ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 10, October 2015

Privacy Preserved Image Recognition on MSB Encrypted Images

Sayyada Fahmeeda Sultana[1], Dr. Shubhangi D.C.[2]

Asst. Professor, CSE Department, PDA College of Engineering, Kalaburgi, India [1]

Professor, Department of CSE, VTU PG Centre, Kalaburgi, India [2]

Abstract: Cloud computing are the most valuable innovations for business, research, development, etc., providing cheap, virtual-services that will require expensive local hardware. With the availability of Cloud Computing we place almost everything in the cloud, but what do we really know about its security. One of the security risks in cloud computing according to Garfunkel is data intrusion. Privacy preservation of online data while offering efficient functionalities has become an important and focused research issue. Encryption is one of the fundamental techniques that manage the digital rights of any personal or other confidential information. In this paper we present a Privacy preserved image recognition system on MSB encrypted face images performed using one time padding, followed by Face image recognition with PCA-principal component analysis followed by SIFT- Scale invariant feature transform on selected images. MSB encryption provides protection of image with low PSNR from un-trusted managing authority cloud server. Whole face image recognition process performed in encrypted domain.

Keywords: Cloud; Face Images; PCA; PCA followed by SIFT; MSB; ROC;

I. INTRODUCTION

The cloud computing is used potentially to provide cost effective, easy to manage, elastic, and powerful resources over the Internet. The area cloud computing ensures the capabilities of the hardware resources by optimal and shared utilization. With the above mentioned and many features encourage the organizations and individual users to shift their applications and services to the cloud [5]. Even the critical infrastructure, for example, power generation and distribution plants are being migrated to the cloud computing paradigm. These services provided by third-party cloud service providers entail additional security threats [6]. The migration of user's assets (data, applications, etc.) outside the administrative control of client in a shared environment where huge number users are collocated escalates the security concerns.

The Technological advances in digital content processing, production and delivery has given rise to a variety of new image and signal processing applications in which security (privacy) risks can no longer be handled in a classical or traditional fashion. In most of the cases, security and privacy risks may require the adoption of new image and video processing services [1-3]. For this reason, the use of cryptographic techniques (Encryption) in image processing applications is becoming increasingly common.

In this work, we propose an enhanced framework for privacy preserving of image recognition in encrypted domain. Biometric images are encrypted by using a fast and robust cryptographic method based on one-time-pad encryption using randomly generated numbers as key with MSB. Encrypted images stored for projection on cloud by PCA followed by SIFT on selected images based face recognition process is applied on these images. This method provides a fast and secure solution for private data protection for biometric templates. At the same time, it forms an enhanced base framework for other image processing applications on biometric data. It has been presented successful application of face recognition scenario and analysed the proposed framework in terms of privacy protection and recognition performance.

II. PROBLEM FORMULATION

A. System Architecture

As illustrated in figure. 1, we have considered a high level system architecture of Privacy preserving Image recognition in encrypted domain. At the core the system consists of two parties client and cloud. Client may represent an individual or enterprise, who owns private and will to outsource the storage and computational complexities to cloud. The task of client is to apply cryptographic technique on image '*I* ' and retrieve cipher image 'C' and upload it on to cloud specifically, to maintain security against unauthorized access. Further the client can retrieve relevant image in course of time by sending query encrypted image.

Cloud: The expected image processing results from cloud is a recognized image in encrypted domain. At the core cloud consists of two entities: PCA to determine the most discriminating features between faces images and SIFT to generate key points and descriptors of query image and on the results obtained using PCA.

B. Security Model

The consideration is the image *I* owned by client to be private. The client's goal is to protect the privacy of image content, while enabling Cloud to execute Recognition algorithms over it without decrypting. We consider in the framework the Cloud to be honest-but curious and independent to view the images, in our design the client

DOI 10.17148/IJARCCE.2015.41086

encrypts the image all computations are performed in encrypted domain.

