisible and fragile, whilst a watermark for audio data can be inaudible and robust. Different watermark are used in different applications due to their differences in digital contents and media data used in applications. The general watermark design pattern – DWM media data is a complete structure that covers all possible watermarks that may be found in e- governance and electronic commerce applications, regardless the media data type of digital contents. The characteristic of digital watermark, described in the general DWM, expresses that it can be either perceptible or imperceptible, and for either case, it can also be robust or fragile.

After studying the various media data, a general strategy of the DWM is derived.

It is noted that watermarks for audio and video data have to be inaudible and invisible respectively, as listeners and watchers like to enjoy these types of media in a noise-free environment. It is because perceptible watermark could be a source of noise from the user's point of view. Watermarks for audio and video data also have to be robust, in the sense that the watermarks can survive after undergoing various common attacks, such as cropping and filtering. Watermarks designed for text documents and manuscripts, has to be invisible, as these documents are already blur after digitization. Any additional noise can likely turn the documents to be unreadable. Any changes or modifications must be noticeable to the viewers and owners. Thus, invisible and fragile watermarking is preferable to text data. For image data, watermarks can be visible and invisible depending on the purposes of the application and digital contents. For promotion and demonstration purposes, digital photograph may carry a visible watermark that can be a company trademark or a copyright mark, When perceptibility of digital contents is a concern, an invisible watermark is a better choice. All existing invisible image watermarking techniques and systems in the literature are robust, while all visible image watermark techniques and systems are fragile.

Using the above results, we conclude the characteristics of watermarks for the four different media data and their corresponding DWM as shown in Figure



* watermark for audio data

DWM audio should be inaudible and robust.

* for video data watermark

DWM video should be invisible and robust.

* Watermark for text data

DWM text should be invisible and fragile.

* Watermark for image data .

DWM image should be invisible and robust.

8. Conclusion

E-governance and e-commerce applications require protection to prevent the misuse of the material they mount for public consumption. However, only a few electronic commerce application developers apply efficient techniques to protect digital contents in their applications, mainly because they are unfamiliar to the technology. Our objective was to develop a scheme that can facilitate electronic commerce application developers to choose adequate digital watermarking techniques for their applications in an efficient way. In this paper, we have proposed watermarking system (DWM) to describe the characteristic of a digital watermark for e-governance and e-commerce type of specific media data.

References

[1] B.M.Macq and J.J. Quisquater. *Cryptology for digital broadcasting . In Proceeding of the IEEE,volume 83*,pages 944-957,June 1995

[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] R. B. Wolfgang and E. J. Delp, "Overview of Image security Techniques with applications in multimedia system", Proc. of SPIE conf.on multimedia networks,vol. 3228, pp297-308, Dallas Texas, 1997

[4] C.W. Zeng, Podilchuk, "Image adaptive watermarking using visual models", IEEE journal on communications, vol 10,no. 4, pp 525-540

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

[6] M. A. Suhail. "Digital Watermarking for Protection of Intellectual Property." In Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property, Chun-Shien Lu, ed. Idea Group Publishing, 2005.

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

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

[9] B. Chandra Mohan, Srinivaskumar, B. N. Chatterjee,"Digital Image and binary images", Int. Journal Imaging systems and Tech., vol 14, no. 4, pp 147-152,, Int. Conf. Proc Vie.2006

[10] Frank Shih, scott Wu, Combinational image watermarking in the spatial and frequency domains, Pattern Recognition 36 pp 969-975,2003

[11] C.S. Lu and Chao Yong Hsu ," Content Dependend watermarking resistance against generalized copy attack", Proc. IEEE international conference on multimedia and expo, Taipei Taiwan ,2004

[12] P. Bass, J.M. Chassery & B. Macq, " Geomatrically invariant Watermarking Using feature points" , IEEE Trasaction on image processing, Vol. 11, No 9, pp 1014 – 1028.,2002

[13] Chuhong, Deepa Kundur, Kwong, Analysis and design of secure watermark-based authentication systems ,IEEE transactions on information forensics and security,1(1),pp 43-45,March 2006

[14] G.L. Guelvouit & Stephane Pateux , " Wide spread spectrum watermarking with side information and interference cancellation", proceeding of SPIE Santa clara CA, Jan 2003

[15] Frank Shih, scott Wu, Combinational image watermarking in the spatial and frequency domains,

[16] Y. Wang, J. F. Doherty, and R. E. Van Dyck, "A Wavelet-Based Watermarking Algorithm for Ownership Verification of Digital Images", IEEE Transactions on image processing, Vol. 11, No. 2,7788, Febrmay 2002 Pattern Recognition 36 pp 969-975,2003

Swati Sherekar received the degree of M.Sc. in compuer sciencein 1994 from Amravati University, Amravati, Maharastra, India. Presently working as Sr. Lecturer in the P. G. Department of Computer Science and having 12 years of teaching experience. Her area of research is Network security, Image Processing and pursuing her Ph.D. in Digital Watermarking for multimedia authentication. She has authored more than 25 research papers at national / international level conferences and journals. She is also working on research projects in this area.

Dr. V.M.Thakare is presently working as Sr. faculty at Department of Computer, SGB Amravati University, Amravati Maharashtra, India. He has received **M.E.**(Advance Electronics from Amravati University, P**.G. DCM**, from IICM, Ahamadabad and Ph.D. in Computer Science . He is having **21 years** of teaching and **14 years** of R&D experience in the field of Computer & IT. He has also served as head of deptt. Of computer science for more than 9 years and served as chairman/member of many expert/technical committee at state and national level. He has also received national level excellent paper award at national level.

He has been actively involved in the research in the area of Robotics and AI, Computer Architectures, ICT, Software Engineering, Wireless Technology and Networking. About 13 research scholars are pursuing for Ph.D. degree under his guidance. He has authored 80 **research papers** at various National / International Conferences and Journals like **IETE, Technimont, IEEE** proceeding and other. He has been invited as a **Keynote Speaker, Invited Speaker, Session Chair** and **Reviewer** for more than 18 International & National Conferences.