ISSN:2348-2079

Volume-6 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

Multiple Integrity Verification and Auditing Protocol Model for Cloud Computing

[1]Ms. N. Zahira Jahan, M.C.A., M.Phil., Associate Professor/MCA,
[2]Mr. S. Piravin, III MCA,
Department of MCA, Nandha Engineering College (Autonomous), Erode-52.
E-mail Id : zahirajahan1977@gmail.com, 1994piavin@gmail.com

***Abstract*— In this project verifiable outsourcing computation into the area of high-dimensional feature extraction and propose a secure verifiable outsourcing scheme of feature extraction based on co-occurrence matrix with single untrusted server. The original images are secret for the server by using a projection of one to many with trapdoor, and we propose a symmetric probabilistic encryption as its concrete construction. The analyzer can obtain true results of feature extraction and detect any failure with a probability of 1 if the server misbehaves. Finally, provide the simulations on extracting CCJRM features. The proposed outsourcing scheme could greatly decrease the computational cost of the analyzer without exposure of the original images and their extraction results.**

***Index Terms*—Auditing Protocol, Cloudcomputing, Multiple Integrity**

I. INTRODUCTION

In multimedia data processing (data owners) are also highly motivated to outsource their huge amount of data files and computationally expensive tasks onto remote cloud servers by leveraging its abundant resources for cost saving and flexibility.An outsourcing the task of feature extraction directly to a cloud server may cause some security risks: the original images and their true features may be disclosed to the server and the analyzer may be cheated to accept false extraction results by an intentional or unintentional server. The new outsourcing schemes need to be proposed to extract high-dimensional features where the original images and their true features are protected from the server, and the outsourcing results returned by the server could be verified successfully by the analyzer.Various prime numbers are assigned as tags for each segment of file which is stored in server. Each segment is having two prime numbers each of which belongs to a different prime orderan outsourcing the task of feature extraction directly to a cloud server may cause some security risks. The original images and their true features may be disclosed to the server and the analyzer may be cheated to accept false extraction results by an intentional or unintentional server by integrating the HLA with random masking, the protocol guarantees that the TPA could not learn any knowledge about the data content stored in the cloud server during the efficient auditing process.

II. LITERATURE SURVEY

A. ADAPTIVE STEGANALYSIS OF LEAST SIGNIFICANT BIT REPLACEMENT IN GRAYSCALE NATURAL IMAGES

L.Fillatre,in this paper deals with the detection of hidden bits in the Least Significant Bit (LSB) plane of a natural image. The mean level and the covariance matrix of the image, considered as a quantized Gaussian random matrix, are unknown. An adaptive statistical test is designed such that its probability distribution is always independent of the unknown image parameters, while ensuring a high probability of hidden bits detection. This test is based on the likelihood ratio test except that the unknown parameters are replaced by estimates based on a local linear regression model. It is shown that this test maximizes the probability of detection as the image size becomes arbitrarily large and the quantization step vanishes. This provides an asymptotic upper-bound for the detection of hidden bits based on the LSB replacement mechanism. Numerical results on real natural images show the relevance of the method and the sharpness of the asymptotic expression for the probability of detection.

B. A MARKOV PROCESS-BASED APPROACH TO EFFECTIVE ATTACKING JPEG STEGANOGRAPHY

Y. Shi, C. Chen and W. Chen, in this paper, a new steganalysis scheme is presented to effectively detect the advanced JPEG steganography. For this purpose, we first choose to work on JPEG 2-D arrays formed from the

magnitudes of JPEG quantized block DCT coefficients. Difference JPEG 2-D arrays along horizontal, vertical and diagonal directions are then used to enhance changes caused by JPEG steganography. Markov process is applied to modeling these difference JPEG 2-D arrays so as to utilize the second order statistics for steganalysis. In addition to the utilization of difference JPEG 2-D arrays, a thresholding technique is developed to greatly reduce the dimensionality of transition probability matrices, i.e., the dimensionality of feature vectors, thus making the computational complexity of the proposed scheme manageable.

