SECURE COMPUTATION OF FACE IDENTIFICATION - SCiFI

Mrs.Mythri.S
Student (M.Tech, CSE),
Department of CSE,
Reva ITM,Bangalore.
s.mythri1@gmail.com

Mrs.Meenakshi Sundaram
Associate Professor
Department of CSE,
Reva ITM,Bangalore.
meenakashi@revainstitution.org

ABSTRACT:-Secure computation of face identification is recently developed secure face recognition systems that ensures the list of faces it can identify remain private. In this work, we study the consequence of malformed input attacks on the system-from both a security and computer vision standpoint. In particular a cryptographic attack that allows dishonest user to undetectably obtain a coded representation of faces on the list, and a visualization approach that exploits this breach, turning the losy recovered codes into human-identifiable face sketches. Evaluation of the approaches on two challenging dataset with face identification tasks given to the computers and human object

KEYWORDS: PRINCIPAL COMPONENT ANALYSIS (PCA), EIGEN VECTOR, EIGEN VALUES

I.INTRODUCTION

This area of study has great applications in security, as we can use facial identification as a form of biometric identification. Identification is where system compares a single image with the list of stored images and determines if it is a close match. This process is especially useful in surveillance for identifying terrorists, criminals, or missing people from a single shot of their face. Video and camera based surveillance is very common and is found to be useful in fighting crime. On the other hand, the ubiquity of such surveillance is a major concern for the public that feels that its privacy is being violated. Our work focuses on face recognition system, which can automatically identify if some know suspects appear in a large set of images. Such systems can be useful, for example, for automatically searching for suspects in a stream of images coming from public places.

On the other hand, these systems can be misused to track people regardless of suspicious, and rogue operator can even combine data from these systems with a universal database linking faces to identities, such as a database of driver's license photos. The proposed SCiFI system matches images taken by a client camera to a list of images (of potential suspect) which are held by a server. Face identification in SCiFI is based on novel face recognition algorithm that performs very well in terms of applicability to real life images and robustness to unseen conditions (e.g., different illumination conditions). The matching is done in a privacy preserving way, using efficient methods of secure computation, and does not reveal any information to the parties, expect for whether a match was found.

Fig.1 Example

II.METHODOLOGY

Implementation part of the project involves the following step

A. Offline processing.

1. Offline processing intern involves preparation of face part vocabulary. In this stage patches from the public databases are extracted.
2. Computation of appearance vocabulary and spatial vocabulary is also done in offline processing.

B. Online processing.

Online facial reconstruction involves

1. Finding best matching patches.
2. Face reconstruction using principle component analysis.

C. Proposed method

Our method consists of two major components. The first is offline stage that builds the facial vocabulary and face subspace from the public database. The second is the online stage that assembles a human face and is done only after a face vector is obtained.

1. **Offline stage:** The face images should come from an external database Y, which are used to create the fragment vocabularies which can be completely unrelated to the people registered in the server's list. All faces are normalized to canonical size, and the positions landmark features (i.e., camera of the eyes) are assumed to be given. Figure 2 gives idea about what is done in offline stage.

