मयि सर्वमिदं प्रोतं
B S A I T M
Since 2001

Journal of Network Communications and Emerging Technologies (JNCET) www.jncet.org
Volume 5, Special Issue 2, December (2015)

Database Watermarking: A Review

Srijan Goswami
Dept of IT, Institute of Computer Engineers, West Bengal, India

Payel Roy
Dept. of CA, JIS College of Engineering, Kalyani, West Bengal, India

Saptarshi Das
Dept of CSE, Saroj Mohan Institute of Technology, Guptipara, West Bengal, India

Nivedita Kar
Dept. of CA, JIS College of Engineering, Kalyani, West Bengal, India

Urmimala Dey
Dept. of CA, JIS College of Engineering, Kalyani, West Bengal, India.

Abstract - Proving the ownership rights in the outsourced databases is an important issue now-a-days. The watermarking method is a technique that can authenticate the database and confirm the ownership. Another major issue is security of the database. This can also be achieved by watermarking. This paper mainly offers a comparative study on the various types of transformation based watermarking methods to achieve the authentication as well as the security.

Index Terms– Watermarking, Authentication, Ownership, Database.

This paper is presented at International Conference on Recent Trends in Computer and information Technology Research on 25th& 26th September (2015) conducted by B. S. Anangpuria Institute of Technology & Management, Village-Alampur, Ballabgarh-Sohna Road, Faridabad.

1. INTRODUCTION

Recently, watermarking has emerged as an active research area. Previously, many theoretical models and applications have been proposed. In various watermarking models, the watermark detector can communicate with the sewer. For example, the detector in the Digimarc Media Bridge Reader makes use of the Internet to search more information based on the extracted message. The theoretical models like zero-knowledge proof [1] and the public watermarking also exploit the communication to the enhance security.

In last few years, some modern enterprises have started bothering about the rapid development of data assets. The enterprises collect a huge amount of the valuable data such as the customers, suppliers, competitions, etc. According to the data in the databases, the enterprise managers can make the significant strategy of the company for the future development. The data stored in various databases often contains important information. Hence, the database authentication can be a solution to avoid attack or threats on the data or the databases.

2. LITERATURE REVIEW

There are some related works in this research area. In 2003 Sujoy et al.[2], proposed a watermarking formulation which exploits a-prior knowledge of the image database. This formulation was realistic because in some applications, the detector had access to the internet. They gave few schemes for the various settings. They also analyzed their performance based on the assumption that the image and noise were Gaussian. They also tested their main idea on the non-Gaussian images that were a set of natural images. In 2007 Meng-Hsiun et al.[3], proposed a scheme that combines the fragile watermarking and SVR technique to achieve the authentication of the database. SVR was exploited to learn the relative between the referenced attribute of tuples and the training samples from the database while embedding the watermark into the selected numeric attribute of the protected table. In 2009 Kaiyin et al.[4], designed a new watermarking technique for relational database using cluster theory. This technique was partitioned subset through clustering the data in the original database and also determined the quantity of the embedding and embedding position by the clustering results. In 2009 Chuanxian et al.[5], presented a study of the feasibility of the watermark embedding in the wavelet domain for a relational database. They studied the feature of the spatial domain of database watermark. It also analyzed that the high frequency wavelet coefficients of the corresponding data followed the Gaussian distribution. Based on the above method of the linear correlation detecting and factors, they proposed the watermarking algorithm for relational database that can embed the watermark successfully in the wavelet domain. In 2010 Mahmoud et al.[6], proposed a novel reversible relational database watermarking technique. This technique could prove the ownership of the database's owner and also attains the full recovery of original database relation when the watermark information extracted and also authenticated. A majority voting technique was also applied to rectify the watermark bits extracted from the data at the watermark extraction phase. In 2010 Song Yigeet al.[7], Presented a relational database robust watermarking algorithm that was based on DCT transform and took the advantage of the frequency domain approach of the multimedia digital watermarking into the relational database watermarking. By the DCT transform on grouped and sorted tuples and modified some of the transformed frequency coefficients to the embed image watermark, only the affecting one attribute of every tuple, the algorithm had good watermarking invisibility and small errors had caused for data. Again in 2010 Hosseinet al.[8], presented a resilient watermarking scheme for the relational database that embeds image bits in small size database as watermark. Experimental results showed that it was robust to the important attacks and the comparison proposed technique with the previously posed methods showed the superiority of this technique to the modification attack. In 2012 Jung-Nan et al.[9], proposed a reversible fragile watermark algorithm which was based on SVR prediction that used the FP-free data mining method.

