A NOVEL TECHNIQUE OF DIGITAL RIGHTS MANAGEMENT IN DIGITAL WATERMARKING

Mrs. Rashmi Soni[1] and Prof.M.K.Gupta[2]

[1] Research Scholar, Department of CSE, AISECT University, Bhopal, M.P., (India)
[2] Professor, Department of ECE, MANIT & Research Supervisor, AISECT University, Bhopal, M.P., (India)

ABSTRACT

The Digital watermarking helps owners in asserting their intellectual property rights on the inventive works. This paper surveys the features and concepts and purpose of DRM techniques. Digital Rights Management (DRM) is a set of technologies that are used by hardware manufacturers, publishers, copyright holders, and individuals with the intent to control the use of digital content. With first-generation DRM software, the intent is to control copying; with second-generation DRM, the intent is to control executing, viewing, copying, printing and altering of works or devices. The term is also sometimes referred to as copy protection, copy prevention, and copy control.

Keywords: Digital watermarking, DRM, Copy control, Copy protection, DRM techniques.

I. INTRODUCTION

A watermark is a secret code or image integrated into an original image. The use of perceptually invisible watermarks is one form of image authentication. A watermarking algorithm consists of three parts: the watermark, the marking algorithm and the verification algorithm. Each owner has a unique watermark. The marking algorithm incorporates the watermark into the image. The verification algorithm authenticates the image, determining both the owner and the integrity of the image [1]. The growing research area, Digital watermarking, has its roots in computer science, cryptography, signal processing, Image Processing and communications [2].

The primary objective of digital watermarking is to embed small amount of secret information, i.e., the watermark into the host digital productions like the image and audio, thus facilitating the extraction at a later stage for the purposes of copyright assertion, authentication, and content integrity verification and the like [3]. Owing to the good results that were obtained, watermarking methodologies have attracted attention [4, 5, 6,].Digital watermarking techniques can be utilized to protect the intellectual property rights of the data by embedding the proprietary information, such as password and company logo, in the host data [7]. The determination of ownership and the detection of tampering are the two purposes of watermarks. The Digital watermarks of ownership are embedded onto digital content for copyright protection, ownership affirmation, and integrity checks since digital content can be employed to obtain the verification of copyright violation after an attack [8]. The techniques like watermarking assist in controlling the unauthorized replication or exploitation of digital content [8], [9], [10]. Digital Rights Management solutions assist the protection of confidential information and premium content from unauthorized use even by authorized users in the corporate and government sectors. The most essential function of DRM system is the copyright protection. The copy control such as permitting no or one or several unlimited copies of the multimedia data, and with or without rights to produce copies of these copies can be enforced by the DRM system [11]. Thus the use of digital watermarking techniques that embed information recognizing the copyright owner's identity within the content is regarded as a promising copyright protection technique [12]. DRM consists of certain techniques which includes encryption, copy control, digital watermarking, fingerprinting, traitor tracing, authentication, integrity checking, access control, tamper-resistant hard- and software, key management and revocations as well as risk management architectures [13].

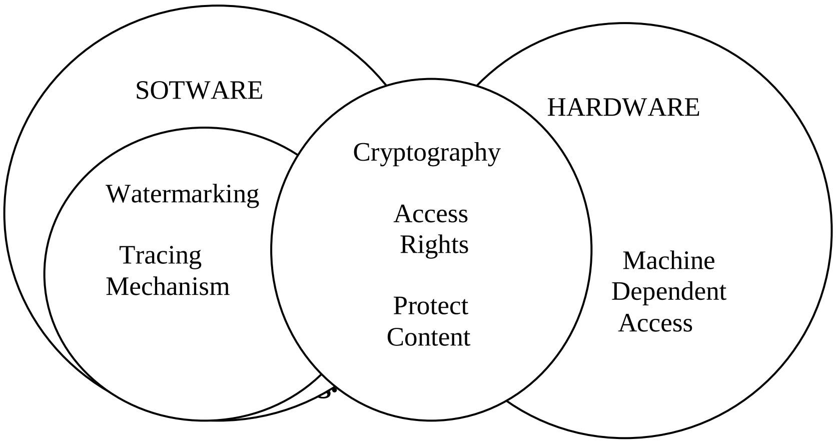
Although watermarking is used in many applications, still there is a risk to security for the embedded watermark against possible malicious attacks. Digital watermarking embeds some information regarding the rights into the digital data, hence guaranteeing copyright protection. Planned for variety of purposes like copyright protection, access control, and broadcast monitoring, the extraction of the embedded data in the future is possible [14]. The information about ownership can be any privacy information that completely identifies the owner during ownership controversies, such as password, logo. The aforesaid information can possibly be hacked by the hackers. There is an opportunity of the owner losing or forgetting the same as well. The hackers may at times brute-force the information and maintain the ownership finally. In addition, the solution for the problem of rightful ownership has not been properly solved. Therefore the design of DRM system needs to address the above mentioned security issues and also solve the ownership dispute. In this paper, we have focused on the prevention of disputes that begin out of ownership claims on digital images and a novel and efficient scheme of DRM technique to deal with it has been developed.