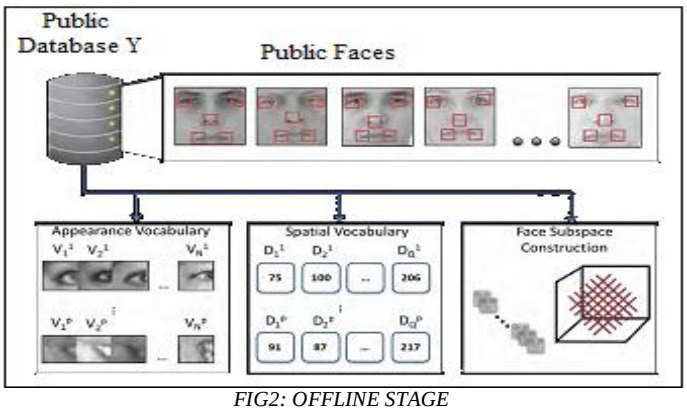


FIG2: OFFLINE STAGE

The figure 2 shows the three major parts of the offline processing stage. At the top of the figure, we build a public face database. Here we show five landmarks indicated by red boxes on each person person's face. The red boxes and their centers serve as windows to build the appearance (bottom left) and spatial vocabularies (bottom middle).the whole faces are also used to build the face subspace (bottom right). Given face images in external database, to form appearance and spatial vocabularies $V_1,\ldots V_p$ and $D_1,..D_p$ use an unsupervised clustering algorithm (k-means) to quantize image patches and distances. We also use the external database Y to construct a generic face subspace. The space of all face images occupies a lower-dimensional subspace within the space of all images, as has been long known in the face recognition community.To compute low-dimensional image representations this face can be exploited. In order to "hallucinate" the portions of a reconstructed face not covered by any of the p patches we exploit a face subspace. Formally, face images in external database Y consist of a set of F vectors $y'_{1,\ldots}y'_{F,}$ where each y'_i is concatenating the pixel intensities in each row of the i-th image. By computing mean face $\mu=1/F\ \Sigma^{F}_{i=1}\ y_i$, and then center original faces by subtracting the mean from each one. Let the matrix Y contain those centered face instances, where each column is an instance $Y=[y_1,\ldots y_F]=[y'_{1-}\mu,\ldots y'_F-\mu]$. Principal component analysis (PCA) identifies the ordered set of F orthonormal vectors $u_1,\ldots u_F$ that describes the data, by capturing the directions with maximal variance. The eigenvectors of $1/F\ \Sigma^{F}_{i=1}\ y'_i\ y_i^T=YY^T$, sorted by the magnitude of their associated eigenvalues,by the definition the desired vectors are the eigenvectors of the covariance matrix computed on Y.The top K eigenvectors define a K-dimensional face subspace.

2. **Online stage:** The SCiFI protocol can be executed after building appearance and spatial vocabularies. A patch face representing the individual using the indices from the vector will be shown by attackers by reverse engineering. The attacker can estimate the missing regions of the face and return a identifiable human face using our reconstruction technique. Figure 3 provides an outline of the second stage of our visual reconstruction.

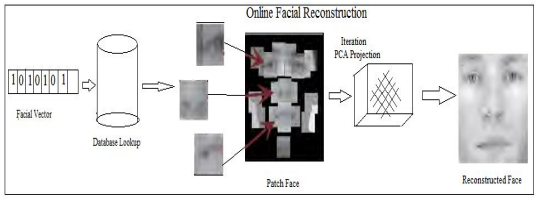
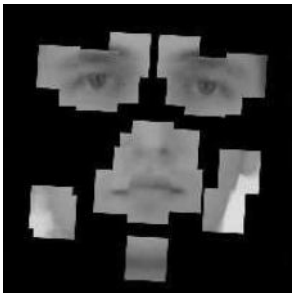


Fig 3: ONLINE STAGE

The figure is an overview of the online face reconstruction process. Given a facial vector from the system, we look up each of the patches that were representative of this face. We can then construct a patch face. Using the patch face as the initial input, we then iteratively project into the face space to synthesize a complete human face. Finding a best matching face: Now we can define how to form patch face reconstruction. For each face of p facial parts, the cryptographic attack defined above yields the n selected appearance vocabulary words and z selected distance words. This encoding reveals which prototypical appearance and spatial was most similar to those that occurred in the original face specifying indices into public vocabularies. Thus, we map retrieved corresponding quantized patches and distance values for each part into an image buffer. We take the n quantized patches and randomly select one of them to reconstruct the appearance of a part i. We average the z distance values for spatial information of part i. We place the patch into the buffer relative to its center, displaced according to the direction oi and the amount given by the recovered quantized distance bin. For example, if n = 4 and $s^a_i=\{1,3,7,19\}$,we look into the patches

$\{v^i_1, v^i_3, v^i_7, v^i_{19}\}$,and compute average then,if say z=2,and he associated distances are $s^s_i=\{4,10\}$,we average patch's center at $½(D^i_4+D^i_{10})o_i$, where the buffer's center is at the origin. To get the patch face reconstruction we repeat this for i=1,…, p.Figure5.3 shows an example patch face. To reverse the SCiFi mapping the process uses all information available in encoding.



Patch Face

Full Face

We first reconstruct the quantized patches based on the binary encoding (left), and then expand the reconstruction to hallucinate the full face given those patches (right).

