Securing Watermarked-Relational Data by Using Encryption and Decryption

[1]Nagarjuna.Settipalli, [2]R Manjula
[1,2]VIT University, Vellore Tamil Nadu, India
[1]settipallinagarjuna@gmail.com , [2] rmanjula@vit.ac.in

ABSTRACT

Ownership rights on outsourced relational database are very crucial issue in today's internet environment and in many content distribution applications, because the rapid growth of the internet and related technologies offered an unprecedented ability to access and redistribute digital content. In earlier existing systems the relational data will be watermarked and directly send to the client system, in these systems while sending relational data from server to client attacker easily copy the data and create same copy of relational data. Here there is no security to watermarked relational data. In our proposed system before sending the watermarked relational data to client side we encrypt the relational data and send it to the client side, at client side decryption will be done to get the original watermarked data. Because of using this encryption technique even an attacker copy the data he/she may not read the watermarked relational data.

Keywords*: Ownership rights, relational data, watermarking, security, encryption, decryption, client, server.*

1. INTRODUCTION

The study of watermarking is started more than 700 year ago. The term watermark is used in 18th century [13]. The main aim of watermarking is to protect a certain data from unauthorized and duplication and distribution by enabling provable ownership over the content. To prove ownership rights is very difficult especially in case of internet and related applications. A watermark describes information that can be used to ownership of data such as the origin, owner, or recipient of client [1]. Most watermarking research is concentrated on multimedia such as audio, video, and images. The difference between digital watermarking and other technology is of three important aspects, firstly unlike encryption, watermarking is imperceptible so that image will not be detracting from the aesthetic sense. Secondly, the watermark and works they embedded in are inseparable; even if works are converted into other file format the watermarks will not be eliminated [12]. Last one is the watermarks will have exactly the same transformation experience as the works, that means we can get the information of transformation by looking at the watermarks. Today digital media are getting more and more popular. Not only multimedia images, video, audio are in digital form, but relational databases are also digitized in the applications, including finance databases, multimedia databases, personal databases. Digital watermarking techniques have been proposed for ownership protection, copy control, annotation and authentication of digital media. Most of digital image watermarking techniques in the literature are proposed for image [5]. However, the digital watermarking for relational database is only addresses by a few authors because there are many differences between the structures of image data and relational data. In this paper we provide the security to the watermarked data by using encryption and decryption. Watermarking detection is blinded. The increasing use of databases in application beyond "behind-firewall processing" is creating need for watermarking databases. Secure watermarking embedding requires that the embedded watermark must not be easily tampered with, forged or removed from the watermarked data [8]. Imperceptible embedding means that the presence of watermark is unnoticeable in the data. Basic characteristics of watermarking are robust, imperceptible, secure and reliable, low complexity, secure hiding place, payload, blind.

- **Robustness:** Robustness means the watermarking should be robust enough to handle any kind of situation [9][2].
- **Imperceptible:** In some cases the watermarking is neither visible by human eyes nor hearable by human ears. It means it can be detected by special processing or special circuit only [1]. This means the watermark will not affect the original host data.
- **Secure and Reliable:** Watermark has unique correct signs marking every one, and thus to achieve the purpose of copyright protection.
- **Low-Complexity:** Low complexity algorithm will ensure effective and timely manner to watermarking embedding, detection and extraction.
- **Secure Hiding Place**: Watermark is embedded in correct place, and that will not be change the format of the original relational databases.
- **Payload:** The amount of information that can be stored in a watermarking.
- **Blind:** The watermark detection is blinded that means to extract the watermark from original data it requires neither the original data nor the watermark. So the watermark [14].

The major applications of watermarking include copy protection, content authentication, traction tracking, and broadcast monitoring [11]. Here copy protection means embedded information about the owner to prevent others from claiming copyright. Content authentication means embedded a watermark to detect modifications to the host data. Broadcast monitoring means embedded a watermark in the original data and use automatic monitoring to verify whether data was broadcasted as agreed. Traction tracking means embedded a watermark to convey information about the legal recipient of the data [10]. This is useful to monitor or trace back illegally produced copies of the data. This is usually referred as “fingerprinting” [20].