II. DIGITAL RIGHTS MANAGEMENT

The DRM Digital Right Management has been broadly applied in the protection of video/audio medias over the internet [15]. In broadcasting system, the broadly applied content protection is CA (Condition Access) [16].Compared with DRM, CA has many disadvantages in security, service model, Value-added Service, etc. The application of DRM technique in broadcasting system is becoming a trend [17] [18].Digital Rights Management (DRM) is a scheme by which content owners use scientific mechanisms to enforce and protect copyrights over the authored digital work. The objective of a DRM system is to restrict the use of content to its rightful user in order to facilitate rightful payment to artists for their work. Depending on usage scenarios and operating environments, DRM systems architecture [19] and implementation differ from vendor to vendor but the basic functionality provided by each system is equivalent, to facilitate publishing of digital content in a manner such that the usage of this content can be controlled. Figure 1 illustrates the various DRM systems types along with the respective functionality achieved by the type of implementation

A typical DRM solution [20] is implemented through software and involves proprietary formats and generally operates in a client-server context. The technologies used for digital management of rights include cryptography and watermarking. Cryptography is used for license management. User rights are expressed in the licenses which are typically implemented as digital certificates. User rights specify the number of usages, temporary or partial use, duration of access, lending rights, and number of devices on which the content can be used. Licenses generally contain an identifier of a user who has purchased the content, or an identifier of a device on which the license may be used.

Watermarking is a data embedding technology used mostly for tracing purposes. It is used to identify the source of illegal distribution by analysing the user-specific identifier embedded in the digital content prior to its distribution. DRM systems can also be realized in hardware through integrated circuits [21]. DRM is the system for protecting the copyrights of data circulated via the Internet or other digital media by enabling secure distribution and/or disabling illegal distribution of the data Some DRM Goals are: - (i) Protection of digital content (ii) Secure distribution (iii) Content authenticity (iv) Transaction non-repudiation (digital signature) (v) Market participant identification (digital certificates). & DRM Techniques are:- (i)Encryption (ii) Public/private keys (iii) Digital certificates (iv) Watermarking (v) Access control (vi)Secure communications protocols (vii) Fingerprinting (viii) Rights specification language (ix) Trust infrastructure (x) Hashing



The term Digital Rights Management - DRM - has its origins in the combined efforts of some vendors, their marketing staff and some other industry analysts in the late 1990s [22]. It is a breakthrough in the progress of Conditional Access Systems (CAS). CP, for Copy Protection, often completes the DRM acronym although CP should be part of a DRM system for Rights Enforcement. DRM spans a broad array of technological and business concepts. It includes relatively specialized technologies such as watermarking, Public Key Infrastructure (PKI) and encryption, as well as other business areas such as pricing, terms, and conditions for use [22]. A main matter for DRM is the lack of a standardized definition for the process and for the key concepts involved [23]. Different interpretations of the term abound, including: "Digital Rights Management refers to controlling and managing rights to digital intellectual property."[22] "Digital Rights Management is "the description, identification, trading, protection, monitoring and tracking of all forms of rights usages over both tangible and intangible resources including management of rights holders relationships it is the "digital management of rights" not the "management of digital rights."[24]

