Digital Watermarking for Secure E-Government Framework

Dilip Kumar Sharma[1]*, Vinay Kumar Pathak[2] and G.P. Sahu[3]

ABSTRACT

During the last decades there has been a tremendous and potential growth in the area of digital media such as text, 2D image, 3D object, audio and video because of their efficient storage, ease of manipulation and transformation but on the other hand these characteristics has made digital media a soft target for unauthorized use. In the last few years, the various techniques are proposed to protect the digital media from unauthorized use. One of such techniques is digital watermarking in which the information contents of any audio, video or image (2D or 3D) is changed by embedding certain data into original data. The embedded data is imperceptible to humans, but can be read by computers or other devices enabled with special secure software and scanner devices. Now a day's electronic Government gaining much importance so the digital watermarking can play a significant role in the area of electronic Government to protect as well as detect the illegal use of digital information. In this paper an attempt has been made to explore the capabilities of digital watermarking as a secure electronic Government framework.

***Keywords*:** Digital watermarking, e-Government, security, Information Communication Technology (ICT)

1. Introduction

E-Government can be visualized as utilization of information and communication technologies for the service of citizens, businesses and other areas of Government. E-Government is a way for government to use the new technologies to provide people with more convenient access to government information and services, to improve the quality of the services and to provide greater opportunities to participate in democratic institutions and process (EzGov, 2000). E-Government involves new styles of leadership, new ways of debating and deciding policies and investments, new ways of accessing education, new ways of listening to the citizens and new ways of organizing and delivering information and services (Kerry Ferguson, 2000). The primary objective of e-Government is betterment of Government services for the citizens, improvement in bilateral interactions with business and industry, transparency in system, revenue growth and or cost reduction. During the present Government system, Government not only providing information unilaterally to the citizens, businesses and other arms of Government but they are also interacting bilaterally for understanding various issues from the other side. On a better hand e-Government system provides a overall efficient systems but as it is based on communication based technologies. So security is the key issue for an efficient e-Government system. Network and information security is the main issue in realizing an efficient e-Government system. Security threats such as virus, trozen horse,

[1] G.L.A Institute of Technology & Management, Mathura, India
[2] H.B.T.I. Kanpur, India
[3] M..N. National Institute of Technology, Allahabad, India
* *Corresponding Author:* (Email: todilipsharma@rediffmail.com, Telephone: +91-9927031755)

spamming, worm and invasion can result due to lack of security features in e-Government system. Government is supposed to provide a secure e-Government system via information communication technology based network. Most of the security threats in e-Government arises due to the following points: The Internet is a bilateral network, Web server and web browser are very complicated software systems having various potential flaws (Hacked web browser and web server can be used by hacker/cracker for conducting further attacks against users and Government organization).

Primary security issues (that may be isolated or combined) in e-Government are confidentiality, information integrity, information authentication/copy right protection, non- repudiation, copy control etc. Any ICT based system must be very secure to protect the confidentiality of information of people/citizens and business persons generally have confidential information. Security, authenticity and verification should go with privacy laws and Government have to ensure the efficient protection of confidentiality and privacy of information. Digital watermarking is basically identified as a tool for copyright protection/ authentication of digital data but due to its inherent characteristics it may improve the security feature of e-Government system.

2. Security Issues in e-Government

In the designing of an efficient e-Government system, security becomes the main issues to be considered. E-Government system is type of on-line system that require a ICT based network to execute properly but e-Government system is different from other on-line system particularly with reference to security as an e-Government system handles a lot of secure and legal information that must be protected from unauthorized users. The Canadian Government is using an advanced Web portal called BusinessGateway.ca not only making available information and communication similar to the Austrian Help.gv but also secure transaction services for businesses (A. Moller, 2000). Security is critical for their successful implementation for e-Government and transaction based services. Some of the security issues in e-Government are discussed below:

- Confidentiality Information should not be accessible to unauthorized users.
- Authenticity When information is received, it should be verified by a person or a project claming to be originator and vice versa.
- Integrity On retrieval or received at other end of a communication network the information should appear exactly as was stored or sent.
- Non- repudiation After sending/authorizing a message the sender should be unable at a letter time, denying having done so.