2. LITERATURE REVIEW

Ashraf Odeh and Ali Al-Haj classify the various types of attacks in watermarked relational database. In [4] paper they discussed about how to overcome the different types of attacks on relational database, and they proposed an effective database watermarking algorithm. RakeshAgrawal and Jerry Kiernan [15] also explained about various possible attacks in watermarking relational databases they are bit attacks, randomization attacks, rounding attacks, subset attack, mix and match attack, inevitability attack. RakeshAgrawal and jerry Kiernan proved that our watermarking technique is robust against all the above attacks they tested this algorithm on real world relational database. RaduSion [14] discussed how to boost up the ownership over categorical data he provided the limits to embedded the watermark in relational data. Ms. ArtiDeshpande and Mr. JayantGadgE [3] proposed an algorithm for how to embed the watermark in relational database and how to detect the watermark from original watermarked table, data partitioning algorithm. DarkoKirovski and Fabien A. P. Petitcolas [6] explained blind pattern matching attack on watermark, and different types of attacks on audio data, strength of watermark on relational database. In [16] RaduSion, Mikhail Atallah and Sunil Prabhakar discussed about rights protection for relational data, challenges of watermarking relational database, and optimization of watermark embedding, they introduces a one algorithm for embedding the watermark in relational database. And the primary key dependencies in relational data. Yanqun Zhan [19] explained what the basic characteristics of watermark and discussed theoretical model of watermarking. The closest to our technique is discussed in an effective approach for watermarking xml data [18], in this paper they discussed about what are the different types of attacks on watermarking relational database and explained about additive attack on xml data. How additive attack is applied by the attacker in various tags in xml data and how to identify those attacks is discussed in this paper. We are taken the same problem on relational database. In all the above previous discussions they discussed about how to watermarking the relational data, multimedia such as audio, video, images. Here the main drawback is no one discussed about the security issues for watermarking relational data and other different types of watermarked multimedia data; they simply apply the watermark and send it to the particular client at client side by using secret key the original watermarking is identified [17]. If attacker simply copy the watermarked data and create the same copy of data, apply the watermarking and claim the ownership rights [7]. This problem was discussed in our proposed system and specified the solution to the problem. Here after applying watermarking to relational data base before send it to the client side system we encrypt the watermarked relational data by using some encryption algorithm and send it to the client side system, so even attacker copy the watermarked data he/she didn’t get the original watermarked data and at client side we decrypt the data to get the original watermarked relational data

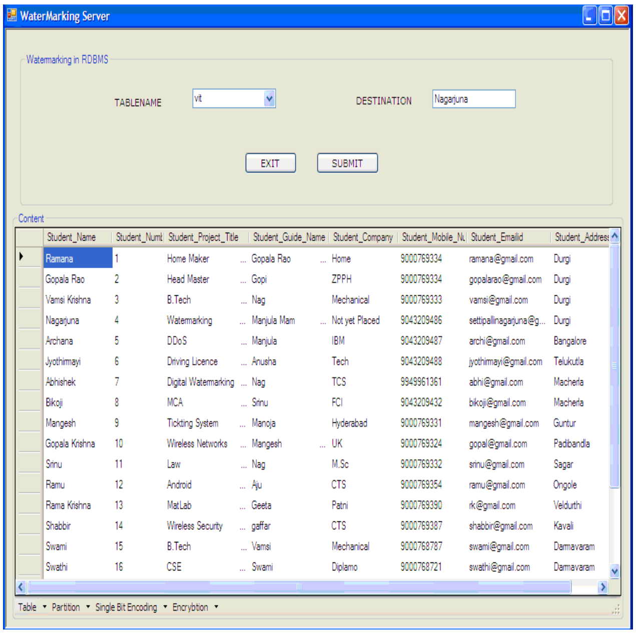
3. PROPOSED DESIGN

In our proposed system we provide the security to watermarked relational data by using encryption and decryption technique. The modules in our proposed system are

3.1 Server side module

3.2 Client side module

In server side system the original table will be extracted from the database to apply watermarking. The server side system contains dataset partitioning, single bit encoding, encryption techniques. Once the table is extracted from the database by using data set partitioning technique the table will be partitioned into number of partitions, then we apply the watermarking by using single bit encoding algorithm. Before sending it to the client side system we apply the encryption algorithm to the watermarked data for providing security. If attacker copies the watermarked relational data he/she never read the content. And at client side the decryption process will be done to get the original watermarked relational data.