Digital Rights Management (DRM) involves the description, layering, analysis, valuation, trading and monitoring of the rights over an individual or organization's assets; both in physical and digital form;

and of tangible and intangible value [25]. DRM covers the digital management of rights - being them rights in a physical form of a work (e.g. a book), or being them rights in a digital form of a work (e.g. an e-book). Current methods of managing, trading and protecting such assets are inefficient, proprietary, or else often require the information to be wrapped or embedded in a physical format [25].The copyright environment consists of three main aspects: rights (what can be protected by copyright) and exceptions (e.g. copies for private use or for public libraries); enforcement of rights (sanctions for making illegal copies and for trading in circumvention devices); and management of rights (exploiting the rights). In the online world, management of rights may be facilitated by the use of technical systems called Digital Rights Management (DRM) systems [26] [7]. DRM consists broadly of 2 elements: the identification of intellectual property and associated rights and the enforcement of usage restrictions. The identification consists in the attribution of an (standard) identifier (such as the ISBN numbers for books) and the marking of the property with a sign (such as a watermark). The description of the rights relies on Rights Expression Languages (REL). The enforcement is based on encryption and key management, by i.e. ensuring that the digital content is only used for purposes agreed by the right holder. DRM is the chain of hardware and software services and technologies leading the authorized use of digital content and managing any consequences of that use throughout the complete life cycle of the content [7].

III. PROPOSED METHOD

The choice of an's and bn's are governed by texture sensitivity of Human Visual System (HVS). The following factors are considered to develop mathematical model. The edge blocks should be least altered to avoid significant distortion of the image. So we can add only small amount of watermark gray value in the edge block of host image. This means that scaling factor an should be close to amax, (the maximum value of the scaling factor) and embedding factor bn should be close to bmin (the minimum value of the embedding factor).

- So, we assume a_n to be directly proportional to variance s n and b n to be inversely proportional to variance s_n. The blocks with mid-intensity are more sensitive to noise than that of low intensity blocks as well as high intensity blocks.
- This means that the an should increase with local mean gray value up to mid gray value and again decrease with local mean gray value. The variation of a_n with mean block gray value is assumed to be Gaussian in nature. The variation b_n with mean gray value is reverse to that of an. Based on the above discussion we propose the following mathematical model.

$$\alpha_n = \alpha_{max} ,$$ (For edge blocks)

$$\alpha_{min} + (\sigma_n (\alpha_{max} - \alpha_{min})/\sigma_{max}) \exp.(-(\mu_n - \mu)^2/2), \qquad \text{-----------------------} \qquad (1)$$

(For other blocks)

$$\beta_n = \beta_{min} ,$$ (For edge blocks)

$$\beta_{min} + (\sigma_{min} (\beta_{max} - \beta_{min}) / \sigma_n)[1 - \exp(-(\mu_n - \mu)^2 / 2)], \qquad \text{----------------------} \qquad (2)$$

(For other blocks)

Where,

- α min and a max are respectively minimum and maximum values of scaling factor,
- β min and b max are respectively minimum and maximum values of embedding factor,
- μ n is normalized mean of each block,
- σ n are normalized variances of each DCT blocks,
- σ min and s max are respectively minimum and maximum values of DCT block variances,
- μ is the normalized image mean.

IV. DRM ARCHITECTURE

The DRM architecture is composed of a standardized set of different building blocks.