Table1: Security Threats and their solution in an on-line system/project

Threat	Security	Function	Technology
Data intercepted or modified illicitly/ Data integrity	Encryption Algorithm/ Hash Function	Encode data to prevent tampering	Cryptography Algorithms, MD5/ SHA etc.
Unauthorized user on one network gains access to another	Firewall	Firewall prevents certain traffic from entering the network or server	VPN / Firewall
False Identity with an intention of fraud	Authentication	Identity verification of both sender and receiver	Password/Digital Signature
Copyright protection of data	Digital watermarking	This type of data is copyrighted but not secret.	Digital Signal/Image Processing, watermarking

3. Digital Watermarking as a security tool

Digital watermarking is a technique to provide security in a digital data by making imperceptible modification in original document that can be identified by a machine but may or may not by a human eye.

It is different from barcode technology as it possess a security characteristics require duplication or modification. Even if the unauthorized user is known to 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 to originator such as date of birth. Watermarked document can give the information about modifications, counterfeits by comparing the watermarked data to original data. The watermark content depend 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.

Private watermarks

A private (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.

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 the model data itself plus 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. 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.

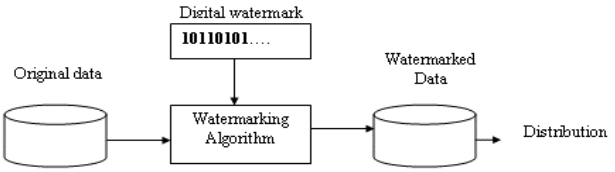

Figure 1(a): Digital watermarking embedding process

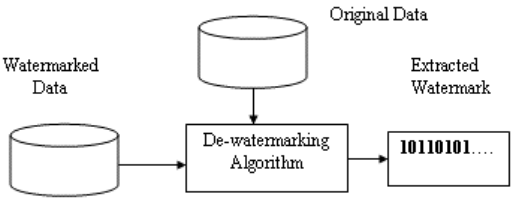

Figure 1(b): Digital watermarking extraction process

Figure 1(a) and Figure 1(b) shows the digital watermarking embedding process and digital watermarking

extraction process respectively in general.

3.1 Characteristics of Digital Watermarking

A watermark is designed to permanently reside in the host data. When the ownership of data is in question, the information can be extracted to completely characterize the owner. To achieve maximum protection of intellectual property with watermarked media, several requirements must be satisfied:

- Undeletable: The watermark must be difficult or even impossible to remove by a malicious cracker, at least without obviously degrading the host signal.
- Statistically undetectable: A pirate should not be able to detect the watermark by comparing several watermarked signals belonging to the same author.
- Robustness: Watermark should be recoverable, which is commonly used for transmission and storage. The watermark should be retrievable even if common signal processing operations are applied, such as signal enhancement, geometric image operations and noise filtering. Watermark should remain in the cover/content after various types of manipulations, both intentional and accidental. Even a fragile watermark should withstand normal alterations. Tolerance against well-defined modifications is essential (Hao-Tian Wu and Yiu-Ming Cheung, 2005).
- Unambiguous: Retrieval of the watermark should unambiguously identify the owner, and the accuracy of identification should degrade gradually in the face of attacks.
- Imperceptibility: A watermark should be integrated with digital data such that it can not be distinguished. The watermark should be perceptibly invisible or transparent (imperceptible). The actual data should not be compromised due to the embedding of watermark. It should be difficult or impossible to remove a digital watermark without noticeably degrading the watermarking content (cover). This is a requirement as the copyright information cannot be altered or modified without authorization.
- Tamper resistant or tamper evident: Any modifications of the watermarked cover should be identified or traced technically.
- Survive multiple encoding or decoding: Difficult to create or extract legitimate watermark without credentials.
- Payload*:* Larger payload is desirable, particularly for applications involving multiple transactions, such as buying and selling.
- Low computational complexity: It should not be the complex for embedding and extracting the watermark. It is crucial for real time applications.
- Secret key: Key for watermark indicates or identifies without any ambiguity the creator of the work, so that it can be used for data authentication and identification.