III .PROPOSED ALGORITHM

Principal component analysis: Based on Face Reconstruction

The remainder of the face image based on the constraints given by the initial patch face is estimated by second stage of our reconstruction approach .We can exploit the structure in the generic face subspace to hypothesize or estimate values for the remaining pixels because these regions are outside of the original SCiFI representation. Associated uses of subspace methods have been investigated for dealing with partially occluded images in face recognition for example, to reconstruct a person wearing sunglasses, a hood, or some other strong occlusion before performing recognition. Here we want to reconstruct portions of the face that are missing, with the end goal of creating a better visualization for a human observer or a machine recognition system. We adopt a recursive PCA technique presented in, which is used to compensate for an occluded eye region within an otherwise complete facial image. Firstly we will initialize the result with our patch face, and then project iteratively into and using public face subspace reconstruction is done each time adjusting the face with our known patches. Comparable to experiments in, ur process makes substantially greater demands on the hallucination, since about 60%-80% of the total face area has no information and must be estimated. Figure 5 gives a sketch of this technique.

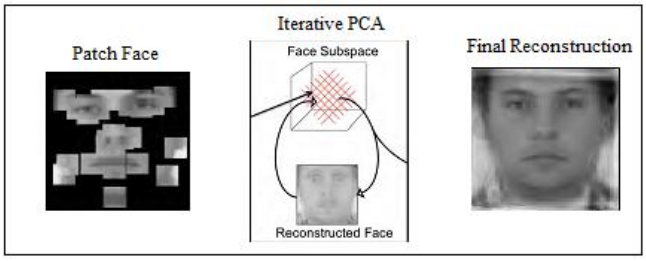


FIG 5: PCA ALGORITHM

The figure 5 illustrates the iterative PCA technique. The input is the patch face and the output is a fully reconstructed face.
Given a novel face x, to obtain its lower-dimensional coordinates in the face space we project face onto the top K eigenvectors (so called eigen faces). Particularly, the i-th Projection coordinate is:

$$w_i=u^T_i(x-\mu),$$

For i=1,…, K.The resulting $w= [w_1,w_2,….,w_k]$ weight vector specifies the linear combination of eigenfaces that best approximates (reconstructs) the original input:

$$\hat{x}=\mu+Uw,$$

Where the i-th column of matrix U is u_i. In our case simply reconstructing once from the lower dimensional coordinates may give a poor hallucination, since many of the pixels have unknown values (and are thus initialized at an arbitrary value of 0). However, by bootstrapping the full face estimate given by the initial reconstruction with the high-quality patch estimates, we can continually refine the estimate using the face space. This works as follows: Let x^0 denote the original patch face reconstruction. Then, define the projection at iteration t as

$$W^t=U^T(x^t-\mu),$$

the intermediate reconstruction at iteration t + 1 as

$$\tilde{x}^{t+1}=\mu+Uw^t,$$

and the final reconstruction at iteration t + 1 as

$$x^{t+1}=\omega x^t+(1-\omega)\tilde{x}^{t+1},$$

Where the weighting term ω is a binary mask the same size of the image that is 0 in any positions not covered by an estimate from the original patch face reconstruction, and 1 in the rest.We cycle between these steps, stopping once the difference in the successive projection coefficients is less than a threshold: max $(|w_i^{t+1} - w_i^t|) < \varepsilon$.

