International Journal of Engineering Innovation & Research
Volume 1, Issue 5, ISSN : 2277 – 5668

Survey of Secure Multimedia Database Using Public Key Cryptography Method and Optimization Techniques

I.Jasmine Selvakumari Jeya
Research Scholar Department of CSE
Hindusthan College of Engineering and Technology
Coimbatore-641 045, Tamil Nadu, India
wjasminejeya@gmail.com
Mobile: +91 9443381609

Dr.J.Suganthi
Professor & Head Department of CSE
Hindusthan College of Engineering and Technology
Coimbatore-641 045, Tamil Nadu, India
Sugi_jeyan@hotmail.com
Mobile: +91 9894068005

Abstract **– Solving the security issues in multimedia database is important issues in stock market data, consumer behavior data, power consumption data, weather data, and internet based application, content distribution application and medical data emerged as a important solution to provide copyright protection, tamper detection, traitor tracing, maintaining integrity of multimedia data. In earlier existing systems the relational database will be partition, watermarked and directly send to the transmission channel, in these systems while sending relational data from server to client attacker easily copy the data and create same copy of original data. Here there is no security in watermarked relational data. The proposed system before sending the multimedia data it apply the composite partition algorithm, watermark optimization techniques and these data are converting into PDF file format. Encrypt the PDF file using RSA algorithm with Jen's public key and send it to the client side. In the client side decryption will be done using same algorithm with Jen's private key to get the original multimedia data and apply the data partition techniques and watermark optimization Techniques. This encryption and decryption technique an attacker copies the data but may not read, insert, delete and update the multimedia data.**

Keywords **– Multimedia database, copy right protection, transmission channel, composite partition, public key, private key, optimization techniques.**

I. INTRODUCTION

The rapid growth of internet and distributed technologies are ability to access and distribute the digital contents [1]. In this paper proposed the multimedia relational database, there are many different between the structure of the multimedia data and relational database. The most watermarking research is concentrated digital data such as audio, video and images. The different between digital watermarking and multimedia relational database is three important aspects [2].Firstly encryption and decryption is used RSA algorithm, watermarking is imperceptible so that it is neither visible by human eyes nor hearable by human ears. It means it can be detected by special processing or special circuit only [2].So that the watermark will not affect the original host data.

Secondly the watermark and multimedia relational database are always together. If watermark multimedia relational database are converted into other file format, the watermark will not be eliminated [1]. The third one is the watermarks will have exactly the same transformation by looking at the watermarks. The digital data are secure through the watermarking concept and cryptography systems.

A watermark describes information that can be used to prove the ownership of data such as the owner, origin, or recipient of the content. Secure embedding requires that the embedded watermark must not be easily tampered with forged, or removed from the watermarked data [3].Cryptography is where security engineering meets mathematics. It provides tools that underlie most modern security protocols. It is probably the key enabling technology for protecting distributed systems, yet it is surprisingly hard to do right [4].

Cryptography has often been used to protect them in the wrong things, or used to protect them in the wrong way. Digital watermarking is defined as the imperceptibly altering a work in order to embed information about that work. In the recent years copy right protection of digital content became a serious problem due to rapid development in technology. Watermarking is one of the important techniques is used to solve the copyright-protection problem.

Digital watermarking can be classified as visible and invisible.

A. Visible Watermarks

The watermarks are viewable to the normal eye such as relational database, bills, and company logos. This type of watermark can be easy viewable without any mathematical calculation but these embedded watermarks can be destroyed easily.

B. Invisible Watermarks

Watermark is embedded are secret, only the authorized persons extracts the watermarks. This type of watermarks is not viewable by an ordinary eye. Invisible watermarks are more secure and robust than visible watermarks. Many of the paper proposed in this model.

In this paper provide the security of the multimedia relational database by using public key RSA algorithm for encryption and decryption .A watermark detection is blinded because watermarks optimization values are embedded. So that attacker copies the database but may not read the watermark multimedia database. The main aim of the decoding is based on threshold based techniques and minimizes the probability of decoding errors. Finally the watermarking technique applies in the tuple deletion, insertion and update attacks.

II. RELATED WORKS

Mohamed Shehab and Arif Ghafoor [1] explained the various types of attacks in watermark relational database. In this paper discussed about how to solve the optimization problem and discuss the efficient techniques to solve the optimization problem and to handle the constraints. This technique is resilient to watermark synchronization errors because the data partition approach that does not require marker tuples. Watermark decoding is based on threshold based techniques so that it minimizes the probability of decoding errors.