3.2 Types of Digital Watermarking Attacks

Simple attacks attempt to damage the embedded watermark by manipulating the whole watermarked data, without separating the watermark. It include linear and general non-linear filtering, waveform-based compression (.jpeg, .mpeg), addition of noise, addition of a cropping, quantization in the pixel domain, conversion to analog, and correction. Detection-disabling attacks try to break relationship between watermark and host data so it is impossible to identify the watermark. This is done mostly by geometric distortion like zooming, shift in spatial or temporal (for video) direction, rotation, shear, cropping, pixel permutations, sub-sampling, removal or insertion of pixels or pixel clusters, or any other geometric transformation of the data. A typical property of this type of attacks is that the watermark remains in the attacked data. Typically, it can be recovered with increased intelligence of the watermark decoder. Ambiguity attacks (other possible names include confusion attacks, deadlock attacks, inversion attacks, fake-watermark attacks and fake-original attacks) attempt to confuse by producing fake data. In an ambiguity attack, the attacker tries to fake a watermark and an object such that the watermark is embedded in the alleged “original” object. Removal attacks attempt to: Analyze the watermarked data, estimate the

watermark or the host data, separate the watermarked data into host data and watermark, discard only the watermark.

3.3 Security features of Digital Watermarking

To design an e-Government framework, security has become a key issue that needs to be addressed, like any other online system. Security is critical in e-Government system to safeguard the confidentiality of transactions and information on the network. Government document and other important material such as birth and death certificate, motor vehicle license, land record, all of which have legal and legislative nuances have to be protected from unauthorized user. As digital watermarking in general have various application in different areas such as protection of intellectual property rights (IPR), decision of right owner, finger printing, copy control, authentication, error recovery, annotation, labeling for data retrieval, linking real objects to the digital world and secret communication etc. We will discuss the capabilities of these features of digital watermarking for the use of electronic Government.

Tracking of printed document source

Several printer companies quietly encode the serial number and the manufacturing code of their color laser printers and color copiers on every document those machines produce. Governments, including the United States, already use the hidden markings to track counterfeiters. In a typical scenario, when distributors sell printers, they obtain information about the purchaser, which is maintained in a database. The purchaser's identity is then associated with the serial number and the manufacturer's name of the machine. A document whose author a governmental agency wants to discover contains only the serial number and the manufacturer's name of the machine on which it was printed, so upon extracting this information from a document, it must consult the distributor responsible for selling the machine. The distributor performs a database query to match the serial number with a purchaser; manufacturers can also do searches if they have access to the database (Jason Tuohey, 2004).

Intellectual Property Right (IPR) Protection

The protection of Intellectual Property Right or IPR protection is the very first targeted application of digital watermarking. This term includes the protection of the rights of the creator, the rights of the legitimate owner, copyright protection, moral rights protection (e.g. the integrity of the work in the respect of the moral beliefs of the creator), and so on (Herzberg and Pinter, 1987). Three of the major tasks in IPR protection area are: demonstration of the ownership in legal disputes, fingerprinting, and copy control. It is very tough to protect the piracy of digital contents. 3D models creation is costly as well as effort taking so protections of these models are very important and responsibility of government.

Decision of Right Owner

In this context the creator of a work (e.g. a song, a picture, a movie or an object) wishes to prove that he is the only legitimate owner of the work. To do so, a watermark identifying him unambiguously is embedded in the work. As previously stated, for this kind of application, it is necessary to use a watermarking algorithm that assures inevitability or non-quasi inevitability of the watermark. A common way to confer a legal value to the verification procedure through watermark detection is to introduce the presence of a Trusted Third Party (TTP) that assigns a unique registration code to the owner of the work in order to proof the ownership of the registered asset without ambiguity. The governmental body can be worked well as TTP so there is requirement of attention on this area while developing and implementing e-Government framework (B.-L. Yeo and M. M. Yeung, 1999). Watermark can inserted to e-mark sheet to prove the identity of candidate or admit card and verification cards.

