IJRRECS/March 2016/Volume-4/Issue-3/5302-5306 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

AN ACTIVE PROPOSAL TOWARDS EMBEDDED DATA EXTRACTION IN DIGITAL MEDIUM

K.Ganesh Sai Sudarsan[1], R.V.Kishore Kumar[2]

[1]M.Tech Student, Dept of CSE, Sri Mittapalli College of Engineering, Guntur, A.P, India

[2]Assistant Professor, Dept of CSE, Sri Mittapalli College of Engineering, Guntur, A.P, India

ABSTRACT:

The countermeasure expertise for data hiding technology is commonly referred as steganalysis. In our work we make a consideration of the problem of blind extraction of data that is embedded on wide band in spectrum domain of digital medium such as image, audio and video. A novel multi-signature steganalysis method known as iterative generalized least squares for hidden data extraction was introduced. We build up multi-signature iterative generalized least-squares core process to look for unidentified data which is hidden in hosts by means of multi-signature direct-sequence spread-spectrum embedding. For improving of recovery performance and particularly for minute hidden messages that create maximum challenge, we recommend an algorithmic upgrade known as cross-correlation improved multi-signature iterative generalized least squares method that depends on the statistical analysis of independent executions of multi-signature iterative generalized least squares on the host.

Keywords: Data hiding, Steganalysis, Multi-signature iterative generalized least squares, Spread-spectrum, Hidden message.

1. INTRODUCTION:

Applications regarding the embedding process of digital data will include verification process in its different forms for instance, permanent fragile watermarking form to notice future tampering and so on. Steganography technique helps in establishing of covert communications among trusting parties [1]. The broad idea of steganographic applications is reasonable trade-off among hidden information which

is resistance for noise or disturbance, the rate of information delivery, as well as low host distortion in support of concealment. In our work we introduce a novel multi-signature steganalysis method known as iterative generalized least squares for hidden data extraction. We make a consideration of the problem of blind extraction of data that is embedded on wide band in spectrum domain of digital medium such as image, audio and video [2]. For the improvisation of recovery performance and particularly for minute hidden messages that create maximum challenge, we recommend an algorithmic upgrade known as cross-correlation improved multi-signature iterative generalized least squares method that depends on the statistical analysis of independent executions of multi-signature iterative generalized least squares on the host. Experimental studies reveal hidden data recovery by probability of error which is close to what might be attained with recognized embedding signatures and recognized original host autocorrelation matrix.

2. METHODOLOGY:

Steganalysis technology is classified as passive as well as active categories. The major task of passive steganalysis is to make a decision of presence or else absence of concealed messages in specified media objects. On the contrary active steganalysis describes the effort of extraction of actual hidden information. As passive steganalysis is being investigated within last few years, active steganalysis is comparatively novel branch of research. Neither original host nor embedding signatures are assumed available. We develop multi-signature iterative generalized least-squares core process to look for unidentified data which is hidden in hosts by means of multi-signature direct-sequence spread-spectrum embedding. Gkizeliet al has developed an iterative generalized least squares process to improve unidentified messages concealed within image hosts by means of spread spectrum embedding. The algorithm contains low complexity as well as strong recovery performance on the other hand, the method is considered exclusively for single-signature spread spectrum embedding in which messages are concealed by means of one signature only and is not generalizable towards multi-signature case [3][4]. Practically, a steganographer would support multi-signature spread spectrum embedding to enhance security as well as payload rate.

In our work we consider problem of improving of unknown messages hidden in digital media hosts by means of multi-signature spread-spectrum embedding. Neither original host nor embedding signatures are assumed obtainable. For the improvisation of recovery performance and particularly for minute hidden messages that create maximum challenge, we recommend an algorithmic upgrade known as cross-correlation improved multi-signature iterative generalized least squares method that depends on the statistical analysis of independent executions of multi-signature iterative generalized least squares on the host. The proposed cross-correlation improved multi-signature iterative generalized least squares technique can attain recovery possibility of error close to what might be attained with recognized embedding signatures as well as host autocorrelation matrix. Experimental studies expose hidden data recovery by probability of error which is close to what might be attained with recognized embedding signatures and recognized original host autocorrelation matrix [5]. Cross-correlation improved multi-signature iterative generalized least squares method offers most effectual blind hidden message recovery and provide itself as effectual countermeasure towards conventional spread-spectrum data hiding.