Sion et al [5] proposed a watermarking technique that embeds the single bit watermarks in the data statistics. The data partitioning technique used in based on the use of special marker tuples which makes it vulnerable to watermark synchronization errors. Thus such technique is not resilient to deletion and insertion attacks.

Rakesh Agrawal and Jerry Kiernan [6] proved that watermarking technique is robust against various types of attacks. The watermarking technique ensures the bit positions of some of the attributes of some of the tuples contain specific values. The tuples attributes within a tuple, bit positions in an attribute, and specific bit values are algorithmically determined under the control of the private key known only the owner of the data.

Yuer Wang, Zhongjie Zhu and Feng Liang and Gangyi Jiang [7] proposed an adaptive mechanism is adopted to choose an optimal embedding scheme for each data sheet. The error correcting coding technology and the majority voting principle are employed to improve the robustness of watermarking. The watermarking can meet the invisibility and the blind detection and good resistance to conventional attacks.

Min Huang, Jiaheng Cao, Zhiyong peng and Ying Fang [8] proposed a New Watermarking Mechanism(NWM) using classifying and twice majority voting method to data's usability relational structure, semantic constraints and robust to various attacks.

Cong Jin and Yu Fu [9] explained the conceptual framework for relational database based on secret sharing technology. These technologies break the main secret into multiple parts and hide them individually in a relational database.

Haiting Cui and Xinchun Cui [10] proposed a public key cryptography, a novel algorithm for watermarking relational databases. In this algorithm, asymmetric keys are used in insetting and detecting database watermark and user can't get anything of the private key copyright through public key.

Hsien-Chu Wu and Frang-Yu Hsu [11] proposed SVR predictive function to obtain characteristic of the database and uses Huffman coding to encode the characteristic for compressing important payload information of the database is used to accomplish tampering detection.

Zhongyan Hu, and Zaihui [12] proposed a novel watermarking method, which embeds an image watermark into relational results verify the effectiveness of the database.

Gross- Amblard [13] proposed a watermarking technique for XML documents and theoretically investigates links between query result preservation and acceptable watermarking alterations.

Chuamcian Jiang, Xiaowel Chen and Zhi Li, [14], proposed a watermarking algorithm, which can embed the watermark into relational database successfully in DWT domain. Watermark embedding is difficult for relational databases. This paper focuses on wavelet high frequency coefficients and easy to embed the watermark bit.

Mustapha Machkour, Youness Idrissi Khamlichi, and Karim Afdel, [15], proposed a content-based watermarking technique, patient's information are encrypted and inserted in an image associated to it. This image, with faculties of object-relational and object-oriented databases, is directly integrated into the database. This is used to check the integrity of the image using the edge map and invariant moments.

Chaokun Wang, Jianmia Wang, Ming Zhou and Guisheng Chen, [16], presented the improvement in watermark security by using image scrambling technology which confuse the well-regulated watermarking information and diffuse errors.

Hequn Xian and Dengguo Feng [17] proposed the data owner controls the watermark key and the watermark generation process, which makes it possible for the owner to falsely accuse an innocent user of pirating. A novel watermark scheme is to solve the problem of leakage identification for the secret relational data.

Jianhua Sun, Zaihui Cao, Zhongyan hu [18], proposed a novel multiple watermarking schemes, which embeds two image watermark into relational database.

Xiangrong Xiao, Xingming Sun and Minggang Chen [19], proposed a novel robust watermarking algorithm based on the second_LSB. The algorithm first groups the data by the hash value of the primary key and positions with the second_LSB of data is every group. The watermark is not directly embedded in one single item, but one bit is embedded into one group by setting a pseudo-random number to the LSB of the data.