The proposed scheme could also use to verify the contents of database. In 2012 Udai P. R. et al.[10] proposed an effective process for the database watermarking in which a proper tuple in the database was chosen for marking and then the chosen bits of the image replaced some bits of the opted attributes of the particular tuple. In 2013 Kamran et al.[11], proposed a technique which was highly resilient against the insertion, deletion, modification and multifaceted attack yet that results in the minimum distortions in original dataset. Regardless of the malicious attack on the watermarked data, watermark bits were successfully decoded with accuracy because decoding accuracy of proposed approach was independent of usability constraints. In 2014 Javier et al.[12], Proposed the robust lossless relational database watermarking technique that made the use of circular histogram modulation. It could be used for verifying the integrity of database and also for verifying the authenticity even if the database had been modified. They had theoretically established and also verified experimentally the performance of the method in terms of the capacity and robustness against the common two attacks: tuple deletion and tuple insertion. In 2015 Rohit et al.[13], proposed a new fragile biometric watermarking process was in the hybrid domain using the Compressive Sensing theory framework.

This current work proposes a comparative study on database watermarking techniques to choose the best method for the authentication and the security of the database.

3. METHODOLOGY

There are several methods which can be used to watermark the database. Some of these techniques were used for our study.

A. Fragile Database Watermarking*:*

In this section, SVR technique was used to get idea about the data correlations of the preserved database and embed the watermark bits. SVR is similar to support vector machine (SVM) applications on function approximation with prediction, and this was proposed by Vapnik [14, 15]. Shen et al.[16] and Tsai et al.[17] proposed few other schemes for images by using SVM to study the pixel-value correlations, subsequently. The function of SVR is to exercise SVM to find out the optimal decision function by manipulating the correlates among the given fragments. Again, this optimal decision function can be used to forecast the object value with the sample data. According to the data correlations of the preserved database, in the proposed idea, fields of a tuple were used to be the feature values, and a tolerable field was selected to get embedded the watermark bit in the tuple.

It was assumed that the architecture of the i^{th} tuple in the preserved table T was t_i (P_K, N_i, C_1, C_2, ..., C_n) where PK is the primary key field, Ni is the tolerable numeric field and C_1, C_2, ..., C_n are other n numeric fields in the table. The numeric fields against negligible distortion were chosen as the objective dataset and the remaining attributes were exercised to be feature datasets. [18] Total number of tuples in the table was referred as m. In the proposed idea, there are three phases introduced to achieve database authentication. All this we can achieve through these three phases:

- Training Phase: in which the SVR gets trained with the tuples, which has been selected by pseudo random number generation code through a private key.

- Embedding phase: in this phase all the tuples gets embedded with watermark bits. For this each numeric field of the table is predicted and trained though SVR predicting function as the bit of the attribute is watermarked the value of that field gets changed by incrementing it by 1.
- Tamper Detection phase: in this phase detection of any kind of tampering or modification of the data has been done or not. It can be detected by comparing the present watermark bit with the original one.

B. Robust Watermarking Method:

Robust watermark algorithm was used to insert watermark bits into the dataset of Alice. This algorithm takes a secret key (S_k) and the watermark bits (W_b) as input and converts the dataset D_s into watermarked dataset D_w. For convenience a reference, Table 1 has been created with the major symbols used in this paper. The distortions made by watermarking are enclosed with the usability constraints matrix UM. In this technique, for every possible type of application, it is defined only once that will use the dataset. The watermark encoding procedure is summarized as follows:

C. Watermark Embedding-

The watermark bits are inserted in the selected tuples by using a robust watermarking function. A bit embedding statistics Δ are being exercised to compute the correction factor τ. This technique inserts every bit of the watermark in each and every selected tuple of each fragment; as a result, it leads to robustness against malicious attacks. The watermarked dataset D_w is handed over to Bob where an invador – Mallory – focuses at exploiting the watermark by introducing different types of attacks. Watermark decoding is the procedure has been discussed for extracting the embedded watermark out of the watermarked dataset D_w, using secret parameters: the secret key S_k, correction factor τ, and decoding threshold γ.