TABLENAME vit

DESTINATION Nagarjuna

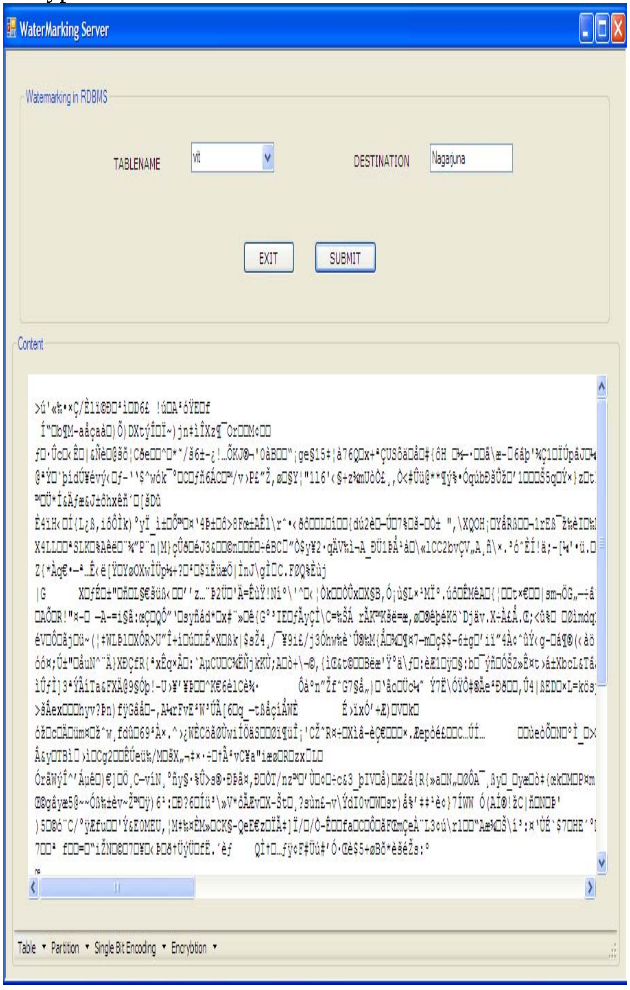
Student_Name	Student_Numt	Student_Project_Title	Student_Guide_Name	Student_Company	Student_Mobile_Nu	Student_Emailid	Student_Address
Ramana	1	Home Maker ...	Gopala Rao ...	Home	9000769334	ramana@gmail.com	Durgi
Gopala Rao	2	Head Master ...	Gopi	ZPPH	9000769334	gopalarao@gmail.com	Durgi
Vamsi Krishna	3	B.Tech ...	Nag	Mechanical	9000769333	vamsi@gmail.com	Durgi
Nagarjuna	4	Watermarking ...	Manjula Mam ...	Not yet Placed	9043209486	settipallinagarjuna@g...	Durgi
Archana	5	DDoS ...	Manjula	IBM	9043209487	archi@gmail.com	Bangalore
Jyothimayi	6	Driving Licence ...	Anusha	Tech	9043209488	jyothimayi@gmail.com	Telukutla
Abhishek	7	Digital Watermarking ...	Nag	TCS	9949961361	abhi@gmail.com	Macherla
Bikoji	8	MCA ...	Srinu	FCI	9043209432	bikoji@gmail.com	Macherla
Mangesh	9	Tickting System ...	Manoja	Hyderabad	9000769331	mangesh@gmail.com	Guntur
Gopala Krishna	10	Wireless Networks ...	Mangesh ...	UK	9000769324	gopal@gmail.com	Padibandla
Srinu	11	Law ...	Nag	M.Sc	9000769332	srinu@gmail.com	Sagar
Ramu	12	Android ...	Aju	CTS	9000769354	ramu@gmail.com	Ongole
Rama Krishna	13	MatLab ...	Geeta	Patni	9000769390	rk@gmail.com	Veldurthi
Shabbir	14	Wireless Security ...	gaffar	CTS	9000769387	shabbir@gmail.com	Kavali
Swami	15	B.Tech ...	Vamsi	Mechanical	9000768787	swami@gmail.com	Damavaram
Swathi	16	CSE ...	Swami	Diplamo	9000768721	swathi@gmail.com	Damavaram

Figure 1 Extracting the table from server side system

In server side system we extract the original table to watermarking partitioning, single bit encoding, serialization; encryption is done at server side system.