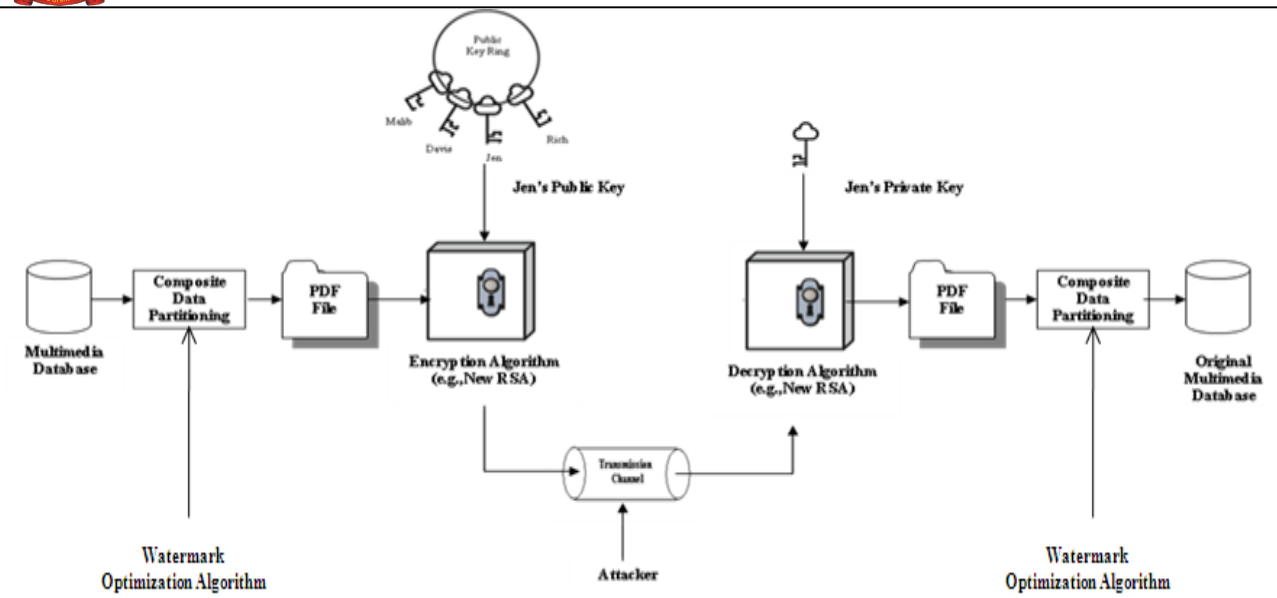

Fig.1. Block Diagram of Watermark Embedding and Public Key Cryptography System

Zhi-Hao [20] proposed a novel method for watermarking relational database, which uses an image as the watermark and this approach is more intuitive and it support the way of watermark identification.

Kalyin huang [21] proposed a cluster-based database watermarking technique which applies cluster theory to the database. This technique partitions subset through clustering the data in original database. The cluster method makes watermarking information more disperse and hidden.

Xiaomei Dong, [22], proposed a database watermarking algorithm resistive to invariability attacks. This algorithm calculating the characteristic code of the original database based on the contents of the database.

Ali Al-Haj and Ashraf Odeh, [23], proposed a watermarking algorithm based on hiding watermark bits in spaces of non-numeric, multi-word, attributes of subsets of tuples. A major advantage of using this approach is the large bit-capacity available to hide large watermark.

Sukriti Bhaltacharya and Agostino Cortesi [24] proposed it does not depend on any particular type of attributes (categorical, numerical) and ensures both authentication and integrity. It is partition based and is able to detect and locate modifications of the trace the group which is possibly affected when a tuple is tampered.

Meixing Le, Angelos Stavrou [25] present Double Guard, an Intrusion Detection Systems system that models the network behavior of user sessions across both the front-end web server and the back-end database. By monitoring both web and subsequent database requests, it is able to ferret out attacks that independent IDS would not be able to identify. Double Guard can detect SQL injection attacks by taking the structures of web requests and database queries without looking into the values of input parameters.

III. CHARACTERISTICS OF DIGITAL WATERMARKS

The main characteristics of digital watermarks are:

A. Robustness

The watermark should be able to with stand after embedding watermark bit and public key cryptography systems, etc.

B. Imperceptibility

The watermark multimedia database should look like same as the original database to the normal eye. The viewer cannot detect that watermark is embedded in it.

C. Security

An unauthorized person cannot detect, retrieve, or modify the embedded watermark database used by the public key cryptography methods.

D. Data Capacity

The amount of information can be stored within the content. The visible and invisible digital watermark can be classified into three types:

1) Robust Watermark

Robust watermark are detectable even after some watermark operation such as watermarking algorithm and cryptography.