The watermark decoding process has been summarized in the steps followed:

D. Data Partitioning-

The same data partition algorithm has been used as in the watermark encoding phase. A dataset gets fragmented into some non-overlapping fragments with the use of a secret key in conjunction with a cryptographic secure hash function.

E. Identification of Watermarked Dataset-

The watermarked tuples are identified by exercising the same procedure as used at the time of encoding.

F. Watermark Decoding-

At this stage, τ and γ the correction factor, and decoding threshold respectively, are used to decode watermark bits. The decoding accuracy of this algorithm does not depend on the usability constraints. As a result, ultimate decoding accuracy is achieved irrespective of the volume of data alterations made by the attacker in the watermarked data.

G. DCT Transform based Relational Database Robust Watermarking Algorithm:

The basic idea of this algorithm was: First of all calculate tuple hash for each tuple of the table based on the user's private key and the primary key of the tuple. Next, calculate group position of each tuple exercising the tuple hash and number of groups in the relation g so that we can number the tuples secretly within groups by the tuple hash. Further, moderate size of a group m that is resolute according to the overall number of tuples n and the number of times, watermark has been embedded. In addition, one of the attributes from the optional attributes was selected by tuple hash for embedding purpose which decides the value involved in DCT with the upper range of the bits. Limit of bits allowed for modification of the attribute k_j is set such a way, so that we can limit the modification in the admissible error range. Afterwards, the medium frequency coefficient gets modified after DCT and finally the attribute values which are determined after IDCT transform to the relation metric were written back and some of them were allowed a certain degree of error. That error did not affect the content of the data.

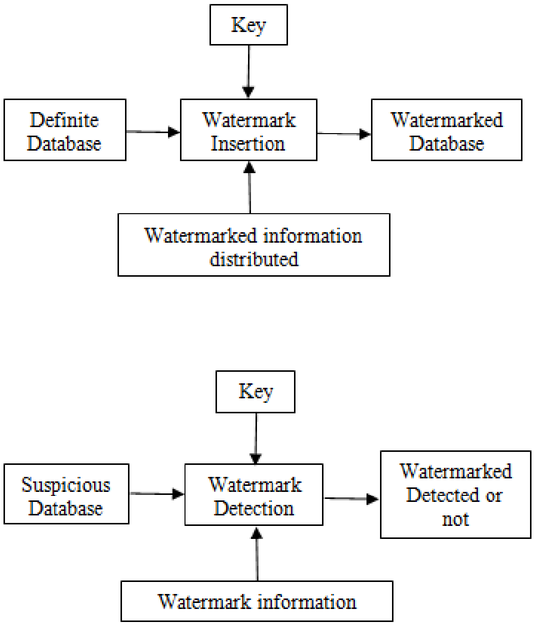

Fig: Basic Database Watermarking Procedure

Here, "degree of error" is described by k_j which means the permissible degree of modifications allowed by attributes.

Besides, the primary key of the database will not be modified, [16] it can be used to address this attack.

4. BIOMEDICAL DATA WATERMARKING

In recent times a number of study have been reported in the area of biomedical data (signal and image) watermarking.