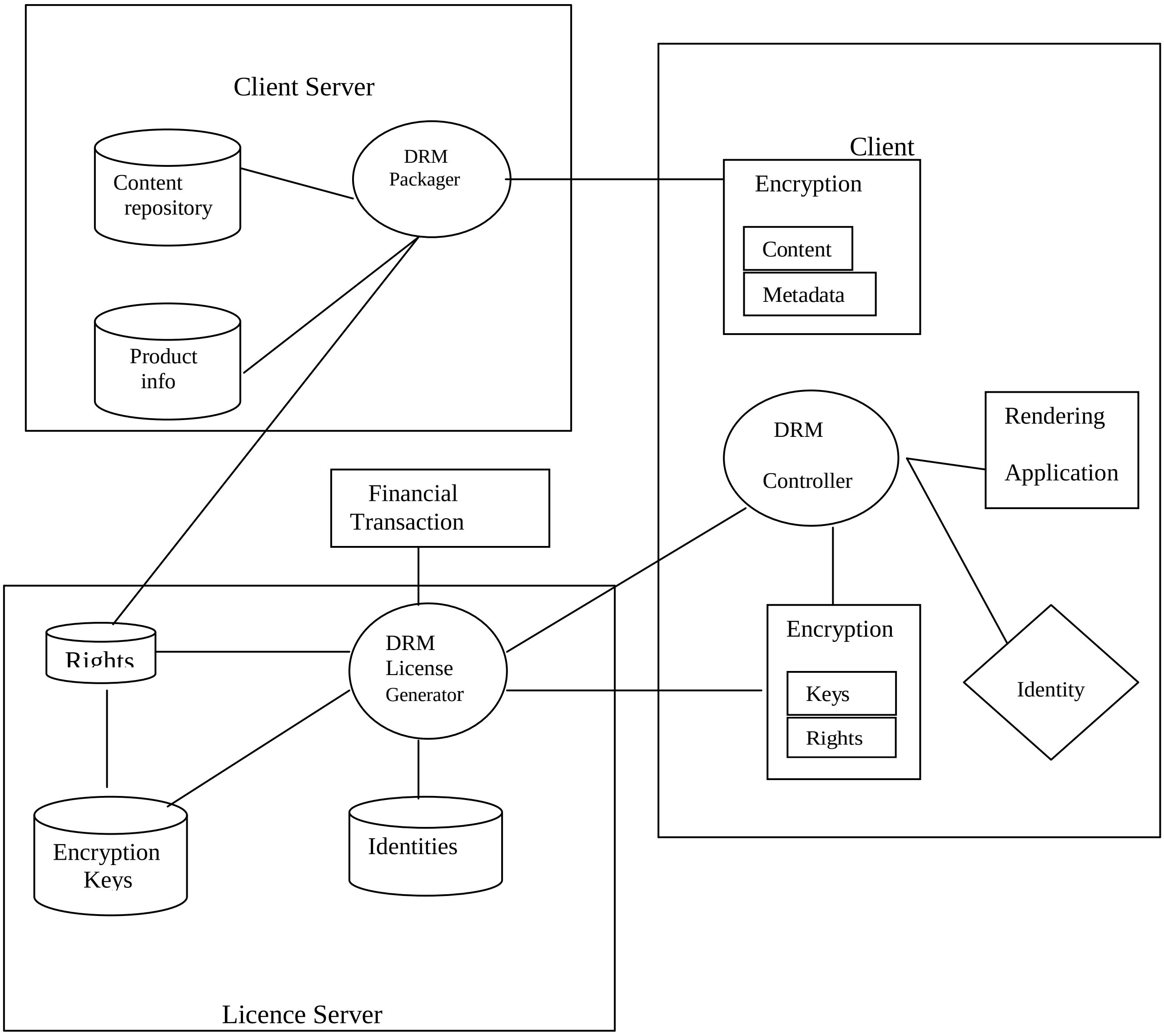


Fig. 2 DRM Architecture [22]

Two different visions from DRM can be presented: an architectural view and a functional view. From an architectural view, three major components can be identified: the content server, the license server, and the client [7] as shown in Figure 2. The content server is a server component on the DRM architecture that consists of the actual content, information about products (services) that the content provider wants to distribute, and functionality to prepare content for a DRM-based distribution.

The license server is responsible for managing licensing information. Licenses contain information about the identity of the user or device that wants to exercise rights concerning the content, identification of the content to which the rights apply, and specifications of those rights.

