Int. J. of Advanced Networking and Applications
Volume:01, Issue: 06, Pages:367-370 (2010)

Data Hiding and Water Marking Security based on nested lattices

V.S Giridhar Akula
Principal, Hasvita Institute of Engineering and Technology, Hyderabad, India
Email: akulagiri2002@yahoo.com
P ChndraSekhar Reddy
Professor Coordinator, Jawaharlal Nehru Technological University, Hyderabad, India
Email: drpcsreddy@gmail.com
N.KalpaLatha
Lecturer, Sri Padmavati College, Tirupati, India
R.Sivam
Assist Professor, Narasaropet Enineering College, Narasarao Pet, India

----------**ABSTRACT**----------
This paper focuses on the security of data hiding principles based on nested lattices. Security key is used in the embedding process to provide security for different watermarked signals. Lattice partitioning is the concept adopted for data hiding. Self similar lattice construction is used to construct nested lattice codes.

Keywords- Cryptanalysis, ditcher, Embedding and decoding, lattice partitioning, watermarking security.

Date of Submission: 26, February 2010 Revised: 20, April 2010 Date of Acceptance: 13, May 2010

I. INTRODUCTION

It has become a difficult task in brining the water marking schemes in the recent days. This leads to a good scope to researchers to concentrate on watermarking security principles [1]. All the parameters of watermarking schemes are treated as public. As in cryptanalysis, the development of practical attacks for finding security keys should be treated as the main concept of security analysis. If the intruder manages to accurately estimate the secret key, then the intruder has total access to the watermarking channel for encoding and decoding the hidden data.

In this paper we have concentrated on nested lattice codes [2], which have the connection between latest results on lattice encoding and decoding and Costa's result [3]. This paper measures the data leakage about the key for lattice Distortion Compensation-Dither Modulation (DC-DM) schemes[4]. DC-DM is a particular implementation of quantization index modulation [5]. The embedding lattices are formed by the Cartesian product of identical scalar quantizers and hence embedding can be designed in a component-by-component basis. This paper explains the mathematical model for lattice data hiding and the lattice construction.

II. MATERIALS & METHODS

Cayre, Fontaine and Furon have proposed Watermarking only attack scenario(WOA) in IEEE transactions and it states that the attacker no loner knows anything about the embedded messages. Comesana, Freire and Gonzalez have explained the fundamental concepts of data hiding security using spread spectrum analysis. Freire, Gonzalez, Furon and Comesana have analyzed the security of lattice based data hiding, but it is mainly restricted to the known message attacks, where the messages embedded in each watermarked signal were assumed to be known by the intruder. This paper measures the information leakage about the DC-DM key, keeping attention in the comparison between Known Message Attack and Watermarked only attack.

This paper exploits and used the concepts like lattices, lattice codes and dithers in encoding and decoding concepts.

Lattice:

A lattice is defined as a discrete subgroup with the natural addition operation. Similarly a lattice of n-dimensional space can be generated by integer mixing of a set of n linearly independent basis vectors. This procedure forms the generating matrix.

Lattices are mainly used to hide the data with the concept of lattice partitioning. The set of all co sets of sub lattice

Volume:01, Issue: 06, Pages:367-370 (2010)

with respect to lattice is called is called the partition of lattice [6]. This paper also uses encoding and decoding principles of encoding and decoding in secret dither concepts. Secret dither algorithm is explained with three important steps to estimate dithers**.**

III.NESTED CODE CONSTRUCTION

A nested code is explained by two parameters, namely coarse lattice and a finite lattice. The process of self similar construction is used here to construct nested code as follows.

Step 1: Define a positive integer I which belongs to N.
Step 2: Compute the finite lattice with an embedding rate R= log(I)/n, where n is the dimensionality of the lattice.
Step 3: Obtain the set of co set leaders.

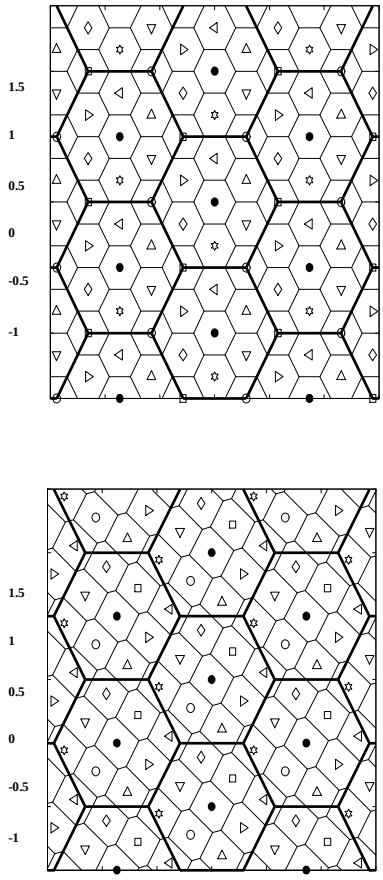

Fig 1: Nested lattices codes with shaping lattice obtained hexagonal by means of self similar construction procedure.

