Asian Journal of Information Technology 15 (10): 1574-1578, 2016
ISSN: 1682-3915

Attempting to Preserve Energy During Private Data Delivery Using Various Encryption Techniques

[1]G. Selvavinayagam and [2]K. Umamheswari
[1]Department of Information Technology, SNS College of Technology,
[2]Department of Information Technology,
PSG College of Technology, Coimbatore, Tamil Nadu, India

Abstract The focus is to examine the energy preservation for mobile system in confidentiality conservation computation unloading because these calculations concentrated programs can preserve the information not by compromising the confidentiality. The security techniques should assure process executed on the guarded information to linger significant and recognizable results. This confidentiality entails large amount of overheads in terms of overhead. The plan is to modify encryption schemes for guarding the recovery of images before forwarding the data to the servers. The performance evaluation is conducted for estimating the image recovery and energy preservation.

Keywords: Energy preservation, mobile system, confidentiality, overhead and encryption scheme

INTRODUCTION

These days mobile systems are used by every individuals for making their jobs easy and its usage became mandatory but the only drawback is its restricted power. The solution to the problem is achieved by transferring the information from mobile systems into large servers which considerably saves systems battery called unloading (Wolski *et al*., 2008; Li *et al*., 2001). But, this as singular does not provide solution for all the problems since there can occur problems in confidentiality with the information stored into the servers due to lack of users direct attention. The earlier discussion mainly aims on making choices on unloading and power consumption. Not all the studies focus on the above problem but simultaneously aims in maintaining the confidentiality in contracting the information (Vimercati *et al*., 2008). The focus is not upon the power consumption spent during providing confidentiality while unloading information.

For guaranteeing confidentiality the information is to be well protected before initiating the transmission into the server. Confidentiality can be achieved either steganography technique or encryption technique (Chandramouli *et al*., 2004). The concept in steganography is that the information is concealed so that the server will not be aware about the information completely. The common encryption techniques is of no use in transferring the guarded information, so it cannot finds it position during data unloading since the information are subjected for decryption at the server before initiating a task with that piece of information. The main drawback is that these techniques different volume of energy consumption for providing confidentiality.

The extraction of images identifies images related to the query and extorts the features of images and studies the features. This focuses on the information and serves a best way for preserving the power. ReqFig and linear straining (Jacobs *et al*., 1995) serves as best techniques for extracting images. Unloading technique requires the image to be secured before transferring them into servers since the tasks accomplished on secured images is significant.

ReqFig is used for searching identical images which is being confined using steganography (Liu *et al*., 2010). But this technique is quite sensitive to direction since if the object present inside the image is shifted it is not possible for the technique to extract identical images. But, it is not at all a problem with linear straining (Ng *et al*., 2005) because it is not sensitive to directions. Confidentiality is achieved using linear straining which is not possible with steganography. A similar technique is focused for encryption in order to safeguard the information when unloading the linear straining extraction algorithm and the analysis for performance and power utilization are also focused. The obtained results show that the proposed technique banks diverse energy levels with diverse levels of confidentiality.

Corresponding Author: G. Selvavinayagam, Department of Information Technology, SNS College of Technology, Coimbatore, Tamil Nadu, India

Literature review: The studies were performed for information unloading with the focus on things to be performed for unloading.

ReqFig (Jacobs *et al*., 1995) is employed for image extraction which produces 2D wavelet decompositions on the image thus searches for huge amplitude features. Linear straining (Ng *et al*., 2005) removes the features on the image at diverse levels and directions for evaluating the comparisons. The focus is upon using the linear straining on an image with diverse levels and directions for attaining strained images and computation is performed on each strained images. The obtained image features from degree of the strained images at each levels and directions along with features for comparison.

Similar encryption (Gentry, 2010; Zhu *et al*., 2006) permits operations carried out on information not by using decryption. Current studies focuses on the feasibility to build a full similar encryption technique but the efficiency still remains an unsolved question.

A limited module for similarities like addition, multiplication and combined multiplication (Fontaine and Galand, 2007) are used widely. These techniques are used in encryption but the similar values in input text vary after decryption. Encryption for a number p with keys x, y by selecting an arbitrary value z in order to attain an encrypted value a = Encrypt (p) = (p+zx) mod V where V = xy. The decryption is achieved by using a key s to obtain a = Decrypt (b) = b mod s. Similar encryption techniques is allowed only for a set of values. Non-integer values must be converted into integers for performing similar encryption techniques.