D. Sequence Diagram

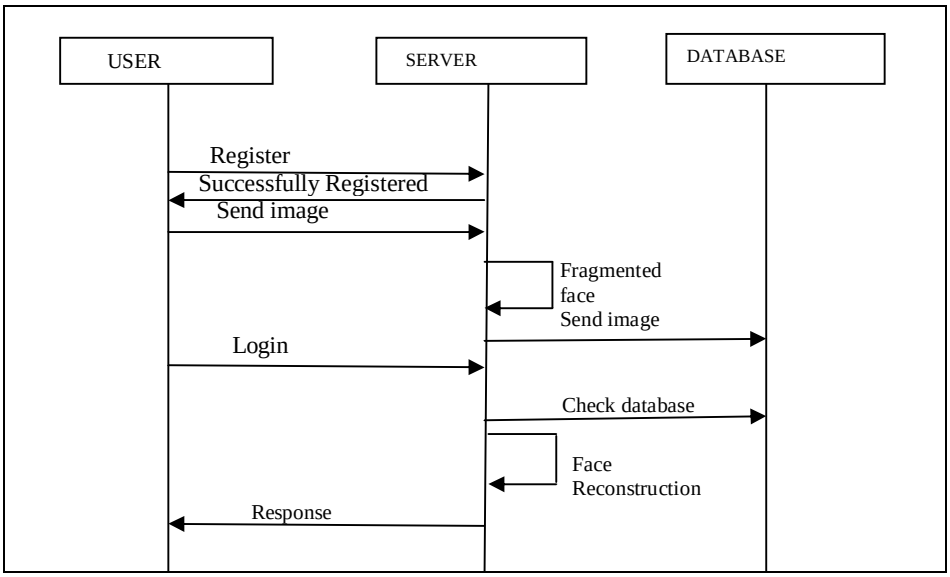


Fig.6 SEQUENCE DIAGRAM

IV. RESULTS AND DISCUSSION

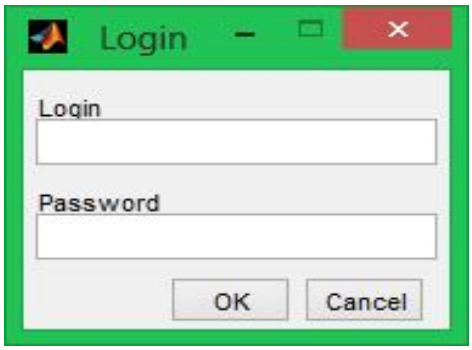


FIG 7 LOGIN PAGE

Login window where authenticated users can login with his username and password.

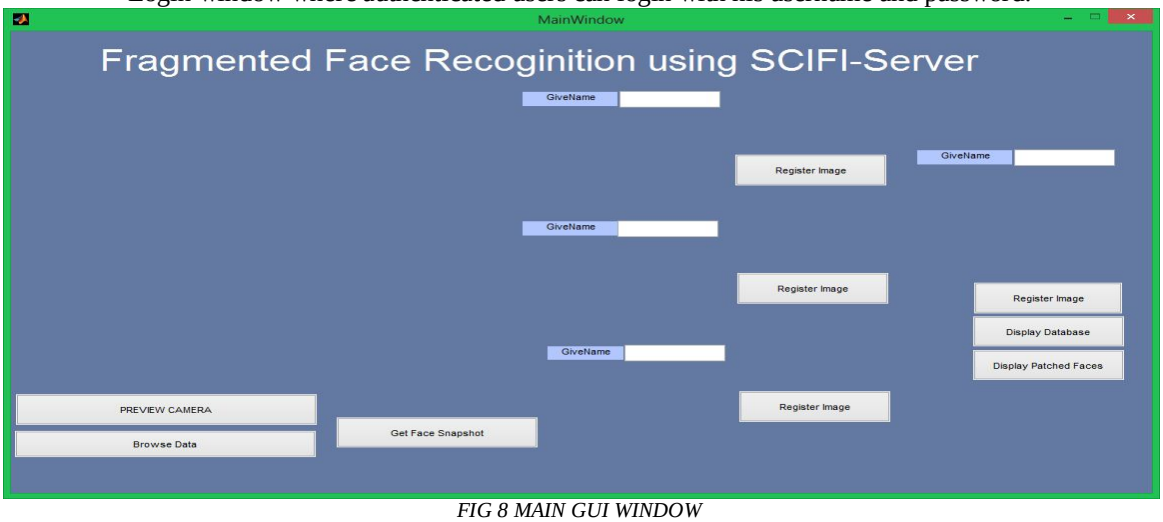


FIG 8 MAIN GUI WINDOW

Fig 6 shows the representation of a main graphical user interface window.

Clicking on PREVIEW CAMERA button turns the camera ON and displays image from camera. Clicking on Get Face Snapshot button crops the face and fragments the image into nose, mouth and eyes. Each fragmented part can be registered by clicking on Register Image button. It will be encrypted and stored in database