Fingerprinting

In this case the watermark identifies the buyer of a digital content. This mechanism represents a deterrent against illegal copy of digital contents by discouraging people to make illegal copy of the watermarked

content. In fact, potentially, it is possible to trace back the illegal copies to identify the hackers of the content. From governments point of view, with the explosion of Internet and peer-to-peer downloading programs, this application is becoming one of the most attractive applications of digital watermarking. Even in this case the watermarking system must exhibit secure robustness. Watermark readability is also a useful property in this context. Watermarked documents such as (watermarked legal documents, mark sheets, forms etc.) discourage the unauthorized copying as removing of watermark can result in distraction of document.

Copy control

When copy prevention systems, such as fingerprinting and ownership demonstration, are not sufficient to protect legitimate right-holders an effective copy protection mechanism must be used. Watermarking technologies, in this context, is only an important part of the whole copy protection system (Barni, M., 2001). In fact, to make a copy protection system effective, a lot of different aspects and problems must be taken in account. For example, recording and playback devices should be designed to give them the capability to recover watermark information inside an asset, and, to decide whether to allow or not, the copy of such asset. A good example of this approach is the copy protection system being developed for DVD technology. In case of e-Government various types of forms can be copied to make various fake multiple copies of the same serial number. This can be discouraged by the use of watermarking.

Authentication

In this application the watermark encodes information required to determine if a digital content is authentic. Imagine a government body circulates a document for a certain event; it is important to guarantee that such document is authentic and that it has not been manipulated or altered in any way [NIST,2004]. For this purpose a semi-fragile watermark can be used. This information can be watermarked by document editing software. After this, if the watermark is correctly recovered, Its a guarantee that the asset is authentic, i.e. it has no suffered any kind of manipulations or alterations. Authentication can be achieved even by robust watermarking. In this case, the watermark carries a summary of the original work. After extraction, to prove data integrity, the summary is compared with the expected one, at this point any mismatch indicates that data tampering has occurred. This can be more important when land registration or construction related 3D data are used. This application can be useful at the user side to authenticate that the data is legal or illegal by using a watermark key.

Error recovery in transmission

The complex network and large size of e-Government framework make the transmission of data in compressed form, such as JPEG for still images, or MPEG-2 or H.263 for video, is very vulnerable to transmission errors. In particular, for video streaming, a single bit error can cause a loss of synchronization that will be visible over an entire group of frames (GOP). To circumvent this problem a controlled amount of redundancy can be introduced at the transmission level in order to recover from errors. For example, one solution could be the use of error correcting codes. Watermarking could be a valid alternative to solve this problem: the redundant information is embedded within the compressed bits stream and used by the decoder to recover from transmission errors. In this kind of feature robustness requirement is relaxed since the watermark must survive no attacks except transmission errors. On the other hand, capacity assumes greater importance, since high capacity allows the transmission of a large amount of redundancy, thus resulting in excellent robustness against errors.

Annotation

In this context the watermark conveys simple annotation or labeling data. Watermarking presents a lot of advantages with respect to conventional techniques to associate such data, for example by using an external database or a header. One of these advantages is the capability of the watermark to survive the digital to analog and analog to digital conversion. Other advantages will be clear in the next, when one can describe a

couple of examples just to give an idea of the potential of watermarking technology in this field. The main requirement for such features is high capacity, while the robustness requirement is usually relaxed.

Labeling for data retrieval
Content-based access to digital archives is receiving more and more attention since nowadays the efficient management of database of multimedia objects, such as images and video, has assumed great importance. Since it is very difficult to automatically analyze the semantic content of the digital objects and retrieve them in the database, a semantic description is associated to each object, typically through a header. The usefulness of watermarking with respect to conventional data labeling, in this context, can be identified by considering an archival of video sequences in MPEG-4 format. Imagine that each video object of the MPEG-4 stream is watermarked with its associated information. At this point, if a watermarked video object is edited to create a different video sequence its associated information are automatically copied with it avoiding the necessity of labeling it again. Similarly, if the object is pasted to a new video after going in analog and back to digital domain, the annotation watermark is not lost, making the semantic description of the new video easier.