C.JPEG IMAGE STEGANALYSIS UTILIZING BOTH INTRA-BLOCK AND INTER-BLOCK CORRELATIONS

C. Chen, Y. Shi, JPEG image steganalysis has attracted increasing attention recently. In this paper, we present an effective Markov process (MP) based JPEG steganalysis scheme, which utilizes both the intrablock and interblock correlations among JPEG coefficients. We compute transition probability matrix for each difference JPEG 2-D array to utilize the intrablock correlation, and "averaged" transition probability matrices for those difference mode 2-D arrays to utilize the interblock correlation. All the elements of these matrices are used as features for steganalysis. Experimental works over an image database of 7,560 JPEG images have demonstrated that this new approach has greatly improved JPEG steganalysis capability and outperforms the prior arts.

D. STEGANALYSIS OF DCT-EMBEDDING BASED ADAPTIVE STEGANOGRAPHY AND YASS

Q. Liu ,in this paper, we aim to detect the state-of-the-art adaptive steganographic system in DCT-embedding and to improve the steganalysis of YASS. To detect DCT-embedding based adaptive steganography, we design the features of differential neighboring joint density on the absolute array of DCT coefficients between the original JPEG images and the calibrated versions. To discriminate YASS steganograms from covers, the candidate blocks that are possibly used for embedding and the noncandidate block neighbors that are impossibly used for information hiding are identified first. The difference of the neighboring joint density between candidate blocks and the noncandidate neighbors is obtained. Support Vector Machine (SVM) and logistic regression classifiers are employed for classification. Experimental results show that our approach is very promising when detecting DCT-embedding based adaptive steganography. Compared to the steganalysis based on CC-PEV feature set, our method greatly improves the detection accuracy; the advantage is especially noticeable in the detection of the steganograms with low relative payload. In steganalysis of YASS, our approach is superior to a previous well-known steganalysis algorithm; our method remarkably improves the detection accuracy especially in the detection of the YASS steganograms that are produced with a large B-block size, which was not well addressed before.

III.METHODOLOGY

A. AUTHENTICATION FILE SELECTION

In this module, the image file selection is carried out open file dialog control and the image is displayed in picture box control. Then the image data is saved into 'Images' table. During saving, the image data, width and height, image type (RGB) are the information saved. In this module, the image is browsed and added in the database table with 'image' column type. During the user settings, 'n' number of images is selected and the image ids are saved into a transaction table.

C. FEATURE EMBEDDED MODEL

In this module, the image data is taken and encoded so that original image is changed matrix form. The encoded matrix data is obtained as input, the source coding function encodes the contents according to the received input rate and required output rate. In the channel coding part, authentication and watermarking are constructed. First the data is packetized, then encoded, followed by authorization and watermarking. To provide dynamic packet protection for an encoded stream, the most important step is to packet size the stream based on its content priority and difference.The operations of authentication and water-marking can directly relate to the multimedia content since the application packet only depends on the multimedia content. As a result, the importance and priority of the packets can be obtained easily.

C. *FEATURE EXTRACTION MODEL*

At the receiver, sequences of packets are received. Then content detection is performed on the received content to test the integrity of the content. The packet errors are found out and the error report (feedback) from receiver to sender is being sent twice so that even if the first information is attacked, the second copy helps to recognize the error details.Inaddition, the original data is received and data type information is retrieved based on proper decoding. Based on the receiver capability, the Normal/High Definition data is find out. The decoding occurs to get image data which contains original image with watermark data then de-watermarking is carried out, checked and raw image data is displayed if watermark found to be correct.

D. ENCRYPTING THE DCT COEFFICIENTS OF JPEG IMAGES

The analyzer first computes all the differences of DCT coefficients and encrypts the absolute values and differences of DCT coefficients by using the proposed symmetric encryption scheme presented respectively. In order to realize the verifiability of outsourcing results returned by the server, the analyzer needs to separately encrypt the absolute values and differences of DCT coefficients of JPEG images for two times. Finally, the analyzer sends the corresponding four ciphertexts of JPEG images to the server.The analyzer truncates and encrypts the absolute values

of DCT coefficients with the truncation value 5 and obtains C12 two ciphertexts and by using the symmetric encryption scheme.