2) Fragile Watermark

Fragile watermarks became invalid even if a slight modification is done to the watermarked image; fragile watermarks are mainly used for authentication purpose.

3) Semi-fragile Watermark

It allows some acceptable distortion to the watermarked data. Beyond this acceptance level if any modification is done to the watermarked data, the watermark will not be detected.

Table:1 Comparisons of Optimization Techniques, Sion et al. Techniques, Double Guard Attack and Proposed Approach (Optimization Techniques and Cryptography Method

	Optimization Techniques[1]	Double Guard Attack[25]	Soin et al.Techniques[5]	Proposed Approach(Optimization Techniques and Public Key Cryptography Method)
Types of Database	Relational Database	Relational Database	Relational Database	Multimedia Database
Data Partition Type	Secure Hash Function	Nil	Hash algorithm	Composite data partition(Range and Hash Partition) and optimization algorithm
Watermark Bits	Multi Bit Encoding	Nil	Single Bit encoding	Multi Bit Encoding
Encryption and Decryption Algorithm	Nil	Nil	Nil	RSA Algorithm
Synchronization Error	Highly vulnerable to such error	Nil	Not vulnerable to such error(Need special marker tuples)	Highly vulnerable to such error (optimization algorithm)
Optimization Algorithm	Genetic and Pattern search algorithm	Nil	Nil	Optimization algorithm
Attacker Channel	Yes	Yes	No	Yes
Data Loss	20%	Nil because this model use web server attack and database attack	80%	Less than 20% because use the encryption algorithm
Time Complexity	Less	Less	Less	Less
Space Complexity	Need large Storage space	Very Loss	Need large storage space	Need less storage space because use optimization techniques
Data Redundancy	No, because use the optimization techniques for data partition	Nil	Yes	No because use the optimization techniques for data partition and RSA Algorithm
Primary Key and Marker Tuples	No need	No Need	Use primary key and special marker tuples for data partition	No need because use the optimization algorithm.
Types of Attack	Insert, delete & Update	Privilege attack, Hijack attack, SQL Injection attack and Direct database attack	Nil	Modify Double Guard Attack
Attack Privileges	Insert, delete & Update	Insert, Delete, Update, Views and Triggers	Nil	Insert, Delete, Update, Views and Triggers

IV. SYSTEM MODEL

Figure 1 shows the main component of the system model. There are two stages in this model. They are encoding stage and decoding stage. In the encoding stage a multimedia data set M partition into $\{p_0,p_1,p_2,\ldots..p_n\}$ partition using composite data partition algorithm and it will apply in the optimization techniques for non overlapping partition and reduce the synchronization error. For the more security purpose it is convert the partition data into PDF file format and these file insert into new public key cryptography algorithm with Jen's public key after that generate the encrypted PDF file in the encoding stage.

The encrypted file transmits through the attacker channel and gives the tuple insertion, alteration and deletion attack. In the decoding stage encrypted file is converted into the original multimedia database using same cryptography algorithm using Jen's private key after that it is apply into the data partition and it will display the same multimedia database.

International Journal of Engineering Innovation & Research
Volume 1, Issue 5, ISSN : 2277 – 5668

V. DATA PARTITIONING ALGORITHM

Many of the paper proposed only hash function for data partitioning [1]. In this approach for more security and have apply the composite range-hash partitioning algorithm for non overlapping partition. Partitioning enhances the performance, manageability, and availability of a wide variety of applications and helps reduce the total cost of ownership for storing large amounts of data. Partitioning allows a table, index, or index-organized table to be subdivided into smaller pieces, where each piece of such a database object is called a partition. Each partition has its own name, and may optionally have its own storage characteristics. Figure 2 shows the overall structure of the Range-Hash partition. There are two keys are used in this diagram.key1 is sales_date create in Range partition and key2 is sales_id create in Hash partition. It is divided into five partitions and each one depends upon the Range-Hash partition.

In the previous approach used the single key for the data partition. If the attacker know the single key, it is easy to copy the original data. The proposed approach used the two partition method and two secrete keys for more security and minimizes the synchronization errors. Table 1 shows the comparisons of previous approach and proposed watermark approach. The example query for range-hash partition is given in table 2. RSA algorithm is used to convert the PDF file into encrypted file and decrypted file. So that nobody can view the data and copy the data.