The aim of the paper is to preserve power while providing confidentiality in information unloading. A similar encryption technique is employed for safeguarding the information for unloading a linear extraction method. The images are encrypted before they are transferred to the server. The information into the server is never subjected to decryption thus guarantying confidentiality.

MATERIALS AND METHODS

Safeguarding confidentiality in information unloading: Unloading information aims to converse power on mobile systems but subsequently the information must be confined before initiating the transfer to server resulting in operational cost for power. Initially, it is needed to construct a model for power based on safeguarding confidentiality during information unloading. Also analysis of features during various image extraction algorithms and confidentiality methods are also done. Finally a technique for power preservation by unloading image extraction with information confidentiality is provided by similar encryption.

Power model: A power model is constructed with the following metrics called calc and vol which denotes the quantity of calculations and the volume of information distributed.

Case 1: Consider execution of a program P in absence of unloading on a mobile system with input information I and produce an output O. The volume of power consumed on mobile system is calculated using:

$$E_c \times \frac{Cal(P)}{S_s} \quad (1)$$

Here, E_c denotes the energy for performing the task and S_s denotes the speed of server.

Case 2: Represents unloading without focusing on confidentiality. The input I and program P are unloaded to the server and finally the output O is returned to the mobile system. The entire volume of power consumed comprises of unused power upon executing the program P and the power for transferring the information I and obtaining the output O through the network is:

$$U_p \times \frac{Cal(P)}{S_s} + N_e \times \frac{Vol(I+O)}{N_b} \quad (2)$$

Where:

U_p = The unused power
N_e = The energy over the network
N_b = The network bandwidth

Case 3: Characterizes the confidentiality safeguard during unloading. The information I is confined as I' using a technique C. In order to gain access to the confined information some alterations are necessary are made into the program and so the program P' is different from P. I' and P' are unloaded into the server while the output O' is given back to the mobile system and then processed by a proportion which is inverse to C^{-1} thus attaining the output O. A considerable quantity of power is consumed for C and C' unused while the server executes P' thus by getting I' and producing O'.

$$E_c \times \frac{Cal(C+C^{-1})}{S_s} + U_p \times Cal(P') + N_p \times \frac{Vol(I'+O')}{N_b} \quad (3)$$

Safeguarding information in image extraction: Extraction of images is severe thus assisting from unloading in order

to conserve power. The focus on confined information is achieved by making changes into image extraction techniques. These changes should also provide significant improvement in performance as compared with the initial course and unconfined information. It is necessary to focus on various extraction algorithms along with diverse schemes for handling confidentiality. The focus is upon two various extraction algorithms, namely ReqFig and linear straining and two diverse schemes for providing confidentiality namely steganography and similar encryption. The steganography concept makes use of an image that envelope to mask the confined image thus making it difficult to identify. This is the common and easy steganogrpahy technique employed for images using an envelope which replaces each and every bits of the confined image. The encryption technique converts the input information into a form which cannot be read easily by others. The steganographic technique does not find any similarity with encryption technique since the encryption techniques requires a key to hide information. ReqFig can imply steganographic techniques (Liu *et al*., 2010) by making use of sequential characteristics in extracting image features. The techniques consider that all images possess same dimensions and directions. Linear straining holds better level of accuracy as compared with ReqFig for finding related images with different directions. Here, the information cannot remain confined if steganography schemes are used since they do not exhibit sequential characteristics. Similar encryption schemes can be employed in linear straining since they likely make use of additions and multiplications on the confined information.

Unloading linear straining with encryption: Here, similar encryption is used to safeguard information when unloading the linear strain extraction. The encryption and decryption techniques are different parts in an operation and it is to be focused that both input and output should not mix up which can be attained using a large key K. This is because a small key value may result in wrong decryption values and significantly corrupt the performance during extraction. A large key requires high calculations to evade thus parallel offers a good means of confidentiality. But is also to be focused that large key requires a lot of energy for transferring and perform calculations on huge volume of information.