IV.ENCODING AND DECODING

In the lattice data hiding principle [7] , the host signal is partitioned into non overlapping blocks of length n. the message to be encoded should undergo channel coding. We use a parameter X which is a n dimensional vector, named as secret dither and is used to randomize the encoding and decoding functions. This vector plays a role as secret key. In DC-DM lattice scheme, each letter is encoded in one block by means of randomized lattice quantizer. The embedding function is implemented by a dithered lattice quantizer.

The widely used decoders are named as lattice decoders in which the encoding message is approximated by selecting the co set which is very close to the attacked vector. The decoder needs the correct realization of X for successful performance.

As shown in fig 2, using the shaping lattice , the coset is obtained and then the block X is quantized to the nearest point and the resulting quantization error is computed. At the end the quantization error is scaled by the distortion compensation parameter and added back to block X in order to obtain the watermarked block Y.

Volume:01, Issue: 06, Pages:367-370 (2010)

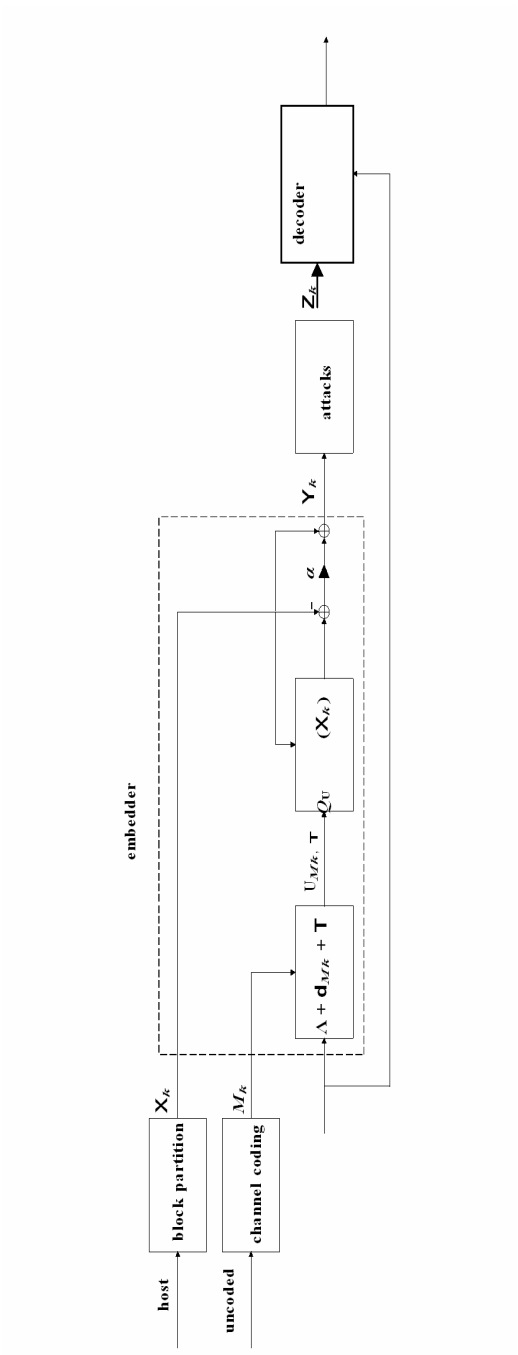

Fig 2 Block diagram showing the lattice data hiding model. Parameter T is the secret dither.

V. SECRET DITHER ESTIMATION ALGORITHM

The beam search strategy [8] will be applied at the time of tree search and the proposed dither estimation procedure is explained below.

Step 1: Initialize the number of feasible paths for the first observation.

Step 2:

(a) Construct a set of candidate paths
(b) Compute the ellipsoids
(c) Compute the score of each path . Arrange all these paths in the descending score and compute beam factors surviving paths.

Step 3: Compute p paths belonging to the equivalence class.

VI. RESULTS

The results are analyzed on lattice DC-DM schemes. It is assumed that the host signal follow a Gaussian distribution with zero mean and variance. It is also assumed that the message passed by the first observation corresponds to the symbol 0. This assumption is to assess the performance of the dither estimator without ambiguities. The trade off complexity accuracy and estimation errors are represented with the following graphs. An accurate dither estimate allows to implement a number of harmful attacks also.