In 2012 Dey et al.[19] paper reported a process of reversible binary watermark embedding into the PPG signal and a watermark extraction mechanism using the Prediction Error Based Algorithm. In this proposal, the generated watermark signal having a satisfactory level of imperceptibility and curvature was collated to the genuine Photoplethysmographic (PPG) signal. In 2012 Dey et al.[20] predicted a novel session based on blind watermarking method with a secret key by embedding binary watermark images into Intravascular ultrasound (IVUS) video. The IVUS video is a tactful diagnostic tool that is used to perceive various cardio-vascular diseases by measuring and recording the anatomy of the heart and adjoined blood vessels in exquisite detail. In 2012 Dey et al.[21] existing work predicts a Lifting Wavelet Transformation based method of binary watermark embedding within the PPG signal as well as the process of extracting watermark from the PPG signal. In this prediction the generated watermarked signal having a satisfactory level of imperceptibility and distortion is collated to the original PPG signal. In 2013 Dey et al.[22] proposed a new method to design the vigorous biomedical content authentication system through embedding the logo of hospital within the electrocardiogram signal through both discrete wavelet transformation (DWT) and cuckoo search (CS). In 2013 Dey et al.[23] predicted a process of attaching watermark in the edges of the images which is the most efficacious for those medical images which are corollary of such imaging processes which has edge detection as one of the essential intermediate parts of the process. Canny edge based watermarking technique is applied on three different medical images: IVUS image, retinal vascular tree image, CT Scan image and the correlation values of the original watermark image and the extracted watermark image are calculated to show the level of acceptability of the predicted technique. In 2014 Pal et al.[24] extant work a reversible watermarking method (Odd-Even Method) is used for watermark insertion and extraction in a bio medical image with large data hiding capacity, security as well as high watermarked quality. In 2014 Chakraborty et al.[25], predicted a method that fixes secret bits into the gray planes of color image, using interpolation method and few trigonometric functions. In 2015 Banerjee et.al. [26], proposed a new color image watermarking process, using the residue number system (RNS). It refers to a large integer using the set of smaller integers that lies on the Chinese remainder theorem of the modular arithmetic for its operation.

There are many other important works of watermarking in the medical field using various data such as text, image, audio etc. [27-36]

1. EXISTING FRAMEWORK

The enhancing utilize of databases in purposes beyond "behind-the-firewalls data processing" is making a comparable require for watermarking databases. The Internet is applying marvelous pressure on data suppliers to produce services that permit users to explore and access databases distantly. Even though this tendency is an advantage to the end users, it illustrates the data suppliers to the threat of data larceny. Providers are consequently insisting technology for discovering pirated copies of their databases. There many frameworks are available for database watermarking. Here are some examples:

A. Watermark Bits Generation-

Watermark bits string 'W_b' is generated through UTC (Coordinated Universal Time) date-time, which is a particular time standard exercised to synchronize the time all over the world. These bits are provided as the instruction to the watermark encoding function.

B. Data partitioning-

The dataset D_s gets fragmented into n non-overlapping fragments with the use of secret key S_k in conjunction with a cryptographic secure hash function.

C. Selection of dataset for watermarking-

To have minimum distortions only a couple of tuples are selected for watermarking at first.

6. COMPARED TABLE

Sl. No.	Author	Motivation	Limitation
1.	Sujoy R. et al. (2003)	They proposed a watermarking formulation which exploits a-prior knowledge of the image database. This formulation was realistic because in some applications, the detector had access to internet. They gave few schemes for the various settings. They also analyzed their performance based on the assumption that the image and noise were Gaussian. They also tested their main idea on the non-Gaussian images that was a set of natural images.	The experiment and analysis showed improvement in performance by using a-prior knowledge of only for image database.
2.	Meng-Hsiun T. et al.(2007)	Proposed a scheme that combines the fragile watermarking and SVR technique to achieve the authentication of the database. SVR was exploited to learn the relative between the referenced attribute of tuples and the training samples from the database while embedding the watermark into the selected numeric attribute of the protected table.	The trained SVR predicting function could only be effective to predict objective value, detect and position of the tamper.
3.	Kaiyin H. et al.(2009)	Designed a new watermarking technique for relational database using cluster theory. This technique was partitioned subset through clustering the data in the original database and also determined the quantity of the embedding and embedding position by the clustering results.	They adopt an odd-even modifying method that assured the minimum modification to the original database.
4.	Chuanxian J. et al.(2009)	Presented a study of the feasibility of the watermark embedding in the wavelet domain for a relational database. They studied the feature of the spatial domain of database watermark. It also analyzed that the high frequency wavelet coefficients of the corresponding data followed the Gaussian distribution. Based on the above method of the linear correlation detecting and factors , they proposed the Watermarking algorithm for relational database	After the watermark distribution to the different parts of the database, the invisibility of the watermark was improved to a certain level.