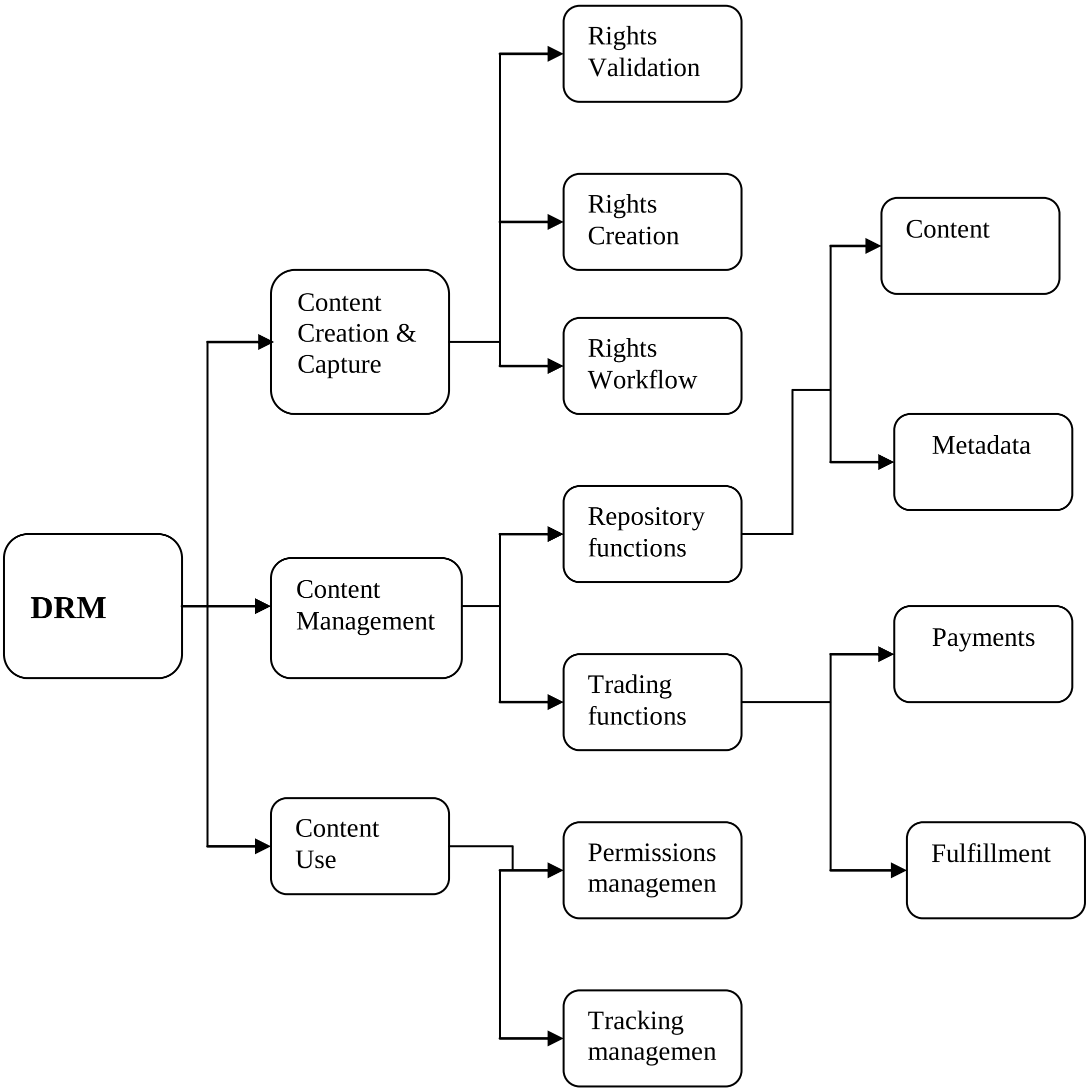


Fig.3 Generic DRM Functional Architecture

The client resides on the user's side and supplies the following functionalities: DRM controller, the rendering application and the user's authentication mechanism [27].

From a functional point of view, the Figure 3 can continue the most important functions of DRM architecture:

1) Content Creation and Capture

2) Content Management

3) Content Use

4.1 Content creation and capture: Managing the creation of content to facilitate trading, including asserting rights when content is first created (or reused and extended with appropriate rights to do so) by various content creators or providers. This module supports:

a. Rights validation - to ensure that content being created from existing content includes the rights to do so and that the rights are consistent.

b. Rights creation -to assign rights to new content, such as specifying the rights owners and allowable use (permissions).

c. Rights workflow - to process content for a series of workflow steps for review and/or approval of rights.

