International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) ISSN: 2395-5325
Volume 4, Special Issue 3 (March '2018)
Proceeding of - National Conference on Recent Trends in Information Technology and Communication,
Conference held at Velammal Engineering College,Chennai,India.

BATCH VERIFYING TECHNIQUE TO EXTRACT IMAGE FEATURES BASED ON CO-OCCURRENCE MATRIX IN CLOUD

Sharon Jennifer E,
Student,
Department of Computer Science and Engineering,
Velammal Engineering College,
Chennai,Tamilnadu,India.

Jenishiya Hannah. N,
Student,
Department of Computer Science and Engineering,
Velammal Engineering College,
Chennai,Tamilnadu,India.

Abimathi A,
Student,
Department of Computer Science and Engineering,
Velammal Engineering College,
Chennai,Tamilnadu,India.

R. Ramya Devi,
Assistant Professor,
Department of Computer Science and Engineering,
Velammal Engineering College,
Chennai,Tamilnadu,India.

Abstract: Cloud computing is an information technology paradigm that enables ubiquitous to share high level services over the internet with minimal efforts. Now-a-days with a rapid usage of cloud most of the organization purchase certain space at cloud server according to their needs.Now, the image features are encrypted and stored in cloud for more secure purposes. After receiving the file, they have to decrypt and find the original file. In our paper, the image file is directly uploaded to the cloud and the features extracted from the uploaded image will be stored in our drive. The automatic key generation is enabled in feature extraction. After uploading, the image seeker can view the broken image from the image selling site. If the image seeker wants to buy the image, he has to send a request to the image owner. The image owner then sends a water mark image to the requested seeker. Image extracting batch verifying algorithm is used to select the required image among the stored image features. After receiving the water mark image, the seeker has to make the payment. The seeker will not be able to download the original image without getting authorization from the owner.

Keywords: Cloud Computing, Image Processing, Image Extraction, Image Handover

I.INTODUCTION

Cloud computing is the long - standing vision of computing as a utility that enables convenient and on- demand access to centralized pool of configurable computing resources. In the present days, companies and individuals have begun to purchase a particular space and have started to outsource their datas to public clouds that makes feasible access control mechanism.Cloud providers typically use a "pay-as-you-go" model, which can lead to unexpected operating expenses if administrators are not familiarized with cloud-pricing models.

When there is so much improvement in the technology there is also so many security issues. Security issues occurs in retrieving the original data or images that are saved in the cloud. This paper describes about extracting the image features that are stored in the cloud with high security.

II.LITERATURE SURVEY

With the rapid development of cloud services, the techniques for securely outsourcing the prohibitively expensivecomputations to untrusted servers are getting more and more attention in the scientific community. Exponentiations modulo a largeprime have been considered the most expensive operations in discrete-logarithm-based cryptographic protocols, and they maybe burdensome for the resource-limited devices such as RFID tags or smartcards. Therefore, it is important to present an efficientmethod to securely outsource such operations to (untrusted) cloud servers. In this paper, we propose a new secure outsourcingalgorithm for (variable-exponent, variable-base) exponentiation modulo a prime in the two untrusted program model. Comparedwith the state-of-the-art algorithm, the proposed algorithm is superior in both efficiency and checkability. Based on this algorithm, weshow how to achieve outsource-secure Cramer-Shoup encryptions and Schnorr signatures. We thenpropose the first efficientoutsource-secure algorithm for simultaneous modular exponentiations. Finally, we provide the experimental evaluationthat demonstrates the efficiency and effectiveness of the proposed outsourcing algorithms and schemes[1].

This paper deals with the detection of hidden bits inthe Least Significant Bit (LSB) plane of a natural image. The meanlevel and the covariance matrix of the image, considered as a quantizedGaussian random matrix, are unknown. An adaptive statisticaltest is designed such that its probability distribution is alwaysindependent of the unknown image parameters, while ensuring ahigh probability of hidden bits detection. This test is based on thelikelihood ratio test except that the unknown parameters are replacedby estimates based on a local linear regression

model. It isshown that this test maximizes the probability of detection as theimage size becomes arbitrarily large and the quantization step vanishes.This provides an asymptotic upper-bound for the detectionof hidden bits based on the LSB replacement mechanism. Numericalresults on real natural images showthe relevance of the methodand the sharpness of the asymptotic expression for the probabilityof detection[2].