Table:2 Example of Range and Hash Partition

```
CREATE TABLE sales_composite
(salesman_id  NUMBER(5),
salesman_name VARCHAR2(30),
sales_amount  NUMBER(10),
sales_date    DATE)
PARTITION BY RANGE(sales_date)
SUBPARTITION BY HASH(salesman_id)
SUBPARTITION TEMPLATE(
SUBPARTITION sp1 TABLESPACE data1,
SUBPARTITION sp2 TABLESPACE data2)
(PARTITION sales_jan2000 VALUES LESS
THAN(TO_DATE('02/01/2000','DD/MM/YYYY'))
PARTITION sales_feb2000 VALUES LESS
THAN(TO_DATE('03/01/2000','DD/MM/YYYY')));
```

Many of the research used to convert the relational database into embedded watermark bit using watermarking algorithm [3]. In this approach partition the multimedia data using range and hash partition and apply the watermark optimization algorithm. The optimization technique is used to generate the optimal watermark bits for each partition. Then each partition is converted into PDF file format and sends it into the encryption algorithm. The RSA algorithm involves three steps: key generation, encryption and decryption. The public key can be known to everyone and is used for encryption of multimedia database and the encrypted data can be decrypted using the private key. The attacker is including in transmission channel. It has deletion attack, insertion attack and modification attack. Finally analyze how much security is applying this model.

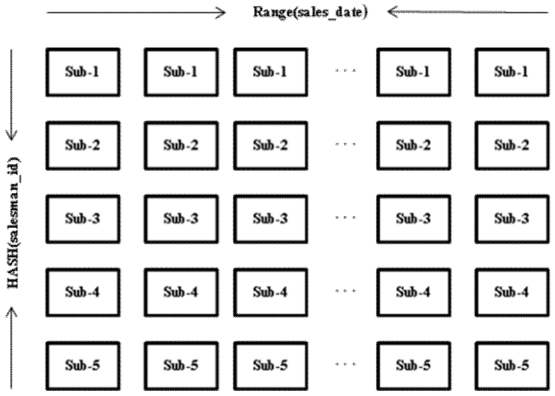

Fig.2. Structure of the Range-Hash Partition

VI. CONCLUSION AND FUTURE WORKS

Comparison of proposed approach and previous approach the data partition, cryptography encryption and decryption and optimization techniques is used to secure the watermarking multimedia database. In the previous approach the encryption will not be used and directly send to the transmission channel. So there is no security in the watermark relational database. Before sending the watermarked multimedia data into the encrypted algorithm the database is partition and using optimization techniques. This output is transmitted into the attacker channel and decrypted using Jen's private key and will partition the original data using watermark optimization techniques. Finally this approach will display the original multimedia database.

REFERENCES

[1] Mohamed Shehab and Arif Ghafoor, "Watermarking Relational Databases using Optimization Techniques," *IEEE Transaction on Knowledge and data Engineering*, Vol.20, No.1, January, 2008.

[2] R.Manjula and Nagarjuna Sellipalli, "Securing Watermaked – Relational Data using Encryption and Decryption," *ARPN Journal of Systems and Software* , Vol.1 No.2, May, 2011.

[3] R.Wolfgang, C.Podilchuk, and E.Delp, "Perceptual watermarks for Digital Images and Video," *Proc. IEEE*, vol.87, pp. 1108-1126, July, 1999.

[4] William Stallings, "Cryptography and Network Security Principles and Practices," *Prentice Hall*, 2006.

[5] R.Sion,M.Atallah, and S.Prabhakar, "Rights protection for Relational Data," *ÏEEE Trans. Knowledge and Data Eng.*,vol.16,no.6,June, 2004.

[6] *R. Agrawal and J. Kiernan, "Watermarking Relational Databases," Proc. 28th Int'l Conf. Very Large Data Bases, 2002.*

[7] Yuer Wang, Zhongjie Zhu and Feng Liang and Gangyi Jiang, "Watermarking Relational Data based on Adaptive Mechanism," *proceedings of the IEEE International conference on Information and Automation*, June 20-23, 2008.

[8] Min Huang, Jiaheng Cao, Zhiyong peng and Ying Fang, "Ä new watermark Mechanism for Relational Data," *Proceedings of IEEE*, 2004.

[9] Cong Jin, Yu Fu and Feng Tao, "The Watermarking Model for Relational Database Based on Watermarking Sharing," *Proceeding of IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 2006..

