ISSN: 2348 - 2117

International Journal of Engineering Technology and Computer Research (IJETCR)
Available Online at www.ijetcr.org
Volume 4; Issue 3; May-June-2016; Page No. 12-16

SECURING SECRET DATA USING WATERMARKING TECHNIQUE WITH GENETIC ALGORITHM AND ATTRIBUTE-BASED ENCRYPTION TECHNIQUE

G.Nithyavani[1], P.Rajesh. M.E.[2]

PG Student, Computer Science and Engineering, Kingston Engineering College, Vellore, India

smileynithya.04@gmail.com

Assistant Professor, Computer Science and Engineering, Kingston Engineering College, Vellore, India

rajesh.p@gmail.com

Abstract

This paper presents a parsimonious model that builds on technology acceptance research and insights from criminology to identify factors that reduce Internet users' intended to use online services. We hypothesize that avoidance of online banking, online shopping and online social networking is increased by cybercrime victimization and media reports. The effects are mediated by the perceived risk of cybercrime and moderated by the user's confidence online. We test our hypotheses using a structural equation modeling analysis of a representative pan-European sample. Our empirical results confirm the negative impact of perceived risk of cybercrime on the use of all three online service categories and support the role of cybercrime experience as an antecedent of perceived risk of cybercrime. Cybercrime risks are avoided by watermarking technique.

***Index terms*:** cybercrime, structural equation model,_ RRW, PEEW, DEW, GADEW, non numerical data.

I. INTRODUCTION:

Watermarking is advocated to enforce ownership rights over shared relational data and for providing a means for tackling data tampering. When ownership rights are enforced using watermarking, the underlying data undergoes certain modifications; as a result of which, the data quality gets compromised. Reversible watermarking is employed to ensure data quality along-with data recovery. However, such techniques are usually not robust against malicious attacks and do not provide any mechanism to selectively watermark a particular attribute by taking into account its role in knowledge discovery. Therefore, reversible watermarking is required that ensures; (i) watermark encoding and decoding by accounting for the role of all the features in knowledge discovery; and, (ii) original data recovery in the presence of active malicious attacks. In this paper, a robust and semi-blind reversible watermarking (RRW) technique for numerical relational data has been proposed that addresses the above objectives.

II. RELATED WORK

G.RoslineNesaKumari et al proposed a good watermarking technique embeds information into a carrier image. In this paper found a novel fact that by inserting the watermark using Least Significant Bit (LSB), the grey value of the image pixel either remains same or increases or decreases to one. The present paper is focused on this issue and found that such ambiguity of grey level values by LSB method comes between successive even and odd grey level values only. The present approach allows high robustness, embedding capacity and enhanced security.

Qing tang Sua,b et al according to the energy concentrating feature of DCT, the two-level DCT is introduced and used to embed color watermark image into color host image, which is completely different with the traditional DCT. For reducing the redundancy of watermark information, the original color watermark image is compressed by the proposed compression method. After two-level DCT, watermarking algorithm can effectively improve the quality of the watermarked image and the robustness of the embedded watermark against various attacks.

E. Gill et al Sequential quadratic programming (SQP) methods have proved highly effective for solving constrained optimization problems with smooth nonlinear functions in the objective and constraints.

Corresponding author: G.Nithyavani

Consider problems with general inequality constraints (linear and nonlinear).W e assume that first derivatives are available and that the constraint gradients are sparse. Second derivatives are assumed to be unavailable or too expensive to calculate.

Aihab Khan et al Fragile zero watermarking scheme to detect and characterize malicious modifications made to a database relation. Most of the existing watermarking schemes for relational databases introduce intentional errors or permanent distortions as marks into the database original content. These distortions inevitably degrade the data quality and data usability as the integrity of a relational database is violated. The proposed fragile scheme is based on zero watermarking approach to detect malicious modifications made to a database relation. In zero watermarking, the watermark is generated (constructed) from the contents of the original data rather than introduction of permanent distortions as marks into the data.

Jean-Baptiste Thomas et al the purpose of this paper is to propose a color image watermarking scheme based on an image dependent color gamut sampling of the L*a*b color space. The main motivation of this work is to control the reproduction of color images on different output devices in order to have the same color feeling, coupling intrinsic information on the image gamut and output device calibration. This paper is focused firstly on the research of an optimal LUT (Look Up Table). This LUT is next embedded in the image as a secret message. The principle of the watermarking scheme is to modify the pixel value of the host image without causing any change neither in image appearance nor on the shape of the image gamut.

Ibrahim Alsonosi Nasir et al the robustness of watermarks to geometric attacks is considered to be the most challenging design requirements for watermarks. Geometric attacks can desynchronize the location of the watermark and hence cause incorrect watermark detection. It is based on embedding multiple watermark bits into the luminance component or the blue component of a color image in discrete wavelet domain. The extraction process does not require the original image.