3.1 ENCRYPTION AT SERVER SIDE SYSTEM

At server side system before extracting the table from the database the required table will be created which contains number of rows and columns. Once the table is created the table will be extracted from the relational database. By using data partitioning technique the extracted table will be partitioned, if the table contains 20 numbers of records the table is partitioned as first record is placed at fourth and fourth record will be places at sixth place and so on. By using single bit encoding technique the watermark bits are embedded into different partitions. In existing systems after embedding the watermark into relational data it will directly send it to the client side system, here there is no security to watermarked data, because watermarking technique can only strength the ownership rights it can't prevent from copying the data. But in our proposed system before sending it to the client side system we apply the encryption to watermarked relational data and send it to the other side. The sample encrypted table will be shown below



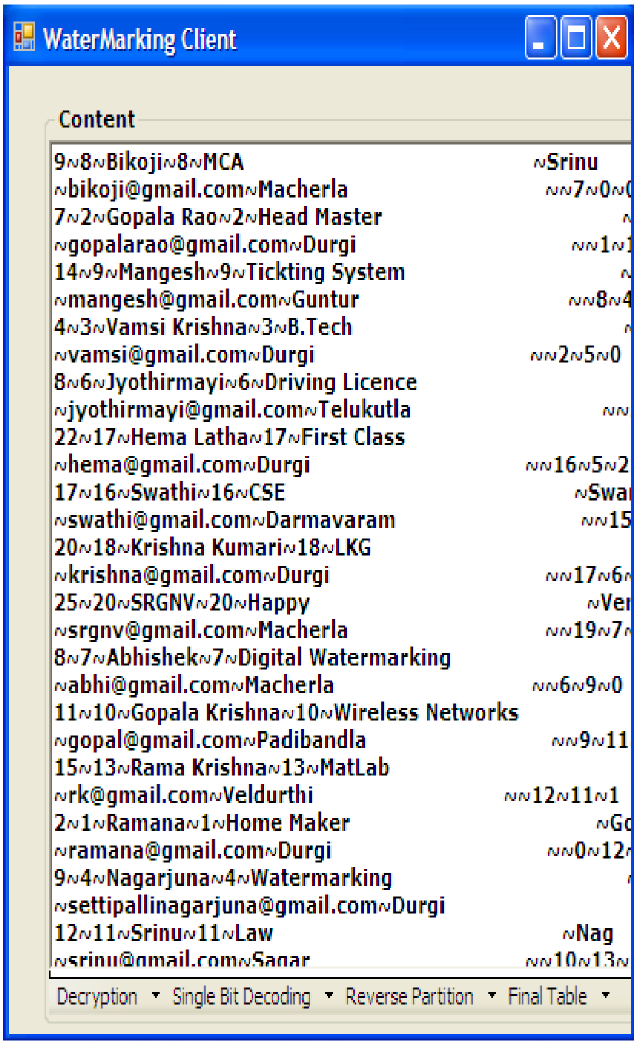
```
[illegible]
```

Figure 2 Encryption at Server side system

After encrypting the watermarked relational data it will directly send it to the client side system, and reverse process will be done at client side system. After decrypting the encrypted the decryption process will be dine.

3.2 DECRYPTION AT CLIENT SIDE SYSTEM

At client side system before reverse partitioning the encrypted watermarked relational data decryption process will be done. The advantage of encrypting the watermarked relational data is if an attacker simply copy the watermarked relational data it is not possible to identify the data. Once decryption process is done reverse partitioning, single bit decoding is done. The sample decryption process will be shown below


WaterMarking Client
Content
Decryption • Single Bit Decoding • Reverse Partition • Final Table •