[10] Hailing Cui, Xinchun Cui, and Mailing Meng, "A public key Cryptography based algorithm for watermarking Relational Databases," *Proceeding of IEEE International Conference on Intelligent Information Hiding and Multimedia Signal processing*, 2008.

[11] Hsien-chu Wu and Frang-Yu Hsu, and Huang-Yu Chen, "Tamper Detection of Relational Database Based on SVR Predictive Difference," *Proceeding of IEEE Eighth International conference on Intelligent Systems Design and Applications*, 2008.

[12] Zhongyan Hu Zaihui Cao and Jianhua Sun, "An Image based Algorithm for watermarking Relational Databases," *Proceeding of IEEE International Conference on Measuring Technology and Mechanisms Automation*, 2009.

[13] Gross-Amblard.D,"Query-preserving watermarking of relational databases and xml documents," *Proc. of the 22nd ACM SIGMOD-SIGACT-SIGART Symp. On Principles of Database*, pp 191–201, June 2003.

[14] Chuanxian Jiang, Xiaowei Chen and Zhi Li, "Watermarking Relational Databases for ownership protection based on DWT," *Proceeding of IEEE fifth International Conference on Information Assurance and Security*, 2009.

[15] Mustapha Machkour, Youness Idrissi, "Data Security in Medical Information System," *Proceeding of IEEE International Conference*, 2009.

[16] Chaokun Wang Jianmin Wang and Ming Zhou Guisheng chen, "ATBami: An Arnold Transform Based on Watermarking Relational data," *Proceeding of IEEE International Conference on Multimedia and Ubiquitous Engineering*, 2008.

[17] Hequn Xian and Dengguo Feng, "Leakage Identification for secret Relational Data using Shadowed Watermarks," *Proceedings of IEEE International Conference on Communication Software and Networks*, 2009.

[18] Jianhua Sun, Zaihui Cao, Zhongyan hu, "Multiple Watermarking Relational Databases using Image," *Proceeding of International Conference on Multimedia and Information Technology*, 2008.

[19] Xiangrong Xiao, Xingming Sun and Minggang Chen, "Second – LSB-Dependent Robust Watermarking for Relational Database," *Proceeding of IEEE Third International Symposium on Information Assurance and Security*, 2007.

[20] Zhi-Hao zhang, Xiao-Ming Jin, Jian-Min Wang, De-YiLi, "Watermarking Relational Database using Image," *Proceedings of IEEE Third International Conference on Machine Learning and cybernetics, Shanghai*, 26-29 August, 2004.

[21] Kalyin huang, Min Yue, Pengfei Chen Yanshan He, and Xizoyun Chen, "A cluster-Based Watermarking Techniques for Relational Database," *Proceeding of IEEE International workshop on Database Technology and Applications*, 2009.

[22] Xiaomei Dong, Xiaohua Li, Ge Yu, Lei Zheng, " An Algorithm Resistive to Invertibility attack in watermarking Relational Databases," *Proceeding of IEEE International Conference on Chinese Control and Decision Conference*, 2009.

[23] Ali Al-Haj and Ashraf Odeh," Robust and Blind Watermarking of Relational Database Systems, "*Journal of Computer Science* 4(12): 1024-1029, 2008.

[24] Sukriti Bhaltacharya and Agostino Cortesi, "Database Authentication By Distortion free Watermarking", *5th International conference on software and data technologies, 2010.*

[25] Meixing Le, Angelos Stavrou**, "**DoubleGuard: Detecting Intrusions in Multitier Web Applications**,"** *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 4, July/August 2012.

AUTHOR'S PROFILE

I.JASMINE SELVAKUMARI JEYA
is a Research Scholar and Assistant Professor in Department of Computer Science and Engineering at Hindusthan College of Engineering and Technology, Coimbatore Her research work focuses on security issues in various database using optimization techniques.

DR.J.SUGANTHI
is working as a Vice Principal and Head of the Department in Computer Science and Engineering, Hindusthan College of Engineering and Technology Coimbatore. She has more than 20 years of academic experience. Her area of research includes Data Mining, Modeling and Simulation, Network Security, Digital Image Processing, Neural Networks, Soft Computing Techniques, Evolutionary strategies. She has published more than 25 books and papers. She is an active consultant for research projects.

.