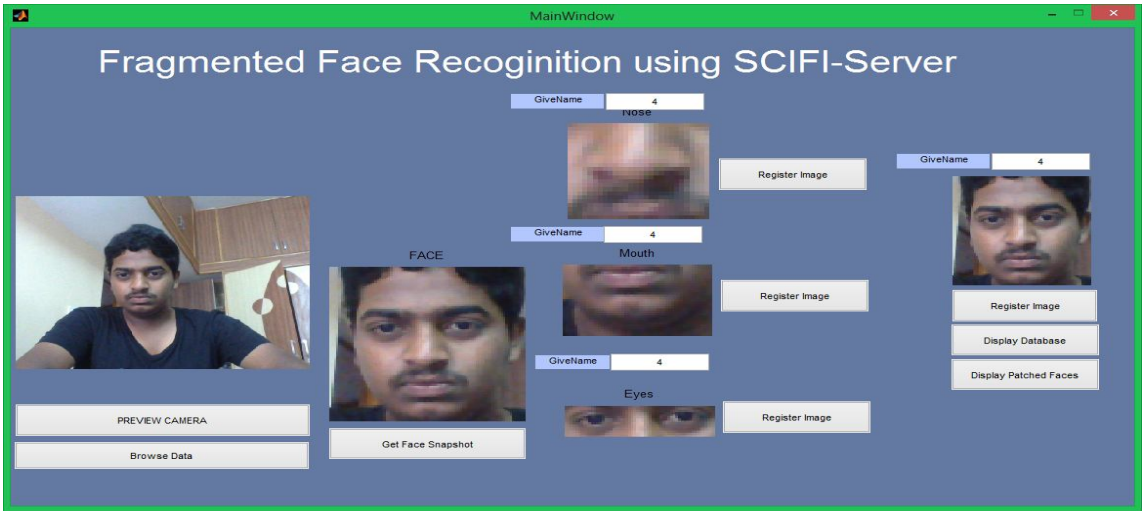


FIG 9 GUI OF FRAGMENTED FACE SCIFI-SERVER

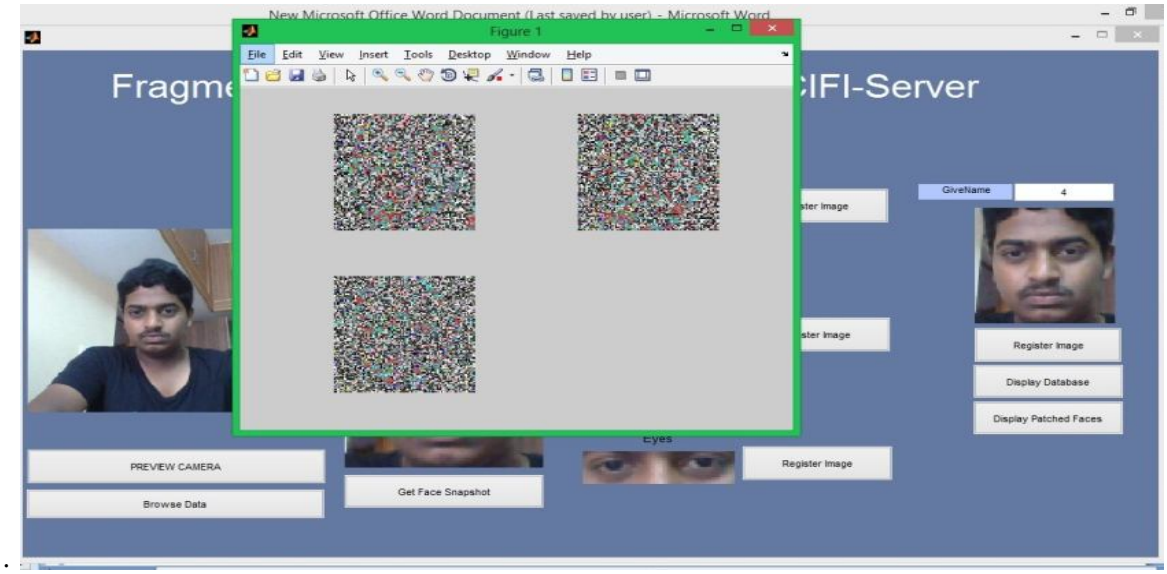


FIG 10 REPRESENTS THE ENCRYPTED FORM OF FACE

Clicking on Register Image button saves the image with given name in database. Clicking on Display Database button displays images in database in encrypted format as shown above.