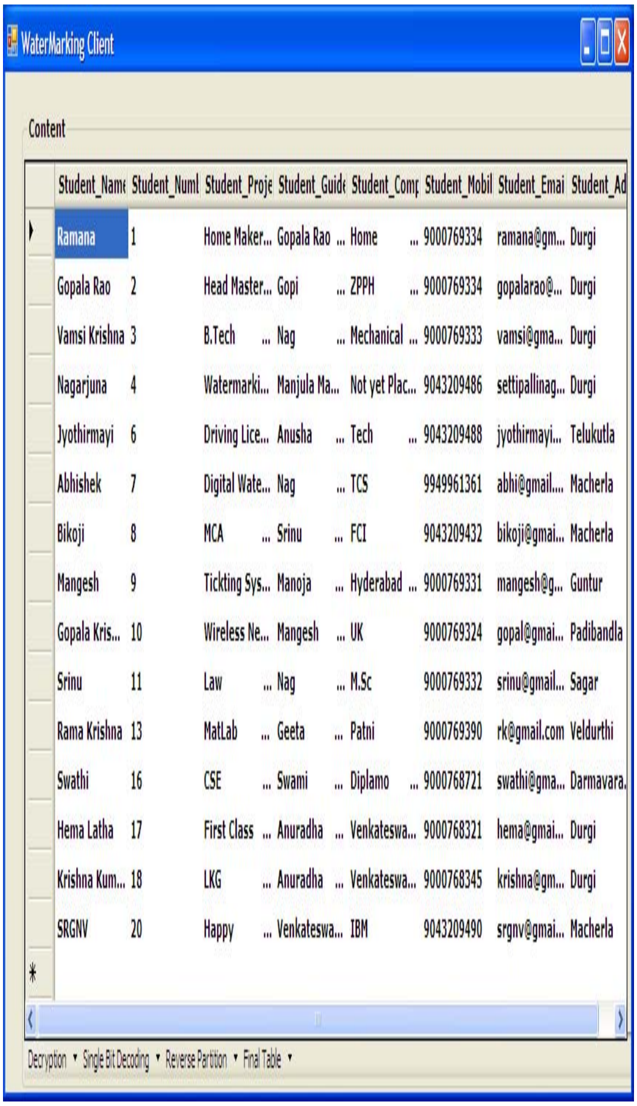
```
9~8~Bikoji~8~MCA                              ~Srinu
~bikoji@gmail.com~Macherla                    ~~7~0~(
7~2~Gopala Rao~2~Head Master                        ~
~gopalarao@gmail.com~Durgi                       ~~1~1
14~9~Mangesh~9~Tickting System                      ~
~mangesh@gmail.com~Guntur                        ~~8~4
4~3~Vamsi Krishna~3~B.Tech                          ~
~vamsi@gmail.com~Durgi                        ~~2~5~0
8~6~Jyothirmayi~6~Driving Licence
~jyothirmayi@gmail.com~Telukutla                   ~~
22~17~Hema Latha~17~First Class
~hema@gmail.com~Durgi                        ~~16~5~2
17~16~Swathi~16~CSE                              ~Swa
~swathi@gmail.com~Darmavaram                      ~~15
20~18~Krishna Kumari~18~LKG
~krishna@gmail.com~Durgi                      ~~17~6~
25~20~SRGNV~20~Happy                              ~Ve
~srgnv@gmail.com~Macherla                     ~~19~7~
8~7~Abhishek~7~Digital Watermarking
~abhi@gmail.com~Macherla                      ~~6~9~0
11~10~Gopala Krishna~10~Wireless Networks
~gopal@gmail.com~Padibandla                    ~~9~11
15~13~Rama Krishna~13~MatLab
~rk@gmail.com~Veldurthi                     ~~12~11~1
2~1~Ramana~1~Home Maker                            ~Gc
~ramana@gmail.com~Durgi                        ~~0~12~
9~4~Nagarjuna~4~Watermarking                         ~
~settipallinagarjuna@gmail.com~Durgi
12~11~Srinu~11~Law                                ~Nag
~srinu@gmail.com~Sagar                       ~~10~13~
```

Figure 3 Decryption at Client side system

After decrypting the watermarked relational data decryption will be done at the client side system so only authorized user can only see the watermarked relational data. After decryption process is done by using single bit decoding technique the decrypted table is decoded for detecting the original watermarked relational data, then reverse partitioning process will be done to get the original table and for identifying the original watermarking. By clicking on the final table button at client side system we will get the source table send by the server side system. In single bit encoding and single bit decoding process a small error will be inserted which can be tolerated by the relational database. In reverse partitioning process the small errors will be removed to get the original watermarked relational data.