Very well after encryption techniques some changes are required on linear straining extraction program. This encryption technique remains similar only for integers since the coefficients are not integers which must be represented using suitable integers. This is achieved by limiting a coefficient c_e to [M] which serves as a rounding value and M is the required limiting value. A large limiting value generates more precise estimation. The calculations are performed only for integers but after setting a limiting value the estimated linear strains are used for confine information. It is to be noted that the encryption technique expands all the pixels into a large integer value for the calculations are performed. Altered extraction techniques are used for both the initial and encrypted information with different directions for accuracy due to estimation.

The linear straining extraction program holds two diverse methods. Before performing encryption all the information are transferred into server. Using encryption it is not possible to unload all the information. The later technique employs operations like division and square root which are not suitable for applying into the encrypted information thus allowing the mobile system to run on unconfined information.

RESULTS AND DISCUSSION

Performance evaluation: The evaluation for information safeguarding, accuracy for extraction and power consumption are performed. The analysis is performed by converting every requested image into one of the following options as blocks holding 4 pixels, grayscale, blocks with 4 pixels mix up, rotating 45 degrees clockwise, rotating 90 degrees clockwise, rotating 180°, movement shadow, zoom shadow and adding external particles. A requested image is subjected to all of these options along with its original form are the equivalent images while the extraction programs focuses in finding an equivalent images from these set. The following are the types of threats for confidentiality (Fontaine and Galand, 2007):

- Threats for encrypted information by the attackers
- Recognized input information where the attackers gain access to the input information which is very well known thus causing a threat to the resulting output also
- Selected input (or) decrypted information attacks are possible by selecting input text or decrypted text

The complication with these attacks decreases for the above mentioned order. The proposed system unloading, encryption and decryption are achieved on mobile systems thus allowing only the server to access the decrypted information. Thus an attacker can make use of only encrypted information for attacks and it is the weakest form of attacks. This can be made worse by changing the encryption keys of various pixels. At this point it is necessary to focus on the size of key.

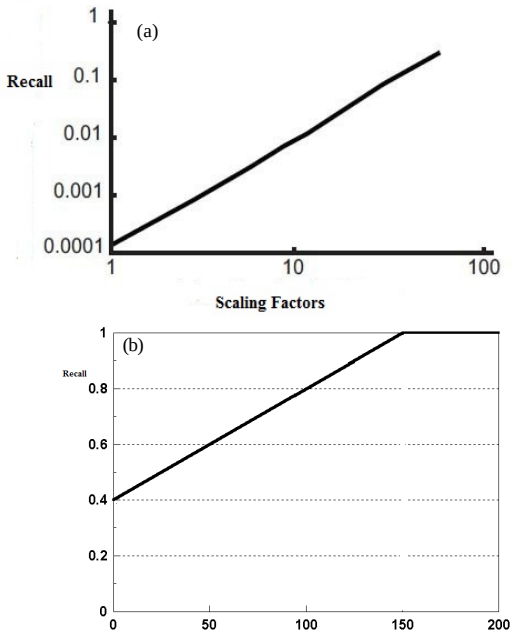

Fig. 1a): Extraction performance with various scaling factors; b): Various K sizes