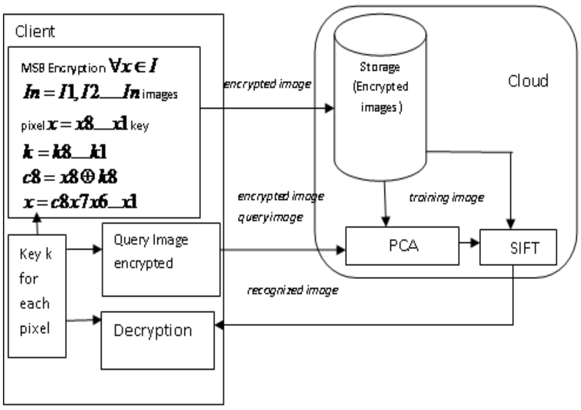

figure1: Overview of Overall System Architecture

C. System Design

Our ultimate goal is to design a privacy preserving face image recognition system that support outsourced face image recognition in encrypted domain. In particular we have the following design goals:

Image content Privacy: As claimed in our proposed system, the cloud entities should not get correct access to the image content. According to the encryption strategies [23] the MSB bit of each pixel is encrypted, the confidentiality of image is protected when each pixel of the image is encrypted. The Encryption of the proposed system is given in Algorithm 1.

```
-------------------------------------------------------------
Algorithm 1 Encryption of MSB bits of Image
-------------------------------------------------------------
Input: The Input Image, $I(M \times N)$ Random number k;
Output: The Encrypted image $I'$;
Step1: For each pixel $\forall p(i,j) \in I$ do
Step1.a: Convert pixel intensity value $p(i,j) \rightarrow b$ into
   binary equivalent;
Step1.b: Convert pixel intensity value $k(i,j) \rightarrow$key into
   binary equivalent;
Step 1.c: Pick MSB of b and MSB of key;
Step 1.d: $c = (MSB\ of\ \ b(8) \oplus MSB\ of\ \ key(8))$
Step 1.e: $C' = cb7b6b5b4b3b2b1$;
 Step 1.e: $I'(i,j) = C'$;
Step 1.f: end for
Step 2: return encrypted image $I'$.
```

D. Face Recognition using PCA followed by SIFT

PCA contains three entities:

1. Database Creation: This function reshapes all 2 dimension images of the training database into 1 dimension column vectors. Then, it puts these 1 dimension column vectors in a row to construct 2 dimensional matrix 'T'.
2. Eigen face core: To determine the most discriminating features between images of faces. This function gets a 2 dimension matrix, containing all training image vectors and returns similar images as outputs which are extracted from training database.
3. Recognition: All centered images are projected into face space by multiplying in Eigen face bases. Projected vector of each face will be its corresponding feature vector. This function compares two faces by projecting images to face space and measuring the Mahalanobis distance between them the minimum distance is the recognized image.

$mahalanobis(u,v) = (u-v)\sum^{-1}(u-v)^T$ Where Σ is the covariance matrix of the input Image I'

$$\Sigma_{j,k} = \frac{1}{n-1}\sum_{i=1}^{n}(I'_{ij} - \overline{I'}_j)(I_{ik} - \overline{I'}_k)$$

E. PCA followed by SIFT

SIFT contains three entities:

The first step in computing the locations of potential interest points in the image by detecting the maximum and minimum of a set of Difference of Gaussian filters applied at different scales all over the image.

Upon, these locations refinement is performed by discarding points of low gray intensity. An orientation is then assigned to each key noted point based on local image features.

At last, a local feature descriptor is computed at each key noted point. Feature is considered to be matched with another feature when distance to that feature is less than a specific fraction of distance to next nearest feature.

In the proposed system the functionality of both PCA and SIFT is combined to get the best recognition accuracy in encrypted domain. The Algorithm 2 gives the design of SIFT followed by PCA.

```
-------------------------------------------------------------
Algorithm 2: PCA followed by SIFT
-------------------------------------------------------------
Input: Encrypted dataset T, Encrypted Query Image Q
Output: Three Recognized Image;
Step 1: Apply PCA on T;
Step 2: Pick k- minimum distances images M by checking
   Mahalanobis distance measure with Q
Step 3: $\forall I \in PCA(result)$ recognized images from M
   of step 2;
Step 3.a: Apply SIFT on last seven bit of pixel;
            $I \rightarrow I1$
Step 3 b: Apply SIFT on last seven bit of pixel;
            $Q \rightarrow Q1$
```

Step 3.c: Measure the percentage of features matched;

$$(I1, Q1) \rightarrow R$$

Step 4: Maximum the percentage of match is the recognized image;

$$F = Max(R)$$

Step 5: Return F a vector of three recognized images

III. EXPERIMENTAL RESULTS

We conduct a thorough experimental evaluation of the proposed system on ORL image dataset of 40 person images for each person 10 images and unordered BioID face image dataset of 15 person images out of both datasets for each person five images were chosen for testing and remaining images for training of database.