E. EXTRACTING THE FEATURES OF ENCRYPTED JPEG IMAGES

After receiving the four ciphertexts of a JPEG image, the server first counts the numbers of DCT coefficient pairs in two C12 ciphertexts and about absolute values, and then counts the numbers of DCT coefficient pairs in other two ciphertexts CC 3 4 and about differences. Therefore, the server returns C12 four results of feature extraction about four ciphertexts and to the analyzer.

F. VERIFYING THE RESULTS OF EXTRACTION AND OBTAINING THE PLAINTEXTS OF FEATURES

The analyzer decrypts the four results of feature extraction returned by the server and adds all the results of same DCT coefficient pairs, and then obtains two co-occurrence matrices of high-dimensional features for one JPEG image. The analyzer compares two matrices and accepts the outsourcing results if they are nearly same with small rate of deviation (close to 0); otherwise, it rejects the results. A rate of deviation occurs because that the DCT coefficients larger than 5 (or smaller than -5) will first be changed to 3, 4, 5 (or -3, -4, -5) randomly and then be encrypted during the process of outsourcing.

G. PRIVACY PRESERVING AUDITING PROTOCOL

In this module, the file name is selected, the file content is split into various segments and each segment is given two prime numbers each of which belongs to two prime order. One is given to user, other is given to third party auditor. The combination of the two is kept in server.During auditing, third party auditor randomly picks the segment ids and send corresponding prime number vector to cloud server. If the credentials match, then the file integrity is said to be verified.

E. BATCH AUDITING PROTOCOL

In this module, during auditing, two processes of same Third-party auditor randomly pick the two set of segment ids and send corresponding prime number vectors to cloud server. If the credentials match, then the file integrity is said to be verified.

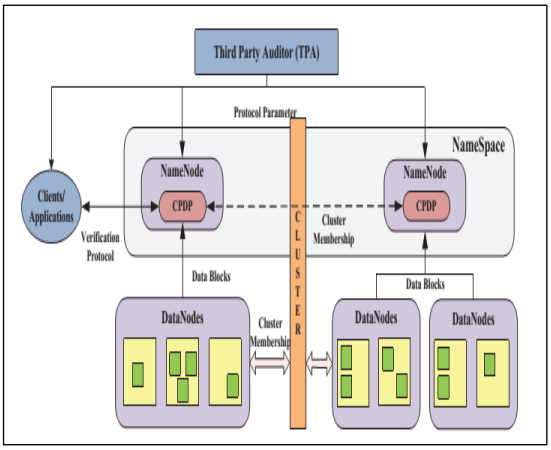

Fig 1.Third Party Auditor

IV. CONCLUSION

The verifiable outsourcing computation into the area of high-dimensional feature extraction and propose a secure verifiable outsourcing scheme of feature extraction based on co-occurrence matrix with single untrusted server.The original images are secret for the server by using a projection of one to many with trapdoor and we propose a symmetric probabilistic encryption as its concrete construction.The technique of public key based homomorphic linear authenticator HLA for short, which enables Third Party Auditor to perform the auditing without demanding the Local copy of data drastically reducescommunication and computation overhead as compared to the straightforward data auditing approaches.

REFERENCES

[1] L.Fillatre, Adaptive steganalysis of least significant bit replacement in grayscale natural images, IEEE Trans. On Signal Processing, 60(2), pp. 556-569, 2012.

[2] Y. Shi, C. Chen and W. Chen, A markovprocess-basedapproach to effective attacking JPEG steganography, IH2006, LNCS 4437, Springer, pp. 249-264, 2006.

[3] C. Chen, Y. Shi, JPEG image steganalysis utilizing both intra-block and inter-block correlations, ISCAS 2008, IEEE, pp. 3029-3032, 2008.

[4] Q. Liu, Steganalysis of DCT-embedding based adaptive steganography and YASS, ACM MM&Sec'11, pp. 77-86, 2011.