		that can embed the watermark successfully in the wavelet domain.	
5.	Mahmoud E. et al.(2010)	Proposed a novel reversible relational database watermarking technique. This technique could prove the ownership of the database's owner and also attains the full recovery of original database relation when the watermark information extracted and also authenticated. A majority voting technique was also applied to rectify the watermark bits extracted from the data at the watermark extraction phase.	When the distortion amount on the data set was decreased and the level of attack was increased, the performance level was not good.
6.	Song Y. et al.(2010)	Presented a relational database robust watermarking algorithm that was based on DCT transform and took the advantage of the frequency domain approach of the multimedia digital watermarking into the relational database watermarking. By the DCT transform on grouped and sorted tuples and modified some of the transformed frequency coefficients to the embed image watermark, only the affecting one attribute of every tuple, the algorithm had good watermarking invisibility and small errors had caused for data.	The general mapping relationship between image watermarking and relational data watermarking in image watermarking into database was weak.
7.	Hossein M. et al. (2010)	Presented a resilient watermarking scheme for the relational database that embeds image bits in small size database as watermark. Experimental results showed that it was robust to the important attacks and the comparison proposed technique with the previously posed methods showed the superiority of this technique to the modification attack.	The general subset attacks like insertion, deletion and modification attacks was not addressed in the proposed method for embedding watermark bits uniformly in relational database and also in evaluating method
8.	Jung-Nan C. et al.(2012)	Proposed a reversible fragile watermark algorithm which was based on SVR prediction that used the FP-free data mining method. The proposed scheme could also used to verify the contents of database.	All the tampered data could not be successfully detected and located also
9.	Udai P. R. et al.(2012)	Proposed an effective process for the database watermarking in which a proper tuple in the database was chosen for marking and then the chosen bits of the image replaced some bits of the opted attributes of the particular tuple.	The technique used only the numeric attributes for marking purpose.
10.	Kamran M. et al.(2013)	Proposed a technique which was highly resilient against the insertion, deletion, modification and multifaceted attack yet that results in the minimum distortions in original dataset. Regardless of the malicious attack on the	The proposed technique was restricted to the numeric unsigned data only.

		watermarked data, watermark bits were successfully decoded with accuracy because decoding accuracy of proposed approach was independent of usability constraints.	
11.	Javier F. C. et al.(2014)	Proposed the robust lossless relational database watermarking technique that made the use of circular histogram modulation. It could be used for verifying the integrity of database and also for verifying the authenticity even if the database had been modified. They had theoretically established and also verified experimentally the performance of the method in terms of the capacity and robustness against the common two attacks: tuple deletion and tuple insertion.	In the selection of parameters there were some constraints of capacity, robustness and distortion was present.
12.	Rohit T. et al.(2015)	A new fragile biometric watermarking process was proposed in the hybrid domain using the Compressive Sensing theory framework.	This process was not robust against median filtering, JPEG compression, and noise addition like salt & pepper noise, Gaussian noise, and speckle noise, cropping attacks and histogram equalization.

7. CONCLUSION

Previously, lot of work has been done for the better performance of the already existing database watermarking methods. But our paper compared the different types of database watermarking method along with the motivations and limitations. Future scope may include the comparison and betterment of various database watermarking techniques like blind, non-blind, reversible, non-reversible etc. Also using the larger dataset may lead to the better performance, which can be used also in the near future for further studies.

REFERENCES

[1] A. Adelsbach, A. Sadeghi "Zero-knowledge watermark detection." In: Proceedings of 4th Int. Workshop on In. Hiding, 2001, 2137: 273-288.

[2] S. Roy,E. Chang "Watermarking with Knowledge of Image Database." In: Proceedings 2003 International Conference, 2003, 3:471-475.

[3] M. H. Tsai, F. Y. Hsu,J. D. Chang,H. C. Wu "Fragile Database Watermarking for Malicious Tamper Detection Using Support Vector Regression". In: Proceedings of Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP), 2007, 493- 496.

[4] K. Huang, M. Yue, P. Chen, Y. He, X. Chen "A Cluster-Based Watermarking Technique for Relational Database". In: Proceedings of Database Technology and Applications- First International Workshop, 2009, 107-110.

[5] C. Jiang, X. Chen, Z. Li "Watermarking Relational Databases for Ownership Protection Based on DWT". In: Proceedings of Fifth International Conference on Information Assurance and Security, 2009, 1:305-308.