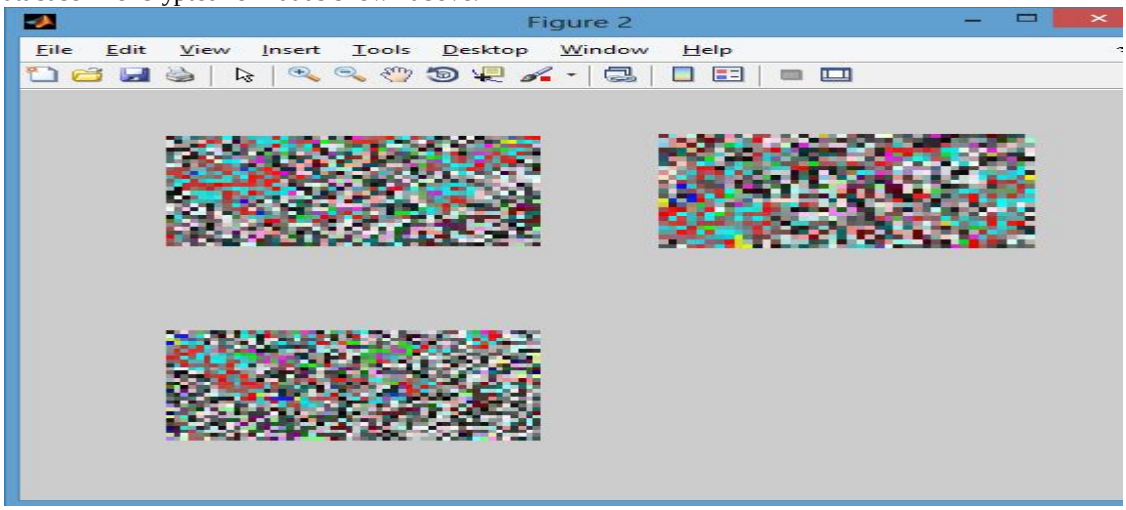


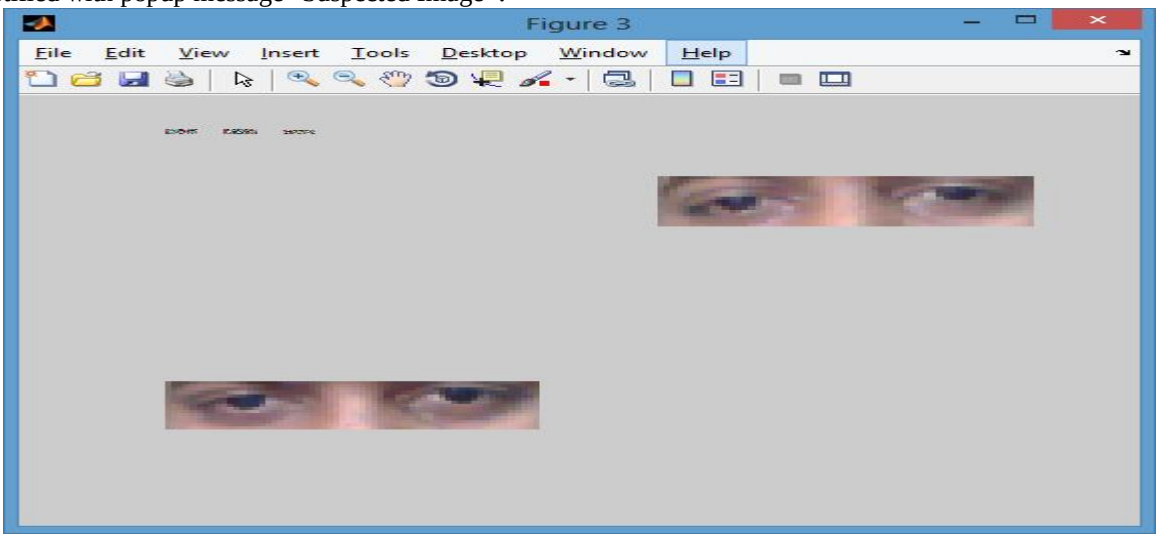
FIG 11 ENCRYPTED IMAGE OF THE PATCH

Clicking on Display Patched Faces button displays the patched images in encrypted format. When we click on display database we get the encrypted form of face stored in database as shown in fig.

FIG 12 SHOWS THE GUI OF CLIENT SIDE

FIG 13 SHOWS IMAGE OF A SUSPECTED PERSON

Clicking on PREVIEW CAMERA button turns the camera ON and displays image from camera. Clicking on Get Face Snapshot button crops the face. When we click on DECRYPT IMAGE button we get decrypted images stored in database as shown below. Clicking on TEST FACE button calculates Euclidian distance between the stored image and captured image and displays matching patches. Euclidian distance of 0.12382 is fixed. Distance below this value will be match and above this will not be considered as match. Then, PCA(Principle Component Analysis) reconstructs and displays face. If there is a match, user will be notified with popup message "Suspected Image".