Privacy and confidentiality of image is maintained using MSB encryption with gives Less Average PNSR as compared to other state of art method [23] Last seven bit encryption. The plot of Average PNSRs for other state of art method is shown in figure 2. Lower the PSNR less identifiable is the image.

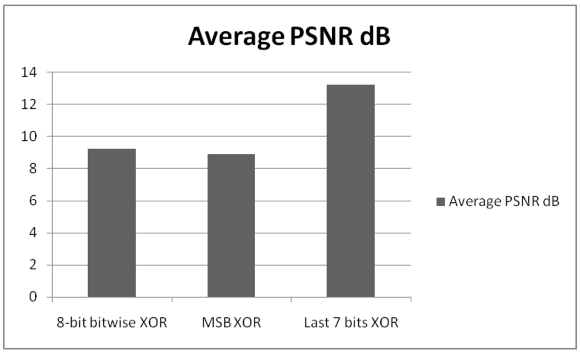

figure 2: Average Peak signal to noise ratio

The structural similarity of image is best shown by histogram figure 3 shows the histograms of images shown by different encryption methods.

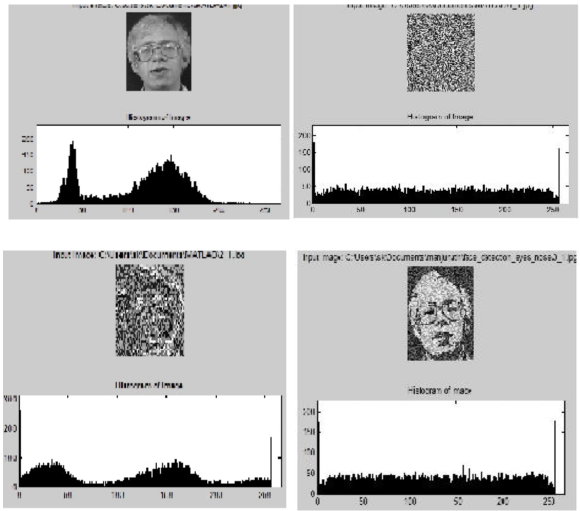

figure 3:a. Original image b. Full 8 bit encryption c. MSB bit encryption d. last 7 bit encryption

However, since our main objective is to perform the face recognition in encrypted domain on MSB encrypted images, which in practical case-complex to achieve due to invisibility of structural features. Which is successfully achieved using PCA followed by SIFT with Rank1 recognition accuracy of 86.6% at 0.3% FAR, Equal Error Rate (EER=0) the ROC curve for recognition accuracy with PCA, SIFT, and PCA followed by SIFT is shown in figure 4.

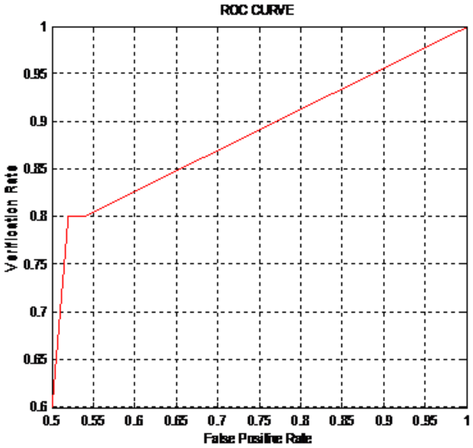

figure 4: ROC Curve

Roc Curve is plotted using on the results obtained from PCA followed by SIFT results for face image recognition in MSB encrypted domain. As seen from the ROC curve AUC (Area under curve) is large area under curve indicating high confidence level of result.

IV. CONCLUSION

With images being the most revealing data uploaded on cloud need the security. One of the measure us of cloud storage in large originations is to maintain the biometric information which can be used for Data mining or cloud owners or workers my querulously examine the images. In this research work, it has been proposed to apply privacy preserved image recognition in encrypted domain based on MSB encrypted images and to achieve good recognition rate with the use of PCA followed by SIFT base recognition, Mahalanobis distance to perform similarity check.

The Rank 1 recognition rate achieved is 85.7 % with 0.01 FAR. The experimental results show that the proposed system is correct and effective for different images in ORL face image dataset. As our ongoing work, we will continue to research on Privacy preserving image detection algorithms for effective utilization over encrypted data.