[6] M. E. Farfoura, S.J. Horng "A Novel Blind Reversible Method for Watermarking Relational Databases". In: Proceedings of Parallel and Distributed Processing with Applications (ISPA), 2010,563 – 569.

[7] S. Yige, L. Weidong, S. Jiaxing, W.M.S. Angela "DCT Transform Based Relational Database Robust Watermarking Algorithm". In: Proceedings of W.M.S. Data, Privacy and E-Commerce (ISDPE), 2010, 61-65.

[8] H. M. Sardroudi, S. Ibrahim "A new approach for relational database watermarking using image". In: Proceedings of Computer Sciences and Convergence Information Technology (ICCIT), 2010, 606-610.

[9] J. N. Chang, H. C. Wu "Reversible Fragile Database Watermarking Technology using Difference Expansion Based on SVR Prediction". In: Proceedings of Computer, Consumer and Control (IS3C), 2012, 690-693.

[10] U. P. Rao, D. R. Patel, P. M. Vikani "Relational Database Watermarking for Ownership Protection". In: Proceedings of 2nd International Conference on Communication, Computing & Security, 2012, 988-995

[11] M. Kamran, S. Suhail, M. Farooq "A robust, distortion minimizing technique for watermarking relational databasesusing once-for-all usability constraints". IEEE Transactions on Knowledge and Data Engineering, 2013, 25(12): 264-270.

[12] J. Franco-Contreras, G. Coatrieux, F. Cuppens, N. Cuppens-Boulahia, C. Roux "Robust Lossless Watermarking of Relational Databases Based on Circular Histogram Modulation". IEEE Transactions on Information Forensics and Security, 2014, 9(3):397-410.

[13] R. Thanki, K. Borisagar "Multibiometric Template Security Using CS Theory–SVD Based Fragile Watermarking Technique". In: Proceedings of WSEAS TRANSACTIONS on INFORMATION SCIENCE and APPLICATIONS, 2015.

[14] V. Vapnik "The Nature of Statistical Learning Theory", Springer-Verlag, New York, 1995.

[15] V. Vapnik "Statistical Learning Theory", John Wiley, New York, 1998.

[16] H. C. Wu., S. Y. Shih, Y. H Lai. "A Dual Database Watermarking Scheme for Malicious Tampering Detection and Copyright Protection". GESTS International Transactions on Computer Science and Engineering, 2006, 34(1): 151-163.

[17] H. H. Tsai, D. W. Sun "Color Image Watermark Extraction Based on Support Vector Machines". In: Proceedings of Information Sciences, 2007, 177(2): 550-569.

[18] X. Yue "The Research on the Relational Database Watermarking Based on the Virtual Primary Key". Hunan, China: Graduate School of Computer Science and Technology of Hunan University.

[19] N. Dey, S. Biswas, A. B. Roy, A. Das, S. S. Chaudhuri "Analysis Of Photoplethysmographic Signals Modified by Reversible Watermarking Technique using Prediction-Error in Wireless Telecardiology". In: Proceedings of International Conference of Intelligent Infrastructure , 47th Annual National Convention of CSI –Kol, 01 - 02 December 2012 , McGraw-Hill Proceeding.

[20] N. Dey, P. Das, A. Das, S. S. Chaudhuri "DWT-DCT-SVD Based Intravascular Ultrasound Video Watermarking". In: Proceedings of Second World Congress on Information and Communication Technologies (WICT 2012), Trivandrum, India: October 30-November 02, 2012.

[21] N. Dey, S. Biswas, P. Das, A. Das, S. S. Chaudhuri "Lifting Wavelet Transformation Based Blind Watermarking Technique of Photoplethysmographic Signals in Wireless Telecardiology". In: Proceedings of Second World Congress on Information and Communication Technologies (WICT 2012), Trivandrum, India: October 30-November 02, 2012.

[22] N. Dey, S. Samanta, X-S. Yang, S. S. Chaudhri, A. Das "Optimisation of Scaling Factors in Electrocardiogram Signal Watermarking using Cuckoo Search". In: Proceedings of International Journal of Bio-Inspired Computation (IJBIC), 2013, 5(5): 315-326.