Linking real objects to the digital world
Another remarkable example concerns the association between a real object and the digital world. The Media bridge system developed by Digimarc Corporation is an example of such vision of watermarking. In this case the value of an image is augmented by embedding within it a piece of information that can be used to link the image to additional information stored on the Internet. For example, such information can be used to link a picture on a newspaper to a web page further exploring the subject of the article. The embedded URL is activated by showing the printed picture to a video camera connected to a PC. Online systems are vulnerable to hackers, and the government has an obligation to prevent the unauthorized disclosure of personal information as well as prevent forgery and alteration of official documents

Covert communications
One of the earliest features of watermarking is sending secret messages. This feature has been modeled by Simmons as the prisoner's problem in which two prisoners want to communicate each other in order to run away from the prison. The problem is that they cannot send directly messages but the prisoner warden act as a messenger. The warden is willing to carry innocuous message but will punish them if he finds that, such messages contain information about escape-plan. The solution is to disguise the escape-plane messages as innocuous messages. As previously stated this feature is more correlated with steganography as watermarking. In fact, in steganographic, imperceptibility assumes a wider sense, i.e. the presence of the hidden message cannot be revealed by any means, such as visual inspection, statistical analysis, etc. So, in this kind of feature, the indefectibility of watermark presence becomes a new requirement for the digital watermarking system.

Software Obfuscation
Software protection has been considered as an amalgamation of watermarking, tamper-proofing, and obfuscation philosophies (Collberg and Thomborson, 2002). Because only authenticated software can sustain secure environment for e-Government.

3.4 Common Attacking Techniques

- Additive noise: This may stem in certain applications from the use of digital to analog (D/A) and analog to digital (A/D) converters or from transmission errors. However, an attacker may introduce perceptually shaped noise (thus, imperceptible) with the maximum unnoticeable power. This action will typically increase the threshold at which the correlation detector works.
- Cropping: This is a very common attack since in many cases the attacker is interested in a small

portion of the watermarked object, such as parts of a certain picture or frames of a video sequence. With this in mind, in order to survive, the watermark needs to be spread over the dimensions where this attack takes place.

- Rotation and scaling: This has been the true battle horse of digital watermarking, especially because of its success with still images. Correlation-based detection and extraction fail when rotation or scaling are performed on the watermarked image because the embedded watermark and the locally generated version do not share the same spatial pattern anymore. An exhaustive search with different rotation angles and scaling factors does yield the correlation peak, but it is prohibitively complex.
- Statistical Averaging: An attacker may try to estimate the watermark and then 'un-watermark' the object by subtracting the estimate. This is dangerous if the watermark does not depend substantially on the data. Note that with different watermarked objects it would be possible to improve the estimate by simple averaging. This is a good reason for using perceptual masks to create the watermark.
- Multiple Watermarking: An attacker may watermark an already watermarked object and later make claims of ownership. The easiest solution is to timestamp the hidden information by a certification authority.
- Attacks at Other Levels: There are a number of attacks that are directed to the way the watermark is manipulated. For instance, it is possible to circumvent copy control mechanisms discussed below by super scrambling data so that the watermark is lost (I. J. Cox and J.-P. M. G. Linnartz,1998) or to deceive web crawlers searching for certain watermarks by creating a presentation layer that alters them. The latter is sometimes called 'mosaic attack' (F. Petitcolas, R. Anderson, and M. Kuhn, 1998).
- Compression: This is generally an unintentional attack which appears very often in multimedia applications. Practically all the audio, video and images that are currently being distributed via Internet have been compressed. If the watermark is required to resist different levels of compression, it is usually advisable to perform the watermark insertion task in the same domain where the compression takes place. For instance, DCT domain image watermarking is more robust to JPEG compression than spatial-domain watermarking.
- Filtering: Low-pass filtering, for instance, does not introduce considerable degradation in watermarked images or audio, but can dramatically affect the performance, since spread-spectrum-like watermarks have a non negligible high-frequency spectral content.