4.2 Content management: Managing and enabling the trade of content, including accepting content from creators into an asset management system. This module supports:

a. Repository functions - to access content and the "metadata" that describes the content and the rights specifications (see Information Architecture) or enabling the access/retrieval of content in potentially distributed databases and the access/retrieval of metadata. The metadata covers Parties, Rights and descriptions of the Works.

b. Trading functions – to enable the issue of licenses to parties who have done deals for rights over content, including, for example, royalty payments.

4.3 Content use: Managing the use of content once it has been traded. This module supports:

a. Permissions management - to enforce the rights associated with the content. For example, if the user has only the right to view the document, then printing will be prohibited.

b. Tracking management - to monitor the use of content where such tracking is a requirement of the user's agreement. This module may need to interoperate with the trading functions to track use or to record transactions for "per use" payments [7]. e.g., the user has a license to play a video ten times.

V. CONCLUSION

The extreme advancements in the area of digital technology have created the need to offer security for copyright protection of digital contents. A DRM system needs to be capable of providing persistent content protection against illegal access to the digital content, restricting access to only those with suitable authorization. Watermarking techniques are being used for this purpose these days. Digital rights management systems enable robust e-commerce, copyright protection, secure distribution and protection of digital data by means of encryption, watermarking, fingerprints, secure communication protocols, trust infrastructures, etc. Digital watermarks as a way of preserving the digital data value are designed to permanently reside in the host data (images, audio data, and video). However the embedded watermark data can be easily hacked by the hackers and thus result as a threat to protection of digital content. To solve the security issues in protecting the rights of digital content, in this paper, we have presented a novel scheme, which uses watermarking and DRM techniques.

REFERENCES

[1] Raymond B. Wolfgang and Edward J. Delp, “A Watermarking Technique for Digital Imagery: Further Studies”, Video and Image Processing Laboratory (VIPER), School of Electrical and Computer Engineering, Purdue University, Indiana, 47907-1285, USA.

[2] Saraju. P. Mohanty. “Digital Watermarking:- A Tutorial Review”, Dept of Computer Science and Engineering, University of South Florida 1999.

[3] Huayin Si, Chang-Tsun Li, “Copyright Protection in Virtual Communities through Digital Watermarking”, Idea Group Publishing, 2005.

[4] N. K. Ratha, J. H. Connell, and R. M. Bolle, “Secure data hiding in wavelet compressed fingerprint images,” In Proceedings of the ACM Multimedia Workshops , pp. 127– 130, USA, 2000.

[5] A. K. Jain and U. Uludag, “Hiding biometric data,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 25, no. 11, pp. 1494–1498, 2003.

[6] K. Zebbiche, L. Ghouti, F. Khelifi, and A. Bouridane, “Protecting fingerprint data using watermarking,” In Proceedings of the 1st NASA/ESA Conference on Adaptive Hardware and Systems , 2006,pp. 451–456

[7] B. Surekha and G. N. Swami “Sensitive Digital Image Watermarking for Copyright Protection” International Journal of Network Security, vol.15, no.1, Jan 2013.

[8] Memon, N. and Wong, P.W., “Protecting digital media content,” Communications of the ACM, Vol: 41, pp.35–43, 1998.

[9] G. Voyatzis, I. Pitas, “The use of watermarks in the protection of digital multimedia products," IEEE Proceedings, July 1999, vol. 87, No. 7, pp 1197-1207.

[10] A.B. Kahng, J. Lach, W.H. M-Smith, S. Mantik, I.L. Markov, M. Potkonjak, P. Tucker, H. Wang, and G. Wolfe, "Constraint-based watermarking techniques for design IP protection," IEEE Trans Comput.-Aided Des. Integrated Circuits Syst., vol.20, no.10, pp.1236–1252, Oct. 2001.

