ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol. 3 , No.1, Pages : 542– 545 (2014)
Special Issue of ICETETS 2014 - Held on 24-25 February, 2014 in Malla Reddy Institute of Engineering and Technology, Secunderabad– 14, AP, India

Hiding data of Digital Images using Lattices

M PurnaChandra Rao [1] M Siva Prasad Reddy [2] .K Rajesh Kumar Reddy[3]
[1]Assistant Professor, Priyadarshini Engineering College, Tirupati
[2]Assistant Professor, Priyadarshini Engineering College, Tirupati, sivaprasad484@gmail.com
[3] Assistant Professor, Kuppam Engineering College, Kuppam, rajeshk535@gmail.com

Abstract:

The main goal of the paper is to exploit the security of data hiding principles with the help of 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:

watermarking security, Embedding and decoding, Cryptanalysis, ditcher, watermarking channels, lattice partitioning, nested lattice codes, dither estimate.

Introduction:

Watermarking principles are plying very significant role in the recent days**.** It has become a difficult task in bringing the design of watermarking schemes in the recent days. This leads a good scope to researchers to concentrate on watermarking security [1]. All the parameters of the 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 & decoding and Costa's result[3]. This paper measures the data leakage about the key for lattice Distortion compensation-Dither modulation (DC-DM) schemes [8]. DC-DM is a particular implementation of Quantization Index modulation [4]. The embedding lattices are formed by the Cartesian product of identical scalar quantizers, 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.

Materials and Methods Used:

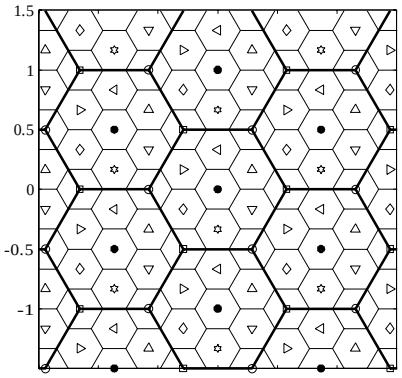
This paper exploits and used the concepts like lattices, lattice codes and dithers in encoding and decoding concepts.

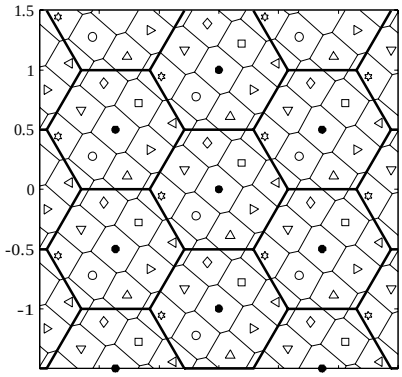
Lattice:

A lattice is defined as a discrete subgroup with the natural addition operation**.**

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol. 3 , No.1, Pages : 542– 545 (2014)
Special Issue of ICETETS 2014 - Held on 24-25 February, 2014 in Malla Reddy Institute of Engineering and Technology, Secunderabad– 14, AP, India





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 with respect to lattice is called is called the partition of lattice[5].

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.

1. 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.

2. Encoding and Decoding

In the lattice data hiding principle[6] , 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.

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol. 3 , No.1, Pages : 542– 545 (2014)
Special Issue of ICETETS 2014 - Held on 24-25 February, 2014 in Malla Reddy Institute of Engineering and Technology, Secunderabad– 14, AP, India

The beam search strategy[7] 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.

Results

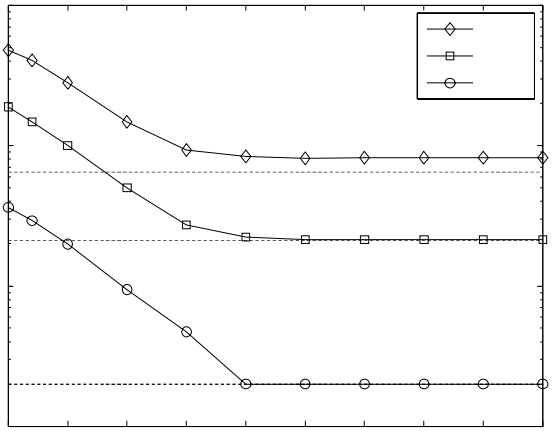
The results are analyzed on lattice DC-DM schemes. It is assumed that the host signal follow a Gaussian distribution with zero mean and variance. It is also assumed that the message passed by the first observation corresponds to the symbol 0. This assumption is to assess the performance of the dither 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.

An early form of data hiding for grayscale images is based on LSB embedding techniques., We will see that these schemes may be interpreted as rudimentary binning schemes.

The method is applicable to host signals of the form , where each sample is encoded using bits representing the natural binary decomposition of an integer between zero and 2 1. For instance, could represent one of the 256 intensity levels of a monochrome image, such as 69 01 000 101 ; the LSB is one in this case. The LSB plane is the length- binary sequence made of all the LSBs. The LSBs can be changed without adversely affecting signal quality, and so LSB embedding methods simply replace the LSB plane with an information sequence; the information rate is 1 bit per sample of .

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol. 3 , No.1, Pages : 542– 545 (2014)
Special Issue of ICETETS 2014 - Held on 24-25 February, 2014 in Malla Reddy Institute of Engineering and Technology, Secunderabad– 14, AP, India



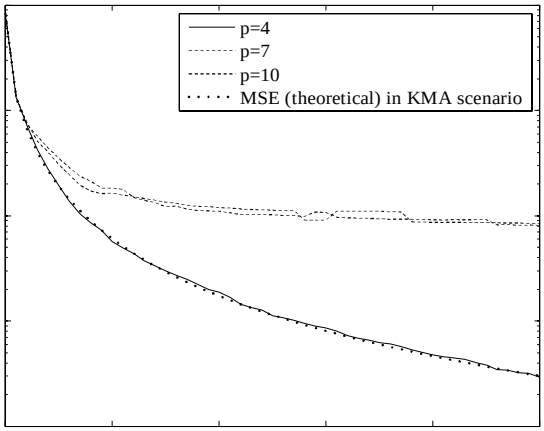


Fig 3: Trade off complexity accuracy and estimation errors.

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.

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] 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.

[5] 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.

[6] 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.

[7] X Huang, A Acero and H W Hon, Spoken Language Processing: A guide to Theory , Algorithm and system Development. Prentice Hall 2001.

[8] 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.