IJRRECS/June 2015/Volume-3/Issue-6/3942-3946 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

AN EFFICIENT PROPOSAL FOR ASSESSMENT OF HIDDEN INFORMATION IN DIGITAL DOMAINS

CH.Manjusha[1], K.Ramesh Babu[2]

[1]M.Tech Student, Dept of CSE, Malla Reddy Engineering College for Women, Hyderabad, T.S, India

[2]Professor, Dept of CSE, Malla Reddy Engineering College for Women, Hyderabad, T.S, India

ABSTRACT:

In recent times, technologies of data embedding are being observed for providing threat towards personal privacy as well as security interests. Several techniques concerning data hiding came into existence. In the past few years, existence of embedded data is investigated in passive detection and active hidden data extraction is a comparatively novel branch of research. In our work, we build up an approach of multi-carrier iterative generalized least squares for extraction of spread spectrum hidden data. We spotlight on blind recovery of hidden secret information within medium hosts by means of multi-carrier or signature direct-sequence spread-spectrum embedding. In blind extraction of spread spectrum embedded information, the unidentified host performs as a source of disturbance to the data that has to be recovered. Multi-carrier iterative generalized least squares might outperform in reasonable to high distortion values of minimum-mean-square error of sample-matrix-inversion in which true carriers are recognized. This is since minimum-mean-square error of sample-matrix-inversion suffers from performance degradation due to minute sample-support alteration. From contradictory data embedding viewpoint, developed algorithm was treated as a means to check security robustness of spread spectrum data hiding schemes.

Keywords: Embedded data, Data hiding, Multi-carrier iterative generalized least squares, Privacy.

1. INTRODUCTION:

Techniques related to data hiding are initially employed in several communication systems like encrypted message, for finding of sender and receiver. One of the significant techniques of data hiding is steganography which differs from cryptography. The objective of steganography is concealing of data from a third party where as aim of cryptography is to construct data unreadable by means of a third party. Embedding algorithm of spread spectrum for blind steganography is on the basis of understanding that host signal performs as a source of interference towards secret message of attention [1]. Such knowledge is constructive for the blind receiver at recovery side to reduce recovery error rate for a specified host signal. In our work, we build up an approach of multi-carrier iterative generalized least squares for extraction of spread spectrum hidden data. From contradictory data embedding viewpoint, developed algorithm was treated as a means to check security robustness of spread spectrum data hiding schemes. Multi-carrier iterative generalized least squares remains the major efficient method to blindly take out hidden messages, although extraction turn out to be more challenging as length of hidden message for every used embedding carrier reduce or number of hidden messages increases [2]. We spotlight on blind recovery of hidden secret information within medium hosts by means of multi-carrier or signature direct-sequence spread-spectrum embedding. No original host or embedding carriers such as signatures or else spreading sequences are identified as fully blind data extraction. This problem of blind hidden data extraction was referred as Watermarked content Only Attack (WOA) within security context of watermarking.

2. METHODOLOGY:

As a common encompassing comment, several applications concerning information hiding, necessitate different acceptable tradeoffs among four essential attributes of data hiding such as: Payload: delivery rate of information; robustness : Resistance of hidden data towards disturbance; transparency: low host distortion in support of concealment function; and security: lack of ability by illegal users to detect communication channel. Several techniques concerning data hiding came into existence. In recent times, technologies of data embedding are being observed for providing

threat towards personal privacy as well as security interests. In the past few years, existence of embedded data is investigated in passive detection and active hidden data extraction is a comparatively novel branch of research. In blind extraction of spread spectrum embedded information, the unidentified host performs as a source of disturbance to the data that has to be recovered [3]. Problem parallels the applications of blind signal separation since they take place in array processing, as well as code-division multiple-access communication Independent component analysis might be utilized to practise hidden data extraction on the other hand ICA-based blind signal separation algorithms are not effectual in correlated signal interference degrade quickly as the dimension of the carrier decreases comparative to message size.

3. INTRODUCTION TO PROPOSED SYSTEM:

We build up an approach of multi-carrier iterative generalized least squares for extraction of spread spectrum hidden data as shown in fig1. For enhanced recovery performance, particularly for minute hidden messages that cause the maximum challenge, a few autonomous M-IGLS re-initializations as well as executions on host leads to concealed data recovery with likelihood of error close to what might be attained with recognized embedding carriers and identified original host autocorrelation matrix [4]. Applications of developed algorithm are, not restricted towards attacking steganographic covert communications by improving secret embedded messages. While the carriers are mutually estimated with embedded information, developed system can moreover be used for entire message removal or else tampering attacks. From contradictory data embedding viewpoint, developed algorithm was treated as a means to check security robustness of spread spectrum data hiding schemes. When the message size is minute, multi-carrier iterative generalized least squares might extremely well converge to unsuitable points. The quality of end convergence point depends greatly on initialization point as well as arbitrary initialization which at initial sight are necessary for mining of blind data extraction that provides minute assurance that iterative system will lead us to suitable and consistent solutions. An encompassing ending over the entire