3.3 FINAL TABLE AT CLIENT SIDE SYSTEM

The final table will be shown at client side system. The main aim of encryption and decryption in our proposed system is even though attackers simply copy the watermarking relational data the attacker may not identify the watermarking relational data. The sample result of final table will be shown below



Student_Name	Student_Numl	Student_Proje	Student_Guid	Student_Comp	Student_Mobil	Student_Emai	Student_Ad
Ramana	1	Home Maker...	Gopala Rao ...	Home ...	9000769334	ramana@gm...	Durgi
Gopala Rao	2	Head Master...	Gopi ...	ZPPH ...	9000769334	gopalarao@...	Durgi
Vamsi Krishna	3	B.Tech ...	Nag ...	Mechanical ...	9000769333	vamsi@gma...	Durgi
Nagarjuna	4	Watermarki...	Manjula Ma...	Not yet Plac...	9043209486	settipallinag...	Durgi
Jyothirmayi	6	Driving Lice...	Anusha ...	Tech ...	9043209488	jyothirmayi...	Telukutla
Abhishek	7	Digital Wate...	Nag ...	TCS	9949961361	abhi@gmail....	Macherla
Bikoji	8	MCA ...	Srinu ...	FCI	9043209432	bikoji@gmai...	Macherla
Mangesh	9	Tickting Sys...	Manoja ...	Hyderabad ...	9000769331	mangesh@g...	Guntur
Gopala Kris...	10	Wireless Ne...	Mangesh ...	UK	9000769324	gopal@gmai...	Padibandla
Srinu	11	Law ...	Nag ...	M.Sc	9000769332	srinu@gmail...	Sagar
Rama Krishna	13	MatLab ...	Geeta ...	Patni	9000769390	rk@gmail.com	Veldurthi
Swathi	16	CSE ...	Swami ...	Diplamo ...	9000768721	swathi@gma...	Darmavara.
Hema Latha	17	First Class ...	Anuradha ...	Venkateswa...	9000768321	hema@gmai...	Durgi
Krishna Kum...	18	LKG ...	Anuradha ...	Venkateswa...	9000768345	krishna@gm...	Durgi
SRGNV	20	Happy ...	Venkateswa...	IBM	9043209490	srgnv@gmai...	Macherla

Figure 4 Sample result of Final table at client side system

4. RESULT AND DISCUSSION

In our proposed system the encryption and decryption process will be done to securing the watermarking relational database. In the previous systems the encryption will not be done, and directly send it to the client side system so here there is no security to the watermarked relational data. In our system before sending the watermarked relational data we apply the encryption and send it to the client side system and at client side system decryption process will be done to get the original watermarked relational data. At client side system exactly reverse process is done. In this system even an attacker copy the watermarked relational data it is not in human readable format.

ACKNOWLDGEMENT

I take this opportunity to express my sincere gratitude to my project coordinator and guide Prof. R Manjula, School of Computing Sciences and Engineering, Vellore Institute of Technology Vellore, for their motivating suggestions, insightful advice, invaluable guidance, help and support in successful completion of this paper and also for constant encouragement and advice throughout my M.Tech program.

REFERENCES

[1] Ajay Goel, ”Improved Digital Watermarking Techniques and Data Embedding In Multimedia.”Department of CSE Singhania University, Rajasthan, Rupesh Gupta Department of Mechanical Engineering, Singhania University Rajasthan, O.P.Sahu Department of ECE, N.I.T. Kurukshetra, Sheifali Gupta Department of ECE Singhania University, Rajasthan, India , 2010.

[2] Ali Al-Aaj and Ashrafbdeh, ”Robust and Blind Watermarking of Relational Database Systems.”Princess sumaya University for Technology AI-Jubeiha,Jordan, 2008.

[3] Ms. ArtiDeshpande, Mr. JayantGadge, “New Watermarking Technique for Relational Databases.” Department of Computer Engineering, Thadomal Shahani Engineering College, Mumbai, ICETET-2009.

[4] Ashraf Odeh and Ali Al-Haj, “Watermarking Relational Database System.” Arab Academy for Financial and Banking Sciences**,** 2Princess Sumaya University for Technology, Amman, JORDA, 2008.