J. Anitha, S et al Digital watermarking technique has been presented and widely researched to solve some important issues in the digital world, such as copyright protection, copy protection and content authentication. Several robust watermarking schemes based on vector quantization (VQ) have been presented. This present a new digital image watermarking method based on SOFM vector quantizer for color images. This method utilizes the codebook partition technique in which the watermark bit is embedded into the selected VQ encoded block.

Rastislav hovanak et al in recent years, access to multimedia data has become much easier due to the rapid growth of the Internet. While this is usually considered an improvement of everyday life, it also makes unauthorized copying and distributing of multimedia data much easier, therefore presenting a challenge in the field of copyright protection. In this paper four original watermarking schemes based on DCT and DWT transformation for ownership verification and authentication of color images were proposed.

Aishwarya.C et al the main aim of this project is to maintain the ownership of Relational Database and also minimizing distortion in the watermarked content. Reversible watermarking is employed to ensure data quality along-with data recovery. Therefore, reversible watermarking is required that ensures watermark encoding and decoding by accounting for the role of all the features in knowledge discovery and original data recovery.

Dr.Yogendra Kumar Jain et al this paper, proposed an improved & logistic digital watermarking scheme, which collected based on Support Vector Machine (SVM) for color image. The watermark is embedded into the discrete wavelet domain of the original image and extracted by training support vector machine, which have the component of the image. For performance enhancement of support vector machine, we consider the adding of momentum coefficient to reduce the error and increase the rate of the learning. The watermark can be successfully extracted by training the support vector machine, and the (SVM) watermarking algorithm is good for many kinds of common attacks. The experimental results reveal that the proposed algorithm can achieve the desired result and high stoutness to

general image processing technique & geometric distortion.

III. GENETIC ALGORITHM

Genetic Algorithm is a type of public-key encryption in which the secret key of a user and the cipher text are dependent upon attributes (e.g. the country he lives, or the kind of subscription he has). In such a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text. A crucial security feature of Attribute-Based Encryption is collusion-resistance: An adversary that holds multiple keys should only be able to access data if at least one individual key grants access.

nP – base population size
nG -- number of generations
rC – rate of crossover
rM – rate of Mutation
Generate initial population or size nP
Evaluate initial population according to fitness criteria
WHILE(current generation< nG)
{
Breed rC*nP new solutions:
Select two parent solutions from current population from child solutions from current population
if(random range (0.0, 1.0) < rM)
Mutate the child solution
Evaluate the child solution according to ritness criteria
Add child to population
remove the Rc * nP least-rit solution from the population
}
return (most fit member of population)

A. PSUEDOCODE FOR GENETIC ALGORITHM

Choose an initial random population of individuals
Evaluate the fitness of the individuals
Repeat
Select the best individuals to be used by the genetic operators
Generate new individuals using crossover and mutation
Evaluate the fitness of the new individuals
Replace the worst individuals of the population by the best new individuals
Until some stop criteria

IV ATTRIBUTE-BASED ENCRYPTION TECHNIQUE

In ABE user private key and ciphertext are associated with set of attributes. Decryption of ciphertext by user is possible only when at least threshold number of attributes overlap between user private key and ciphertext. Different from traditional PKC IBE, ABE is intended for one - many encryption means, ciphertext is not necessarily encrypted to one particular user. To get more general access control, variant of ABE that is Key- Policy-ABE (KP-ABE). In this variant, ciphertext is associated with set of attributes and each user secret key is embedded in access structure. Because of this user can decrypt a ciphertext only if ciphertext attribute satisfy access structure embedded in his private key. Ciphertext-Policy ABE (CP-ABE). CP-ABE is reverse way of KP-ABE. This means ciphertext is associated with access structure and user secret key is embedded in set of attributes. Formally KP-ABE and CP-ABE can be defined as below.

A. Key-Policy Attribute-Based Encryption(KP-ABE)

KP-ABE algorithm Setup takes as an input security parameter k, and returns public key PK which is used for encryption by sender and secret master key MK which is used by TA to generate user secret keys.
KP-ABE algorithm Encryption takes as inputs message M, public key PK, set of attributes γ and outputs ciphertext
KP-ABE algorithm Key Generation takes as input access structure T and MK. It outputs secret key SK that enables users to decrypt to a message encrypted under set of attributes γ if and only if γ matches T.
KP-ABE algorithm Decryption takes as input SK for T & E which was encrypted under γ and it outputs 'M' if and only if γ satisfies user's structure T.

B. Cipher text-Policy Attribute-Based Encryption(CP-ABE)

CP-ABE algorithm Setup takes as an input security parameter k, and returns public key PK which is used for encryption by sender and secret master key MK which is used by TA to generate user secret keys.
CP-ABE algorithm Encrypt takes as input PK, M & T; and outputs cipher text CT.
CP-ABE algorithm Key Generation takes as an input γ associated with user & MK. It outputs SK used to

decrypt message encrypted under T if and only if γ matches T.