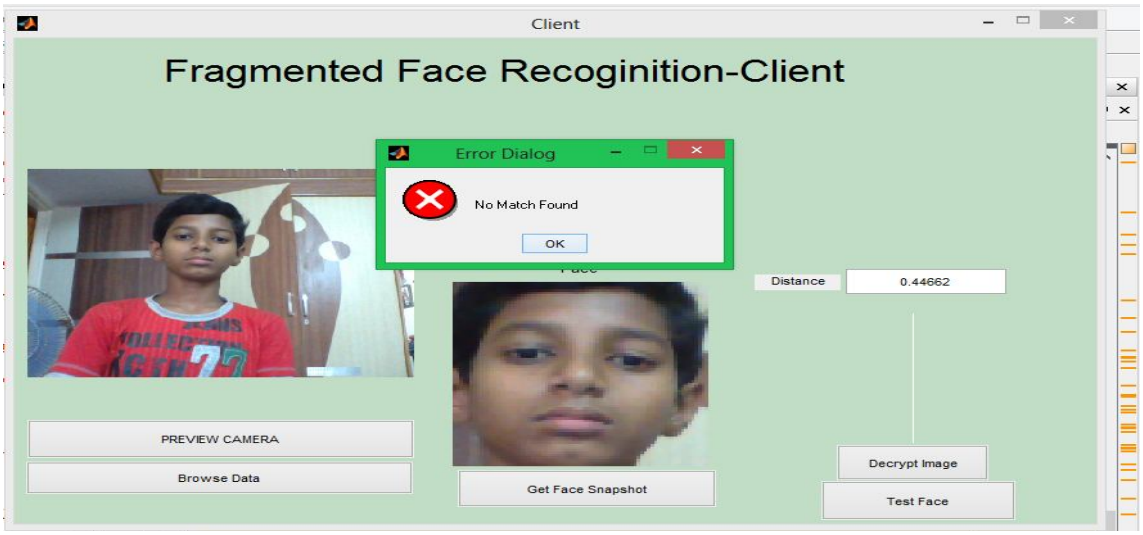


FIG 15 GUI FOR NO MATCH

In above snapshot, Euclidian distance is more than threshold value of 0.12382 and therefore, it is not considered as a match.

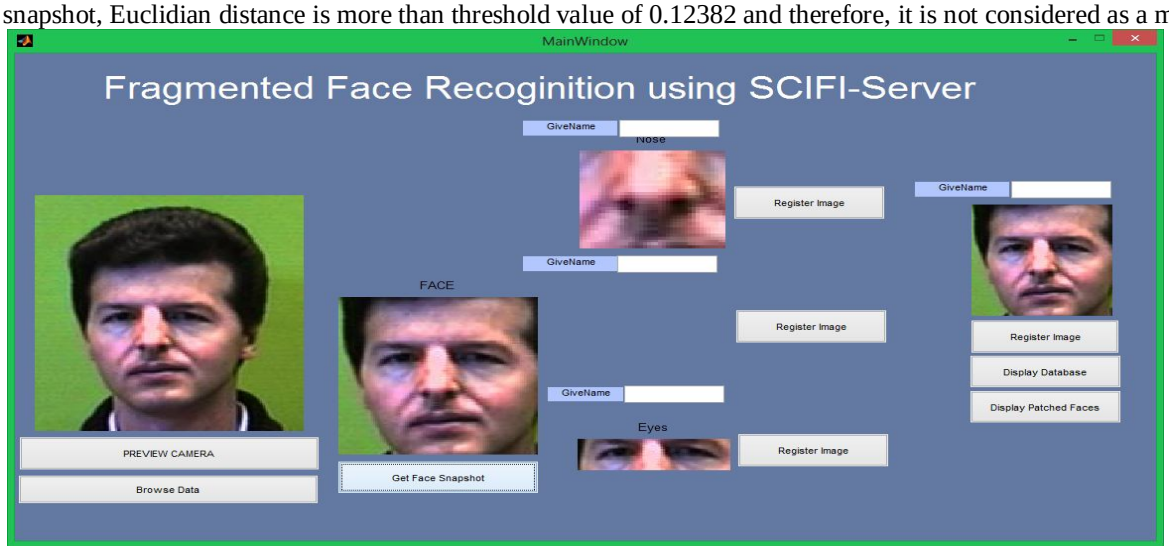


FIG 16 REPESENTS GUI FOR BROWSE DATA

Clicking on Browse Data button opens 'Select Files to Open' window, where we can browse and select images to compare as shown below.