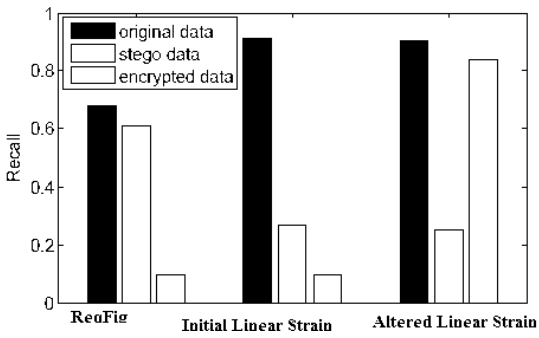

Fig. 2: Comparison of various methods with extraction performance

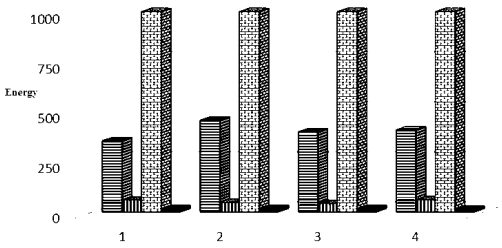

Fig. 3: Power utilization in various unloading methods

All the above mentioned options on image is applied to ReqFig, initial linear strain, altered linear strain on initial information, steganographic information and output information obtained as a result of encryption. Each and every technique is executed on a server with 6 requisitions for searching into a repository of images gathered over internet to estimate the extraction performance. The measuring factor M and the size of the key K have their influence over the extraction performance. Figure 1a depicts the results of K and when the value of K is 5 the recall becomes nearly 0. Larger the value of K the estimation is more accurate and the performance of extraction gets better. The performance faces diversion when the value of K crosses a value more than thousands. Figure 1b depicts the results of size of the key K. When, the input is small the recall holds smaller values because mostly the results produced have errors. The improvement in performance is achieved only when the size of key increases and finally attains a constant value. Figure 2 depicts the similarities of extraction performance from the methods employed on the input information. The linear straining holds a better performance as compared with ReqFig when finding an image from the initial repository of images holding some images with different directions. When the information are confined using steganography ReqFig attains about 85% of performance contrast with finding initial information while the recall is less when the information are subjected for decryption. Initial linear straining holds better performance on finding initial information with a recall of 0.93 but the performance on steganographic and encrypted information are not up to the level thus fostering modifications. Upon finding similarities between initial information the altered linear straining holds better performance nearly to find unconfined information and focuses on improving the performance on encryption. This is to be noted that various image extraction algorithms reuires diverse confidentiality schemes. Here the steganography performs well for ReqFig and encryption serves better for linear straining. Figure 3 depicts the power consumed in total in each and every unloading technique.

CONCLUSION

The study focuses on techniques for unloading image extraction for preserving the power with confidentiality. The information is safeguarded using similar encryption and the information is transferred to a server. The technique is executed and the similarities for calculating the extraction performance and power consumption are achieved. The output depicts that the proposed technique holds a better performance as

compared with the extraction performed directly without unloading and preserves power to different levels by selecting diverse keys in the encryption.

REFERENCES

Chandramouli, R., M. Kharrazi and N. Memon, 2003. Image Steganography and Steganalysis: Concepts and Practice. In: IWDW 2003, Kalker, T., I.J. Cox and Y.M. Ro (Eds.). LNCS., 2939, Springer Verlag, Berlin/Heidelberg, pp: 35-49.

Fontaine, C. and F. Galand, 2007. A survey of homomorphic encryption for nonspecialists. EURASIP. J. Inf. Secur., 2007: 1-15.

Gentry, C., 2010. Computing arbitrary functions of encrypted data. J. Commun. ACM, 53: 97-105.

Jacobs, C.E., A. Finkelstein and D.H. Salesin, 1995. Fast multiresolution image querying. Proceedings of the 22nd Annual Conference on Computer Graphics and Interactive Techniques, September 6-11, 1995, ACM, New York, USA., ISBN: 0-89791-701-4, pp: 277-286.

Liu, J., K. Kumar and Y.H. Lu, 2010. Tradeoff between energy savings and privacy protection in computation offloading. Proceedings of the 16th ACM/IEEE International Symposium on Low Power Electronics and Design, August 18-20, 2010, ACM, New York, USA., ISBN: 978-1-4503-0146-6, pp: 213-218.

Ng, C.R., G. Lu and D. Zhang, 2005. Performance study of gabor filters and rotation invariant gabor filters. Proceedings of the 11th International Conference on Multimedia Modelling, January 12-14, 2005, IEEE, New York, USA., ISBN: 0-7695-2164-9, pp: 158-162.

Vimercati, S.D.C.D., S. Foresti, S. Jajodia, S. Paraboschi and G. Pelosi *et al.*, 2008. Preserving confidentiality of security policies in data outsourcing. Proceedings of the 7th ACM Workshop on Privacy in the Electronic Society, October 27-31, 2008, ACM, New York, USA., ISBN: 978-1-60558-289-4, pp: 75-84.

Wolski, R., S. Gurun, C. Krintz and D. Nurmi, 2008. Using bandwidth data to make computation offloading decisions. Proceedings of the IEEE International Symposium on Parallel and Distributed Processing, April 14-18, 2008, IEEE, Miami, Florida, ISBN: 978-1-4244-1694-3, pp: 1-8.