3. AN OVERVIEW OF PROPOSED SYSTEM:

Our work focuses on active spread spectrum steganalysis. Active steganalysis explains the effort of extraction of actual hidden information and it is comparatively novel branch of research. We intend to improve blindly data hidden within hosts by means of direct sequence spread-spectrum embedding. Neither original host nor embedding signatures are recognized. We make a consideration of the problem of blind extraction of data that is embedded on wide band in spectrum domain of digital medium such as image, audio and video. We build up multi-signature iterative generalized least-squares core process to look for unidentified data which is hidden in hosts by means of multi-signature direct-sequence spread-spectrum embedding. In blind active spread-spectrum steganalysis unidentified host acts as basis of interference towards data to be extracted and, in a means, the difficulty parallels blind signal separation applications since they take place in fields of array processing as well as code-division

multiple-access communication systems. Re-initialization as well as re-execution of multi-signature iterative generalized least squares method is constantly promising but challenge is how to consider whether solutions returned by multi-signature iterative generalized least squares method are consistent or not devoid of any side information. A precisely firm and intense measure of quality of active solution of steganalysis is difference within bit-error rate that is experienced by considered recipient as well as steganalyst. For recovery performance and particularly for minute hidden messages that create maximum challenge, we recommend an algorithmic upgrade known as cross-correlation improved multi-signature iterative generalized least squares method that depends on the statistical analysis of independent executions of multi-signature iterative generalized least squares on the host [6]. Hidden data recovery was revealed by probability of error which is close to what might be attained with recognized embedding signatures and recognized original host autocorrelation matrix. The cross-correlation enhanced multi-signature iterative generalized least squares technique can attain recovery possibility of error close to what might be attained with recognized embedding signatures as well as host autocorrelation matrix. In assumption that embedded secret messages are autonomous equally distributed random sequences as well as independent towards cover host, independent component analysis-one particular family of blind signal separation methods possibly utilized to approach the problem of hidden data extraction. On the other hand independent component analysis basis blind signal separation methods will degrade quickly in presence of related signal interference as is precisely case within spread spectrum image or video or else audio embedding.

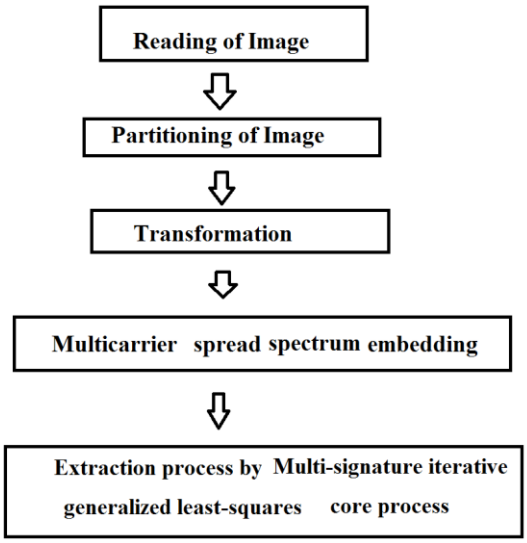

Fig1: Modules for data hiding and extraction

4. CONCLUSION:

Digital data embedding within digital media is an area of information technology of quickly growing commercial, in addition to national security. A novel multi-signature method known as iterative generalized least squares was introduced for hidden data extraction. For improving of recovery performance and particularly for minute hidden messages that create maximum challenge, we recommend an algorithmic upgrade known as cross-correlation improved multi-signature iterative generalized least squares method that depends on the statistical analysis of independent executions of multi-signature iterative generalized least squares on the host. Multi-signature iterative generalized least-squares core process was introduced to look for unidentified data which is hidden in hosts by means of multi-signature direct-sequence spread-spectrum embedding. Here we consider the problem of blind extraction of data that is embedded on wide band in spectrum domain of digital medium such as image, audio and video. Hidden data recovery was revealed by probability of error which is close to what might be attained with recognized embedding signatures and recognized original host autocorrelation matrix. The projected cross-correlation improved multi-signature iterative generalized least squares technique can attain recovery possibility of error close to what might be attained with recognized embedding signatures as well as host autocorrelation matrix. Cross-correlation enhanced multi-signature iterative generalized least squares method offers most effectual blind hidden message recovery and provide itself as effectual countermeasure towards conventional spread-spectrum data hiding.

REFERENCES

[1] C. Cachin, "An information-theoretic model for steganography," in Proc. 2nd Intern. Workshop on Information Hiding, Portland, OR, Apr. 1998, pp. 306-318.

[2] G. J. Simmons, "The prisoner's problem and the subliminal channel," in Advances in Cryptology: Proc. CRYPTO'83. New York, NY: Plenum, 1984, pp. 51-67.

[3] J. Fridrich, Steganography in Digital Media, Principles, Algorithms, and Applications. Combridge, UK: Combridge Univeristy Press, 2010.

[4] 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.

[5] 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.

[6] C. Qiang and T. S. Huang, "An additive approach to transform-domain information hiding and optimum detection structure," IEEE Trans. Multimedia, vol. 3, pp. 273-284, Sept. 2001.