3.5 Security Parameter of Digital Watermarking

In an e-Government system it is compulsory to protect unauthorized copy, misappropriation and misrepresentation of digital information. There are various criteria of security assessment of ICT based networks. One of the most important criteria is the European Information Technology Security Evaluation Criteria (ITSEC). Which assist the security of information communication and technology based network. This criterion coves the three basic threats:

- Confidently (unauthorized information revealing)
- Integrity (unauthorized data modification)
- Availability (unauthorized withholding of information or resources)

Security covers the fact that if the information is altered, then how much alteration is done in the original document. Thus there is a need to developing a new technology that will protect the integrity of digital information and secure the intellectual property right (IPR) of right owner. In recent years digital watermarking is main technique for the security purpose of digital information. Authentication of digital information becomes a key area of research due to latest advancement in information communication and networks/project based technologies require a security solution to prevent their misuse due to the

distribution of information over networks. Digital watermarking is gaining importance because of the increase use of Internet based network. Various security scheme for online networks are proposed based on cryptographic method of digital watermarking for protecting unauthorized use of digital data/information. Digital watermarking is a useful tool for e-Government 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 (Z. Bojkovic, D. Milovanovic, 2003).

Table2: Five classes of watermarks and quality parameters (Z. Bojkovic, D. Milovanovic, 2003)

Watermark	Quality Parameter
Copyright Watermark	• High Robustness • Verification process is usually private, but public can also be desirable • Imperceptible • Blind methods are usually more practicable. • Capacity should feet the needs fro a rightful owner identification
Finger print watermark	• Copyright watermark • Non blind techniques are useful
Broadcast and copy control watermark	• Finger print watermark • Low complexity required
Annotation	• Verification process is usually private, but public may be desirable • Robustness is less important in most cases • Security is not usually important • Blind methods are preferable • High capacity
Integrity watermark	• Copyright watermark • Robustness needed until the data is semantics is destroyed

4. Concluding Remarks

Security and authentication of information is the main concern for effective implementation of e-Government. Digital watermarking can be utilized for authentication of data. It is effective technique for protecting intellectual property (IP) rights by embedding information in digital data. Despite numerous existing cryptographic and watermarking algorithms, applied to online systems, many open questions and future research problem remain untouched with reference to their implementation to e-Government prospective. Proper implementation of e-Government required optimum combination of traditional set of rules and a new set of cyber laws. All the methodologies and modalities of electronic transaction have to be worked out, so that nothing goes unaccounted. The overall objective of cyber laws should be to provide a self-contained, simple and enforceable set of rules, which facilitate secure and efficient e-Government framework. In an online project various security techniques are used between sender and receiver such as cryptography technique, anti virus and firewall etc. All the existing security techniques try to protect the information in between sender and receiver but at the receiving end the user is not able to validate the security/authenticity of the received information. Digital watermarking can play a significant role in this regard. By using watermarking technique, user can check the validity or authenticity of the received watermarked information with a watermarking extraction process and a watermark key. In this paper digital watermarking is proposed as a subordinate to the existing security mechanisms for enhancing the security of information exchange in e-Government system.

5. References

1. A. Moller,(2000), Naestved – A Digital City in Europe, Presentation for International Symposium on Digital Cities in Chitose, October 24-25, www.naeskom.dk/nk.nsf.