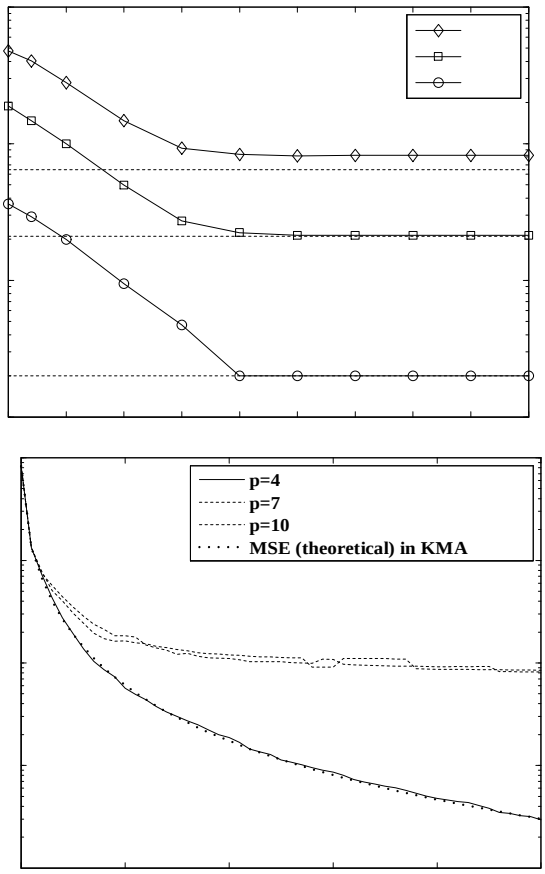

Fig 3: Results showing MSE for p=4, p-7 and p=10.

VII. CONCLUSION

This paper explained the security provided by data hiding schemes. These schemes are based on nested lattice codes randomized by means of secret dithering. Through these concepts the security level of many practical scenarios is fairly low. Security risks are minimized by reusing the secret key for few times. The encoding parameters used in this paper will maximize the security.

VIII. ACKNOWLEDEMENTS

It is our privilege to express our gratitude to the people who have involved in completing this work either directly or indirectly. Firstly we would like express our special thanks to Dr K Soundararajan, Rector, JNTU, Anatapur and our beloved guru Padmasri Dr V Rajaraman, Hon Professor, IISc, Bangalore, who has helped us with their constant support to complete the work. Also we would like to thank Mr Naendra Kumar and Mr Sasidhar, Sr Software engineers at Rapdigm, USA for helping us technically for analyzing results. At the end it is our duty to mention thanks to our friend Dr P Subbaiah, Kadapa.

REFERENCES

[1]. F Cayre, C Fontaine et al,. "watermarking security: theory and practices", IEEE Traans. Signal Processing, vol 53, no.10, oct 2005.
[2]. P.Moulin and R Koetter, "Data hiding codes," proceedings of IEEE, vol 93, no 12, pp.2083-2126, December 2005.
[3]. M H M Costa, " Writing on dirty paper," IEEE Transactions on Information theory, vol 29, no 3, pp 439-441,May 1983.
[4]. P Comesana, F Perez-Gonzalez and F Balado, " On Distortion-compensated dither modulation data-hiding with repetition coding." IEEE Transactions on Signal Processing, vol 54, no 2, pp 585-600, February 2006.
[5]. B Chen and G Wornell, " Quantization Index Modulation"; a class of probably good methods for digital watermarking and information embedding", IEEE Transactions on Information Theory, Vol 47, pp 1423-1443, May 2001.
[6]. U Erez, S Litsyn and R Zamir, " Lattices which are good for(almost) everything", IEEE Transactions on Information Theory, vol 51, no 10, pp 3401-3416, October 2005.
[7]. J H Conway and N J A Sloane, sphere packings, lattices and groups, 3rd ed., ser. Comprehensive Studies in Mathematics. New York: Springer-Verlag.1999, vol 290.
[8]. X Huang, A Acero and H W Hon, Spoken Language Processing: A guide to Theory, Algorithm and system Development. Prentice Hall 2001.

Authors Biography

Dr P Chandra Sekhar Reddy is presently working as the Professor coordinator at Jawaharlal Nehru Technological University, Hyderabad. He has rich teaching experience and worked in various designations at JNTU, Anantapur and JNTU Hyderabad. Worked as the HOD for CSE and ECE departments at JNTUA, Dr Reddy is an author for text books and published technical papers in many National and International Conferences and Journals. Two people have completed their research under his guidance and 10 more research scholars are working under his stewardship. His areas of interest are Computer Networks, Digital Image Processing, Mobile Computing etc.,

Prof V S Giridhar. Akula is presently working as the principal at Hasvita Institute of engineering and technology, Hyderabad. He has total 17 years of teaching experience (as HOD-CSE and Principal at various engineering colleges) and is also an author for 5 text books and many of his technical papers were published in National and International Journals and Conferences.

N KalpaLatha is working as the Librarian at Padmavati College, Tirupati and she is writing papers in Library sciences based on Computer networks.

R Sivam is presently working as an assistant professor at Narasarao Pet engineering College, Narasarao Pet, India