Today, the most accurate steganalysis methods fordigital media are built as supervised classifiers on feature vectorsextracted from the media. The tool of choice for the machinelearning seems to be the support vector machine (SVM). In thispaper, we propose an alternative and well-known machine learningtool—ensemble classifiers implemented as random forests—andargue that they are ideally suited for steganalysis. Ensembleclassifiers scale much more favourably w.r.t. the number of trainingexamples and the feature dimensionality with performance comparableto the much more complex SVMs. The significantly lowertraining complexity opens up the possibility for the steganalystto work with rich (high-dimensional) cover models and train onlarger training sets—two key elements that appear necessaryto reliably detect modern steganographic algorithms. Ensembleclassification is portrayed here as a powerful developer tool thatallows fast construction of steganography detectors withmarkedlyimproved detection accuracy across a wide range of embeddingmethods. The power of the proposed framework is demonstratedon three steganographic methods that hide messages in JPEGimages[3].

We propose two ciphertext-policy attribute-based key encapsulation mechanism (CP-AB-KEM) schemes that for the firsttime achieve both outsourced encryption and outsourced decryption in two system storage models and give corresponding securityanalysis. In our schemes, heavy computations are outsourced to Encryption Service Providers (ESPs) or Decryption Service Providers(DSPs), leaving only one modular exponentiation computation for the sender or the receiver. Moreover, we propose a generalverification mechanism for a wide class of ciphertext-policy (cf. key-policy) AB-KEM schemes, which can check the correctness of theConcretely, we introduce a stronger version of verifiabilitywhich guarantees that a user cannot accuse DSP of returning incorrect resultswhile it is not the case.

Attribute-based encryption (ABE) provides a mechanism for complex access control over encrypted data.However in mostABE systems, the ciphertext size and the decryption overhead, which grow with the complexity of the access policy, are becomingcritical barriers in applications running on resource-limited devices. Outsourcing decryption of ABE ciphertexts to a powerful third partyis a considerable manner to solve this problem. Since the third party is usually believed to be untrusted, the security requirements ofABE with outsourced decryption should include privacy and verifiability. Namely, any adversary including the third party should learnnothing about the encrypted message, and the correctness of the outsourced decryption is supposed to be verified efficiently.We propose generic constructions of CPA-secure and RCCA-secure ABE systems with verifiable outsourced decryption fromCPA-secure ABE with outsourced decryption, respectively. We also instantiate our CPA-secure construction in the standard model andthen show an implementation of this instantiation. The experimental results show that, compared with the existing scheme, ourCPA-secure construction has more compact ciphertext and less computational costs. Moreover, the techniques involved in theRCCA-secure construction can be applied in generally constructing CCA-secure ABE, which we believe to be of independent interest[5].

III. IMAGE FEATURE EXTRACTION

This application consists of 3 modules. The 3 main modules are Extracting image features, User request processing and Payment and Image handover.

3.1EXTRACTING IMAGE FEATURES

Feature data files which has extension as .jpg, .jpeg, .png only can be uploaded.After storage the image in the database has to be extracted. The image extraction is done using the matrix format and its stored in the user drive with a key generation. This is stored in co-occurrence matrix format using the RGB, height and width values of the image.

3.2USER REQUEST PROCESSING

The image seeker will be able to view only the broken images for security purpose in cloud.Using the image`s name, the image seeker will be able to identify the image. Once the image seeker sends a request to the authorized image owner, the image owner will send a watermark image to the requested image seeker. This watermark image is sent for security purposes and the image seeker will not be able to do anything with the watermark image.

3.3 PAYMENT AND IMAGE HANDOVER

When satisfied with the watermark image the seeker has to make the payment. Once the payment is done the original image will be sent by the image owner that can be downloaded by the seeker.

IV.IMPLEMENTATION

The following are the implementation of how the images are being extracted and processed.