CP-ABE algorithm Decrypt takes as input CT`, SK for γ. It outputs M if and only if γ satisfies access structure associated with CT. Beside primitive functionalities for ABE, many works have been proposed to provide better privacy protection for ABE which includes ABE with user accountability, ABE with attribute hierarchy, CP-ABE with hidden policy.

Pseudocode For Attribute-Based Encryption
Extract the sequence number from the packet
Extract the offset and mask of the history vector
If offset is zero then no history
Else
{
substract offset from the sequence number to give first packet in history
while the mask !=0
{
subtract one from sequence number
if low bit is set in mask then add packet to history
Shift mask to the right one bit
}
}
Decompress packet
Extract acknowledgement vector and the sequence number of most recently received
Packet and bit mask

V CONCLUSION

The proposed approach is to secure the video data hiding based using Bit stream level data hiding and selective embedding. The is divided into frames and the secret data is embedded within the video frames that will provide a secure location for data hiding. Secret data embedding is performed using DWT and the data is hidden in one of the high frequency sub band of DWT by tracing pixels in that sub band. The embedding is done by entropy encoder using Huffman encoding that has unique prefix code. Use of ABE algorithm the security is enhanced that is secure data is converted to cipher text and then it will hidden in the frames embed the data into the video. Video and data are separated using decoding technique.

VI ACKNOLEDGMENT

I would like to take this opportunity to express my profound gratitude and deep regard to my guide, *Prof.P.Latha CSE, Kingston Engineering College*, for her exemplary guidance, valuable feedback and constant encouragement in completing this paper. Her valuable suggestions were of immense help in getting this work done. Working under her, was an extremely knowledgeable experience. Also, I would like to extend my sincere gratitude to my parents and my brothers for their constant support and encouragement in completing this paper.

REFERENCES

1. Y.-C. Liu, Y.-T. Ma, H.-S. Zhang, D.-Y. Li, and G.-S. Chen, “A method for trust management in cloud computing: Data coloring by cloud watermarking,” Int. J. Autom. Comput., vol. 8, no. 3, pp. 280–285, 2011.
2. (2012, Feb. 4).Walmart to start sharing its sales data. [Online]. Available: http://nypost.com/ p/news/business/walmart-opens-up
3. (2013, Apr. 11). Identity theft watch. [Online]. Available: http:// scambook.com/blog/2013/ 04/ identity-theft-watch-customerpasswords-stolen-from-walmart-vudu-video-service/
4. (2013, Feb. 26). Securing outsourced consumer data. [Online]. Available: http://databreaches. net /securing-outsourced-consumer-data/
5. (2012, Jun. 3). As patients’ records go digital, theft and hacking problems grow.
6. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, “Secure spread spectrum watermarking for multimedia,” IEEE Trans. Image Process., vol. 6, no. 12, pp. 1673–1687, Dec. 1997.
7. Cox, M. Miller, J. Bloom, and M. Miller, Digital Watermarking. Burlington, MA, USA: Morgan Kaufmann, 2001.
8. P. W. Wong, “A public key watermark for image verification and authentication,” in Proc. IEEE Int. Conf. Image Process., 1998, vol. 1, pp. 455–459.
9. P. W. Wong and N. Memon, “Secret and public key image watermarking schemes for image authentication and ownership verification,” IEEE Trans. Image Process., vol. 10, no. 10, pp. 1593–1601, Oct. 2001.

10. F. A. Petitcolas, "Watermarking schemes evaluation," IEEE Signal Process. Mag., vol. 17, no. 5, pp. 58–64, Sep. 2000.

11. J. T. Brassil, S. Low, and N. F. Maxemchuk, "Copyright protection for the electronic distribution of text documents," Proc. IEEE, vol. 87, no. 7, pp. 1181–1196, Jul. 1999.

12. R. Agrawal and J. Kiernan, "Watermarking relational databases," in Proc. 28th Int. Conf. Very Large Data Bases, 2002, pp. 155–166.

13. R. Sion, M. Atallah, and S. Prabhakar, "Rights protection for categorical data," IEEE Trans. Knowl. Data Eng., vol. 17, no. 7, pp. 912– 926, Jul. 2005.

14. S. Subramanya and B. K. Yi, "Digital rights management," IEEE Potentials, vol. 25, no. 2, pp. 31–34, Mar.-Apr. 2006.

15. P. E. Gill, W. Murray, and M. A. Saunders, "Snopt: A sqp algorithm for large-scale constrained optimization," SIAM Rev., vol. 47, no. 1, pp. 99–131, 2005.

16. K. E. Parsopoulos and M. N. Vrahatis, "Particle swarm optimization method for constrained optimization problems," Intel. Technol.–Theory Appl. New Trends Intell. Technol., vol. 76, pp. 214– 220, 2002.

17. R. Hassan, B. Cohanim, O. De Weck, and G. Venter, "A comparison of particle swarm optimization and the genetic algorithm," in Proc. 46th AIAA/ASME/ASCE/AHS/ASC Struct., Struct. Dyn. Mater. Conf., 2005, pp. 1–13.