REFERENCES

1. Georgia Sakellaria, George Loukasb, "A survey of mathematical models, simulation approaches and testbeds used for research in cloud computing", Simulation Modeling Practice and Theory , Volume 39, December 2013, Pages 92–103;
2. José A. Gonzalez-Martinez, Miguel L. Bate-Lorenzo, Eduardo Gomez Sanchez, Rafael Cano-Parra, "Cloud computing and education: A state-of-the-art survey", Computers & Education, Volume 80, January 2015, Pages 132–151;

DOI 10.17148/IJARCCE.2015.41086

3. Farrukh Shahzad, "State-of-the-art Survey on Cloud Computing Security Challenges, Approaches and Solutions", Proceeding Computer Science Volume 37, 2014, Pages 357–362;
4. Moghe, U., Lakkadwala, P., Mishra, D.K., "Cloud computing: Survey of different utilization techniques", Sixth International Conference on Software Engineering (CONSEG). IEEE Conference Publications, Pages: 1 - 4, DOI: 10.1109/CONSEG.2012.6349524.
5. QiangDuan, Yuhong Yan, Vasilakos, A.V., "A Survey on Service-Oriented Network Virtualization Toward Convergence of Networking and Cloud Computing", IEEE Transactions on Network and Service Management , Year: 2012, Volume: 9, Issue: 4, Pages: 373 - 392, DOI: 10.1109/TNSM.2012.113012.120310;
6. Zhao, W., Chellappa, R., Phillips, P. J. & Rosenfeld, A. "Face recognition: A literature survey", ACM Comput.Surv., ACM, 2003, 35, 399-458.
7. Bowyer, K. W., Chang, K. & Flynn, P. "A survey of approaches and challenges in 3D and multi-modal 3D + 2Dface recognition", Comput. Vis. Image Underst., Elsevier Science Inc., 2006, 101, 1-15.
8. Chang, K. I., Bowyer, K. W. & Flynn, P. J. "An Evaluation of Multimodal 2D+3D Face Biometrics", IEEE Trans. Pattern Anal. Mach. Intell., IEEE Computer Society, 2005, 27, 619-624
9. Abate, A. F., Nappi, M., Riccio, D. &Sabatino, G., "2D and 3D face recognition: A survey, Pattern Recogn.Lett.", Elsevier Science Inc., 2007, 28, 1885-1906,
10. Kachare, N. B. &Inamdar, V. S., "Survey of Face Recognition", Techniques International Journal of ComputerApplications, 2010, 1, 29-33.
11. Chellappa R. Wilson, C. S. S., "Human and machine recognition of faces: a survey", 1995, 83, 705-741.
12. T.A.M. Kevenaar, G.J. Schrijen and A.H.M. Akkermans, "Face recognition with renewable and privacy preserving binary templates", IEEE Automation Identification Advanced Technologies: 21-26, 2005.
13. H. Lu and K. Martin and F. Bui and K.N. Plataniotis and D. Hatzinakos, "Face recognition with biometric encryption for privacy-enhancing selfexclusion", DSP, pp.1-8, 2009.
14. C. Busch and A. Nouak, "3d face recognition for unattended bordercontrol", Security and Management, pp. 350-356, 2009.
15. K. Martin, H. Lu, F. Bui, K. N. Plataniotis and D. Hatzinakos, "A biometric encryption system for the self-exclusion scenario of face recognition", IEEE Systems Journal vol.3 (4), pp. 440-450, 2009.
16. Z.Erkin, et al., "Privacy preserving face recognition", Privacy Enhancing Technologies Symposium, pp. 235-253, 2009.
17. M. Osadchy, B. Pinkas, A. Jarrous and B. Moskovich, "Scifi-a system for secure face identification", IEEE Symposium on Security and Privacy, pp. 239-254, 2010.
18. A. Ross and A. Othman, "Visual Cryptography for Face Privacy", Prof. of SPIE on Biometric Technology for Human Identification,2010.
19. M. Upmanyu, et al., "Efficient privacy preserving video surveillance", ICCV: 1639-1646, 2009.
20. W. Puech, Z. Erkin, M. Barni, S. Rane and R. L. Legendijk, "Emerging cryptographic challenges in image and video processing,", ICIP, 2012.
21. S. Ergun, U. Guler and K. Asada, "A high speed IC truly random number generator based on chaotic sampling of regular waveform", IEICE Tran. 94-A(1): 180-190, 2011.
22. F. Dufaux, "Video scrambling for privacy protection in videosurveillance-Recent results and validation framework", In SPIE, 2011.
23. Ovgu Ozturk Ergun, "Privacy Preservating face recognition in encrypted Domain", in IEEE, 2014.