Figure 4.1 Image publisher registration page

Figure 4.2 Image publisher login page

Figure 4.3 Image seeker registration page

Figure 4.4 Image seeker login page

Figure 4.5 Uploading the image page by the image owner

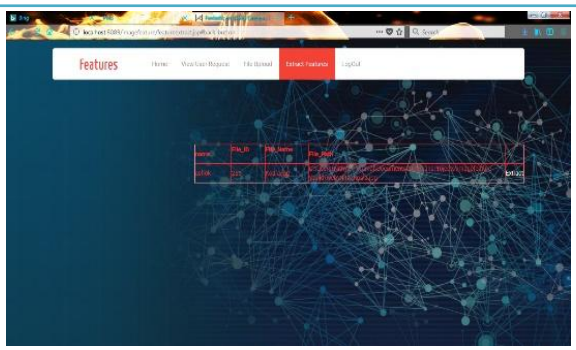

Figure 4.6 Feature extraction for the uploaded images

Figure 4.7 Image name and broken image that is viewed by the user

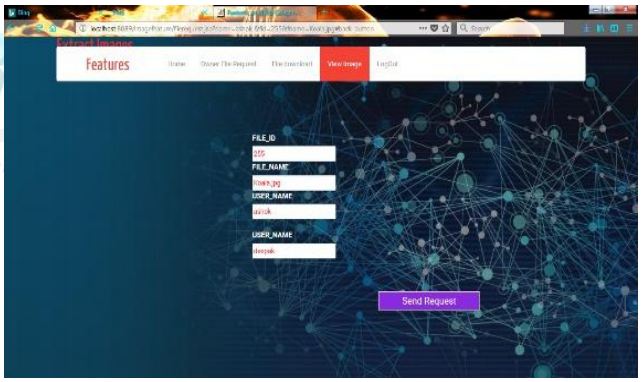

Figure 4.8 Request sent to the owner by the user

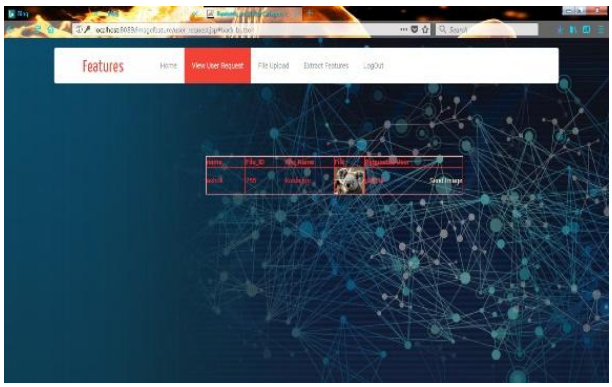

Figure 4.9 Viewing of request by the owner

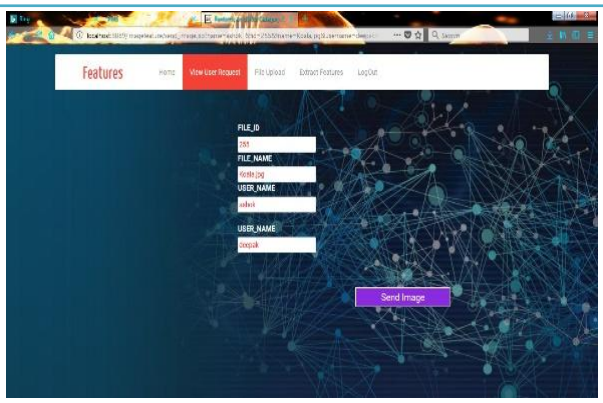

Figure 4.10 Sending watermark image by the owner to the requested user

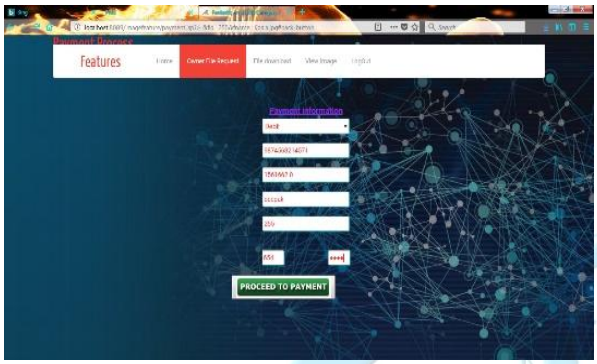

Figure 4.11 Payment by the user

V. CONCLUSION

Thus from this study it is noted that an image features can be extracted and downloaded by the image seeker with high security and better efficiency. The image is highly secured and the image publisher can sell the image using this online application.

VI.REFERENCES

[1]. Xiaofeng Chen, Jin Li, Jianfeng Ma, Qiang Tang, and Wenjing Lou, Senior Member, IEEE, "New Algorithms for Secure Outsourcing of Modular Exponentiations" in IEEE Transaction on Parallel and Distributed Systems, Vol. 25, No. 9, September 2014.

[2]. Lionel Fillatre, Member, IEEE, "Adaptive Steganalysis of Least Significant Bit Replacement in Grayscale Natural Images" in IEEE Transactions on Signal Processing, Vol. 60, No. 2, February 2012.

[3]. Jan Kodovský, Jessica Fridrich, Member, IEEE, and Vojtěch Holub, "Ensemble Classifiers for Steganalysis of Digital Media" in IEEE Transactions on Information Forensics and Security, Vol. 7, No. 2, April 2012.

[4]. Hui Ma∗, Rui Zhang∗, Zhiguo Wan, Yao Lu and Suqing Lin, "Verifiable and Exculpable Outsourced Attribute-Based Encryption for Access Control in Cloud Computing" in IEEE Transactions on Dependable and Secure Computing, 2015.

[5]. Xianping Mao, Junzuo Lai, Qixiang Mei, Kefei Chen, Jian Weng, "Generic and Efficient Constructions of Attribute-Based Encryption with Verifiable Outsourced Decryption" in IEEE Transactions on Dependable and Secure Computing, 2015.