executed experiments is that multi-carrier iterative generalized least squares remains the major efficient method to blindly take out hidden messages, although extraction turn out to be more challenging as length of hidden message for every used embedding carrier reduce or number of hidden messages increases. It is also significance pointing out that, in these studies, multi-carrier iterative generalized least squares might outperforms in reasonable to high distortion values of minimum-mean-square error of sample-matrix-inversion in which true carriers are recognized. This is since minimum-mean-square error of sample-matrix-inversion suffers from performance degradation due to minute sample-support alteration. While blind data extraction algorithmic expansion was on basis of most common spread spectrum embedding, developed algorithm can moreover be functional to more superior spread spectrum embedding schemes for instance improved spread-spectrum as well as correlation-aware enhanced spread-spectrum [5]. We consider difficulty of blindly extracting unidentified messages hidden within image hosts using multi-carrier/signature spread-spectrum embedding. No original host or embedding carriers are assumed to be accessible. We have introduced a low complication multi-carrier iterative generalized least squares algorithm. The approach of multi-carrier iterative generalized least squares can attain likelihood of error to a certain extent close to what might be attained with recognized embedding signatures as well as recognized original host autocorrelation matrix and reveals itself as an effectual countermeasure to existing spread spectrum data embedding [6].

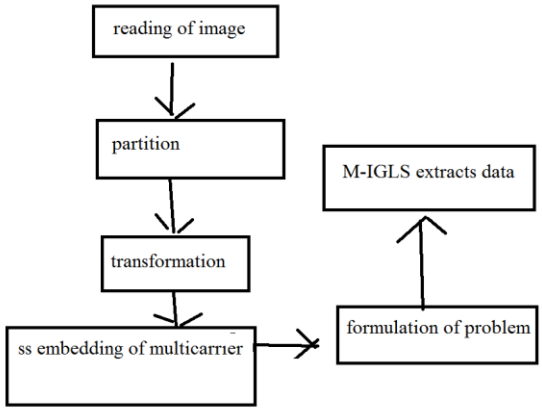

Fig1: An overview to data hiding and extraction

4. CONCLUSION:

Techniques related to data hiding are initially employed in several communication systems like encrypted message, for finding of sender and receiver. In our work, we build up an approach of multi-carrier iterative generalized least squares for

extraction of spread spectrum hidden data. We spotlight on blind recovery of hidden secret information within medium hosts by means of multi-carrier or signature direct-sequence spread-spectrum embedding. Problem of blind hidden data extraction was referred as Watermarked content Only Attack (WOA) within security context of watermarking. Multi-carrier iterative generalized least squares might outperform in reasonable to high distortion values of minimum-mean-square error of sample-matrix-inversion in which true carriers are recognized. The approach of multi-carrier iterative generalized least squares can attain likelihood of error to a certain extent close to what might be attained with recognized embedding signatures as well as recognized original host autocorrelation matrix and reveals itself as an effectual countermeasure to existing spread spectrum data embedding. From contradictory data embedding viewpoint, developed algorithm was treated as a means to check security robustness of spread spectrum data hiding schemes. Multi-carrier iterative generalized least squares remains the major efficient method to blindly take out hidden messages, although extraction turn out to be more challenging as length of hidden message for every used embedding carrier reduce or number of hidden messages increases.

REFERENCES

[1] Y. Wang and P. Moulin, "Perfectly secure steganography: Capacity, error exponents, and code constructions," IEEE Trans. Inform. Theory, vol. 54, pp. 2706-2722, June 2008.

[2] Federal plan for cyber security and information assurance research and development, Interagency Working Group on Cyber Security and Information Assurance, Apr. 2006.

[3] R. Chandramouli, "A mathematical framework for active steganalysis," ACM Multimedia Systems Special Issue on Multimedia Watermarking, vol. 9, pp. 303-311, Sept. 2003.

[4] H. S. Malvar and D. A. Florencio, "Improved spread spectrum: A new modulation technique for robust watermarking," IEEE Trans. Signal Proc., vol. 51, pp. 898-905, Apr. 2003.

[5] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shannon, "Secure spread spectrum watermarking for multimedia," IEEE Trans. Image Proc., vol. 6, pp. 1673-1687, Dec. 1997.

[6] J. Hernandez, M. Amado, and F. Perez-Gonzalez, "DCT -domain watermarking techniques for still images: Detector performance analysis and a new structure," IEEE Trans. Image Proc., vol. 9, pp. 55-68, Jan. 2000.