[23] N. Dey, P. Maji, P. Das, A. Das, S. S. Chaudhuri. "An Edge Based Watermarking Technique of Medical Images without Devalorizing Diagnostic Parameters". In: Proceedings of International Conference on Advances in technology and Engineering, NMIMS University, Mumbai, India , January 23-25, 2013.

[24] A. K. Pal, N. Dey, A. Mukherjee, S. Samanta, S. S. Chaudhuri. " A Hybrid Reversible Watermarking Technique for Color Biomedical Images". In: Proceedings of IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Madurai, Dec 26-28, 2013.

[25] S. Chakraborty, P. Maji, A. K. Pal, D. Biswas, N. Dey. "Reversible Color Image Watermarking using Trigonometric Functions". In: Proceedings of International Conference on Electronic Systems, Signal Processing and Computing Technologies, Nagpur, 09-11 January, 2014.

[26] S. Banerjee, S. Chakraborty, A. K. Pal, N. Dey, R. Ray. "High Payload Watermarking using Residue Number System". In: Proceedings of International Journal of Image, Graphics and Signal Processing (IJIGSP). MECS-press, China, 2015, 7(3):1-8.

[27] N. Dey, S. Chakraborty, S. Samanta. "Optimization Of Watermarking in Biomedical Signal". Lambert Publication, Heinrich-Böcking-Straße 6, 66121 Saarbrücken, Germany.

[28] N. Dey, B. Nandi, P. Das, A. Das, S. S. Chaudhuri. "Retention Of Electrocardiogram Features Insignificantly Devalorized As An Effect Of Watermarking For A Multi-Modal Biometric Authentication System". Published by Advances in Biometrics for Secure Human Authentication and Recognition, 2013, 450, July 2013.

[29] N. Dey, P. Maji, P. Das, S. Biswas, A. Das, S. S. Chaudhuri "Embedding of Blink Frequency in Electrooculography Signal using Difference Expansion based Reversible Watermarking Technique". Seria, Electronics and Communications.

[30] N. Dey, S. Mukhopadhyay, A. Das, S. S. Chaudhuri "Using DWT analysis of P, QRS and T Components and Cardiac Output Modified by Blind Watermarking Technique within the Electrocardiogram Signal for Authentication in the Wireless Telecardiology". In: Proceedings of I.J. Image, Graphics and Signal Processing (IJIGSP), 2012, 7, 33-46.

[31] N. Dey, M. Pal, A. Das "A Session Based Watermarking technique Within the NROI of Retinal Fundus Images for Authencation Using DWT,Spread Spectrum and Harris Corner Detection". In: Proceedings of International Journal of Modern Engineering Research, 2012, 2(3): 749-757.

[32] N. Dey, G. Mishra, B. Nandi, M. Pal, A. Das, S. S. Chaudhuri "Wavelet Based Watermarked Normal and Abnormal Heart Sound Identification using Spectrogram Analysis". In: Proceedings of IEEE International Conference on Computational Intelligence and Computing Research (ICCIC),Tamilnadu College of Engineering,Coimbatore,India, Dec 18 - 20, 2012.

[33] N. Dey, S. Biswas, P. Das, A. Das, S. S. Chaudhuri "Feature Analysis for the Reversible Watermarked Electrooculography Signal using Low Distortion Prediction-error Expansion". In: Proceedings of International Conference on Communications, Devices and Intelligent Systems (CODIS), Jadavpur University, Dec-28-29, 2012.

[34] S. Acharjee, S. Chakraborty, R. Ray, S. Nath, N. Dey "Watermarking in Motion Vector for Security Enhancement of Medical Videos". In: Proceedings of International Conference on Control, Instrumentation, Communication and Computational Technologies, 10-11 July 2014.

[35] S. R. Chowdhury, S. Chakraborty, W. B. Abdessalem Karaa, R. Ray, N. Dey "Effect of Demons Registration on Biomedical Content Watermarking". In: Proceedings of International Conference on Control, Instrumentation, Communication and Computational Technologies, 10-11 July 2014.

[36] S. Bose, S. R. Chowdhury, S. Chakraborty, S. Madhulika, Nath, N. Dey. "Effect of Watermarking in Vector Quantization based Image compression". In: Proceedings of International Conference on Control, Instrumentation, Communication and Computational Technologies, 10-11 July 2014.