V.CONCLUSION

We present a novel attack on a secure face identification system that control detailed perception from both security as well as computer vision techniques. While the SCiFI system appropriately claims security only under the honest but-curious model, we have demonstrated the dangerous consequences of such a system when exposed to a dishonest adversary. Our vision contributions are to stretch the limits of subspace-based reconstruction algorithm for visualization of severely occluded faces.

REFERENCES

[1] M. Osadchy, B. Pinkas, A. Jarrous, and B. Moskovich, ″SciFI - a system for secure face identification,″ in IEEE Symposium on Security and Privacy, 2010.
[2] M. Gerbush, A. Luong, B. Waters, and K. Grauman, ″Reversing SCiFI: The dangers of malicious adversaries,″ Manuscript, 2010.
[3] W. Zhao, R. Chellappa, P. Phillips, and A. Rosenfeld, ″Face recognition: A literature survey,″ Acm Computing Surveys (CSUR), 2003.
[4] M. A. Turk and A. P. Pentland, ″Face recognition using eigenfaces,″ in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Hawai, Jun. 1992.
[5] T. Cootes, C. Taylor, D. Cooper, J. Graham, and A. Lanitis, ″Active shape models,″ Computer Vision and Image Understanding 1995.
[6] A. Lanitis, C. Taylor, and T. Cootes, ″Automatic interpretation and coding of face images using flexible models,″ Pattern Analysis and Machine Intelligence, IEEE Trans-actions 1997.
[7] T. F. Cootes, G. J. Edwards, and C. J. Taylor, ″Active appearance models,″ in Proceedings of European Conference on Computer Vision, vol. 1407, 1998.
[8] V. Blanz and T. Vetter, ″A morphable model for the synthesis of 3D faces,″ in Proceedings of the 26th annual conference on Computer graphics and interactive techniques.ACM Press/Addison-Wesley Publishing Co., 1999.
[9] F. Li and H. Wechsler, ″Robust part-based face recognition using boosting and transduction,″ in BTAS07, 2007.
[10] M. Fischler and R. Elschlager, ″The representation and matching of pictorial structures,″ Computers, IEEE Transactions on, vol .100 1973.
[11] P. Felzenszwalb and D. Huttenlocher, ″Pictorial structures for object recognition,″ International Journal of Computer Vision, vol. 61, 2005.
[12] A. Juels and M. Wattenberg, ″A fuzzy commitment scheme,″ in Proceedings of the 6th ACM conference on Computer and communications security. ACM, 1999.
[13] A. Juels and M. Sudan, ″A fuzzy vault scheme,″ Designs, Codes and Cryptography, 2006.
[14] Z. Erkin, M. Franz, J. Guajardo, S. Katzenbeisser, I. Lagendijk, and T. Toft, ″Privacy preserving face recognition,″ in Privacy Enhancing Technologies. Springer, 2009.
[15] A. Sadeghi, T. Schneider, and I. Wehrenberg, ″Efficient privacy-preserving face recognition″,Information, Security and Cryptology 2010.
[16] C. Du and G. Su, ″Eyeglasses removal from facial images,″ Pattern Recognition Letters, 2005.
[17] B.-W. Hwang and S.-W. Lee, ″Reconstruction of partially damaged face images based on morphable face model,″ IEEE Transactions on Pattern Analysis and Machine Intelligence (PAMI), vol. 25, no. 3, 2003.
[18] A. Lanitis, ″Person identification from heavily occluded face images,″ in ACM Symposium on Applied Computing, 2004.
[19] Y. Saito, Y. Kenmochi, and K. Kotani, ″Estimation of eyeglassless facial images using principal component analysis,″ in International Conference on Image Processing, 1999.
[20] Z.-M. Wang and J.-H. Tao, ″Reconstruction of partially occluded face by fast recursive pca,″ Computational Intelligence and Security Workshops, International Conference on, 2007.
[21] P. Viola and M. Jones, ″Rapid object detection using a boosted cascade of simple features,″ 2001