[11] E. T. Lin, A. M. Eskicioglu, R. L. Lagendijk, and E. J. Delp., “Advances in digital video content protection.” IEEE: Special Issue on Advances in Video Coding and Delivery, pp: 171–183, 2005.

[12] Scott Craver, Stefan Katzenbeisser, "Copyright protection protocols based on asymmetric watermarking: The ticket concept", In Communications and Multimedia Security Issues of the New Century, pp 159–170, 2001.

[13] Ian Kerr, "Hacking privacy: Why We Need Protection from the Technologies That Protect Copyright", in proc. of Conference on privacy and identity, 2007.

[14] Xu, S. Dexter, A. M. Eskicioglu, “A Hybrid Scheme of Encryption and Watermarking,” IS&T/SPIE Symposium on Electronic Imaging 2004, Security, Steaganography, and Watermarking of Multimedia Contents VI Conference, 2004,Vol. 5306, pp. 725-736..

[15] Shaojun Zhu, “The comparison and study of DRM standard”, East China Normal University Master’s Dissertations, 2004, pp.7-20

[16] Jun Chen, “The realization of CA on DTV”, Chinese Academy of Sciences Doctor’s Dissertations, 2004.

[17] Rosenblatt B., Trippe B., Mooney S., "Digital Rights Management - Business and Technology", M&T Books, 2003.

[18] Martin M., Agnew G., Boyle J., McNair J., Page M., Rhodes W., "DRM Requirements for Research and Education - Discussion Paper", The NSF Middleware Initiative and Digital Rights Management Workshop, 2002.

[19] Susanne Guth. “A sample drm system”, Springer-Verlag Berlin, Heidelberg, 2003, vol 2770, pp 150-161

[20] Laurent Michaud, Mathieu Massot, and Alain Puissochet. “Digital rights management (drm) - drm and virtual content distribution.” Technical report, IDATE Digiworld, 2005.

[21] W. Shi, H. Lee, R. Yoo, and A. Boldyreva. “A Digital right enabled graphics processing system.” In Proceedings of the 21st ACM SIG-GRAPH/EUROGRAPHICS Symposium on Graphics Hardware, 2006, pp 17-26

[22] Rosenblatt B., Trippe B., Mooney S., "Digital Rights Management - Business and Technology", M&T Books, 2003.

[23] Martin M., Agnew G., Boyle J., McNair J., Page M., Rhodes W., "DRM Requirements for Research and Education-Discussion Paper”, The NSF Middleware Initiative and Digital Rights Management Workshop, 2002.

[24] Iannella R., "Digital Rights Management (DRM) Architectures."D-Lib Magazine, vol.7, no.6, http://www.dlib.org/dlib/june01/iannella/06iannella.html, 2001.

[25] Rosenblatt B., "Integrating DRM with P2P networks - Enabling the future of Online Content Business Models", Giant Steps Media Technology Strategies, November 2003.

[26] Commission Staff Working Paper - "Digital Rights Background, Systems, Assessment", European Commission, February 2002.

[27] Rosenblatt B., Tripp B., Mooney S., "Digital Rights Management: Business and Technology", John Wiley & Sons, 2001.

Bibliographical Note’s

Mrs. Rashmi Soni received B.TECH in 2008 from B.I.S.T Bhopal & M.TECH degree in (Computer Science & Engineering) 2011from R.I.T.S Bhopal and pursuing PhD in (Computer Science & Engineering) from AISECT UNIVERSITY Bhopal (M.P) in 2012 till date, respectively. Till now total 5 papers published in International Journals/International Conference/National journal. Areas of interests are: Image Processing., Digital watermarking, Visualization, Image sharpening and restoration, Image retrieval, Image Recognition.

Dr. M.K. Gupta received B.TECH (Electronics) from MANIT Bhopal in 1975, M-TECH (Electronics) from IIT Roorkee in 1992, PhD from BU Bhopal in 2006. Currently he is professor in MANIT Bhopal & Research Supervisor, AISECT University Bhopal (M.P). Till now 25 papers published in International Journals/International Conference/National journal. Areas of interests are: VLSI, Integrate Circuit, Microprocessor, Control System, and Image Processing.