[5] S. Craver, N.Memon, B.-L.Yeo, andM. M. Yeung. “Resolving rightful ownerships with invisible

watermarking techniques: Limitations, attacks, and implications. ”IEEE Journal of Selected Areas in Communications, 16(4):573–586, 1998.

[6] DarkoKirovski and Fabien A. P. Petitcolas, ”Blind Pattern Matching Attack on Watermarking Systems. ”IEEE Tractions on signal processing, Vol. 51, NO. 4, April 2003.

[7] Fabien A.P. Petitcolas, Ross J. Anderson, and Markus G. Kuhn, Fabien A.P. Petitcolas, Ross J. Anderson, and Markus G. Kuhn, “Attacks on Copyright Marking System.”Notes in Computer Science, Portland, Oregon, USA, 14 17 April, 1998.

[8] Fernando Perez-Gonzalez and Juan R. Hernandez, ”A Tutorial on Digital Watermarking.” Dept. Tecnologıas de las Comunicaciones, ETSI Telecom., Universidad de Vigo, Spain, 1999.

[9] Frank Hartung and Bernd Girod, ”Watermarking of Uncompressed and compressed video.” Telecommunication Institute, University of Erlangen-Nurembery, 1998.

[10] Jonathan K. Su, Frank Hartung and Bernd Girod,” Spread Spectrum Watermarking: Malicious Attacks and Counterattacks.” Telecommunication Laboratory, University of Erlangen Nuremberg, Germany, 1999.

[11] S.P .Mahanty, “A Tutorial Review Report.” Department of Electrical Engineering, Indian Institute of Sciences, Bangalore, India, 1999.

[12] Mohamed Shehab, ArifGhafoor, IEEE, Elisa Bertino, Fellow, “Watermarking Relational Databases Using Optimization-Based Techniques.”IEEE, Vol.20, 2008.

[13] Podilchuk, C.I. and Delp., E.J, ”Digital Watermarking: Algorithms and Applications. ”IEEE Signal Processing Magazine, 2001.

[14] RaduSion, ”Proving Ownership over Categorical Data. ”Computer Sciences and the Center for Education and Research in Information Assurance and Security, Purdue University, USA, 2004.

[15] RakeshAgrawal, Jerry Kiernan, “Watermarking Relational Databases.” IBM Almaden Research Center, china, 2002.

[16] R.Sion, M.Atallah, and S.Prabhkar, “Right Protection for Relational Data. ”IEEE Trans. Knowledge and Data Engineering, Vol16 no.6, June 2004.

[17] VikasSaxena, J.P.Gupta, ”Collision Attack Resilient Watermarking scheme for Colored Images Using DCT.” IAENG, International journal of Computer Sciences, 2007.

[18] Wilfred Ng and Ho-Lam Lau, “Effective Approaches for Watermarking XML Data. ”Department of Computer Science, the Hong Kong University of Science and Technology, Hong Kong, 2005**.**

[19] Yanqun Zhang, “Digital Water marking Technology: A Review. ”Department of Computer Science and Technology, China University of Mining and Technology, 2009.

[20] Yingji u Li, Member, IEEE, VipinSwarup, and SushilJajodia, Senior Member, IEEE, “Fingerprinting Relational Databases: Schemes and Specialties.” Vol no.2, March 2005.

AUTHORS PROFILE

Prof. R.Manjula received her B.E in Computer Science & Engineering from University of Vishwesvaraya and Engineering, Bangalore, Karnataka State, India in 1992 and M.E in Software Engineering from Anna University, Tamil Nadu, India in 2001. She is now working as Associate Professor and also as Ph.d Candidate affiliated with School of Computing Science and Engineering at Vellore Institute of Technology, Vellore, India. Her area of specialization includes Software Process modeling, Software Metrics, Software Metrics, Software Testing and Metrics, XML-Web Services and Service Oriented Architecture.

Nagarjuna.Settipalli received his B.Tech in Computer Science and Engineering from Newton’s Institute of Engineering, Macherla, Andhra Pradesh State, India in 2008. He is now Pursuing his M.Tech at VIT University, Vellore, Tamil Nadu State, India. His interest includes watermarking, wireless network security, and he also developed a mobile application GSM Based Ticketing System for Airlines and a Cache Simulator as a miniproject.