2. Barni, M. et al., (2001), Digital Watermarking for copyright protection: A communication perspective, *IEEE Communication Magazine*, 39: 8, pp. 90-91, August.
3. B.-L. Yeo and M. M. Yeung, (1999)., Watermarking 3D objects for verification, *IEEE Computer Graphics and Applications*, vol. 19, no. 1, pp. 36–45.
4. Collberg C., and Thomborson C., (2002). Watermarking, Tamper-proofing and Obfuscation- Tools for Software Protection. *IEEE Transactions on Software Engineering*, Vol. 28, No. 8, pp 735-746.
5. EzGov., (2000)., Realizing e-Government. EzGov White Paper. Access at: www.ezgov.com/ white_papers_art3_1.jsp.
6. F. Petitcolas, R. Anderson, and M. Kuhn(1998), Attacks on copyright marking systems *in Information Hiding* (D. Aucsmith, ed.), vol. 1525 of Lecture Notes in Computer Science, (Berlin), pp. 218–238, Springer-Verlag, 1998.
7. Hazarika, Jatin,(2004). Inauguration of the E-Government Workshop in AASC, AARC.
8. Herzberg Amir and Pinter Shlomit S., (1987)., Public protection of software, *ACM Transactions on Computer Systems*, vol. 5, no. 4, pp 371-393.
9. Hao-Tian Wu and Yiu-Ming Cheung, (2005), A Fragile Watermarking Scheme for 3D meshes, *MM-SEC'05*, ACM pp 117-123
10. I. J. Cox and J.-P. M. G. Linnartz (1998), Some general methods for tampering with watermark, *IEEE J. Select. Areas Commun*, vol. 16, pp. 587–593.
11. Jason Tuohey, (2004), Government Uses Color Laser Printer Technology to Track Documents accessed from http://www.pcworld.com/article/id,118664-page,1/article.html on 5 Oct 2007
12. Kerry Ferguson (2000). World information flows and the impact of new technology: is there a need for international communication policy and regulation?, *Social dimensions of information technology: issues for the new millennium*, Idea Group Publishing, Hershey, PA,
13. NIST (National Institute of Standards & Technology), Thornton, J. (2004). E-Authentication Guidance. Available at http://csrc.nist.gov/kba/Presentations. Accessed Sept. 2007.
14. O. Benedens and C. Busch., 2000, Towards Blind Detection of Robust Watermarks in Polygonal Models. *Computer Graphics Forum*, 19(3).
15. Z. Bojkovic, D. Milovanovic(2003), Mu1timedia Con tents Security :Watermarking Diversity and Secure Protocols 6th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Service, TELSIKS 2003. Volume 1, 1-3 Oct.pp:377 - 383 vol. 1

About the Authors

Dilip Kumar Sharma is B.Sc., B.E. (Honours) (CSE), M.Tech.(IT) and member of AIMS International, USA, CSTA, USA, life member of CSI, Mumbai, IETE, New Delhi, ISTE, New Delhi, SSI, Thiruvananthapuram and ISCA, Kolkata. He has published papers in international/ national conferences and international journal. Presently he is working as a Lecturer at G.L.A. Institute of Technology and Management, Mathura, India since March 2003. He is also coordinator of Computer Society of India G.L.A.I.T.M. Student Branch since 2004. His research interests are digital watermarking, e- business/e-government and software engineering. He has guided various projects and seminars undertaken by the students of B. Tech.

Vinay Kumar Pathak is B.Tech(CS), M.Tech.(CS) and PhD(CS) .He is working as Professor and Head, dept. of computer science & engineering at H.B.T.I. Kanpur .He has published various papers in international/ national conferences of repute. He has attended various short term course/seminar/workshop/conferences and also organized various conferences. His research interests are Computational Geometry and Image Processing. Presently he is guiding three students for Ph. D degree and also guided more then thirty five B.Tech. projects.

G P Sahu is working as Assistant Professor at the School of Management Studies, M N National Institute of Technology, Allahabad, India. He has more than ten years of teaching and research experience. He pursued his doctoral work at the Department of Management Studies, Indian Institute of Technology (IIT) Delhi. His research interests are in the areas of MIS and E-government. He has published research papers both in journals and conferences proceedings. He has coordinated several international conferences such as "4th International Conference on E-governance (15-17 December, 2006) at IIT Delhi", an International Conference on "Integrating World Market-Living Excellence through Technology and Beyond...." (January 5-6, 2002). He has also edited books on *"Integrating World Market"* in 2002 and "*Delivering E-government"* in 2006. He is now the Programme Chair of the 5th International Conference on E-governance, ICEG-2007 (28-30 December 2007) at Hyderabad, India.