Face Search in Encrypted Domain

Wei Qi Yan [1)] and Mohan S Kankanhalli [2)]

[1)]Auckland University of Technology, New Zealand
[2)]National University of Singapore, Singapore

Abstract. Visual information of images and videos usually is encrypted for the purposes of security applications. Straightforward manipulations on the encrypted data without requiring any decryption have the advantage of speed over performing those operations in spatial, temporal, frequency or compressed domain. In this paper, we will investigate encrypted image search. More specifically, given a face image as the target object, we search it amongst encrypted images. We accomplish the search by using a novel method that extracts features and locates the face object region within the given encrypted image. We evaluate the search results by using precision and recall as well as F-measure. Our experiments reveal that there exists a trade-off between the quality of search and the quality of encryption, namely, stronger encryption leads to poorer search results.

Keywords: Image encryption, object detection, encrypted domain.

1 Introduction

One of straightforward ways of securing digital image transmission is to encrypt the images [23][11][29]. In image encryption, traditional methods like those of asymmetric encryption in public key systems [6] are often adopted, other methods including image scrambling using Hilberts Space-filling Curves (HSC) [17] as well as image sharing based on Chinese Remainder Theorem (CRT) [26] and Visual Cryptography(VC) [20], etc. have also been employed.

Since digital images have relatively huge volume of file size when compared to text, direct manipulations of encrypted images have been highly recommended for the sake of saving space and speeding up the computation [1]. There already has been a slew of inaugural work in this direction. For example, digital image enhancement has been adopted in encrypted domain [14]. Visual features such as histogram and SIFT have been extracted from encrypted domain for a variety of applications [21]. The empirical methods such as clustering and classification on encrypted domain have been developed to group visual objects in categories [30]. Recently, face emotion recognition has been attempted in encrypted domain [22] which is often thought as an important biometric issue, the focus of relevant research work has been shifted from compressed domain to encrypted domain [7][22].

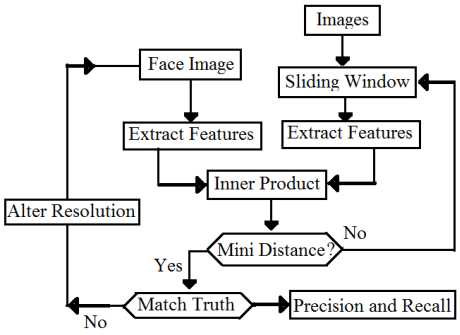

Fig. 1. Flowchart of search in encrypted domain

In this paper, the goal of our research is to accurately find a face within an encrypted image. We perform face object search in scrambled images since scrambling is deemed as a form of encryption. Motivated by face detection and recognition in computer vision [12], search and retrieval in encrypted domain [16][28], and the mighty value of reuse of encrypted data [18], in this paper we will develop a face object search algorithm based on Hilberts Space-filling Curves (HSC) as shown as Figure 1.

Given an image, we segment it into identical sized blocks and use DCT (Discrete Cosine Transform) transform to transfer the pixel values to frequency domain. The reason why we select DCT transform is that most of images and videos are stored in JPEG and MPEG formats nowadays which are based on DCT transform. Using DCT transform could greatly reduce our processing time.

We also employ the HSC curves based image scrambling for encrypting the images to make sure that the encrypted image is secure enough. [17] Given an encrypted image having face objects, we search for the encrypted face along scanline order from top-left to bottom-right. The precision and recall as well as F-measure for evaluating the search results are calculated.

Our contributions of this paper are listed below.

(1) *Encrypting digital images using the scrambling algorithm based on Hilberts space-filling curves.* In this paper, we will utilize the HSC based image encryption [17][2] and present our findings along with face object searching. The key for image encryption is a pseudo random number which is used for selecting different HSC curves so as to scramble an image.

(2) *Searching for the given face object hierarchically in the encrypted image and locate it.* We conduct hierarchically search on given encrypted images in multi-resolution. The features are extracted based on mean, variance and histogram which preserve the invariance of the encrypted image. This approach allows the face object to be scaled, rotated or having various lighting conditions in encrypted domain before the search.

(3) *Evaluating performance of face object search in encrypted domain.* In this paper, we take use of the Wild Face Dataset for our experiments. The precision

and recall as well as F-measure will be taken into consideration for the search evaluations.

The challenges of this work are to find the given face in encrypted domain hierarchically, there may have many faces within a given image. Our goal in all the cases is to find each face and mark it using a rectangle. The rest of this paper is organized as follows. The related work will be introduced in Section 2, our contributions will be presented in Section 3, Section 4 will provide the experimental results and analysis, conclusion and future work will be stated in Section 5.

2 Related Work

With regard to search in encrypted domain, usually lexical features and quantitative features as well as security-specific features are employed for the purposes of confidentiality [15], the domain of these search is usually limited to text encryption. In order to fully utilize the outcomes, homomorphic encryption [8], Yaos Garbled circuits (GC) [19] and reuse of encrypted values [18] have been adapted for data encryption recently. [25][11][3]

Homomorphic encryption is a form of encryption that allows computations to be carried out on ciphertexts. A cryptosystem is said to be homomorphic with respect to an operation $\star$, if another operation $\circ$ exists such that, given two plaintexts m_1 and m_2,

$$D(E[m_1] \circ E[m_2]) = m_1 \star m_2 \tag{1}$$

where D and E indicate the decryption and encryption operators respectively. If the function of operation $\star$ is identical to that of the operation $\circ$, the homomorphic encryption satisfies,

$$D(f(E[m])) = D(E(f[m])) = f[m] \tag{2}$$

From functional viewpoint, we have,

$$D(f(E[\cdot])) = D(E(f[\cdot])) = f[\cdot] \tag{3}$$

Namely,

$$D(f(E)) = D(E(f)) = f \tag{4}$$

This indicates the operators f and E are commutative in the encrypted domain.

The homomorphic encryption is possible to be propagated to other media such as image or picture, even audio and video. Based on the prevalent image encryption methods such as Hilberts Space-filling Curves (HSC) based scrambling, the encryptions are able to be iteratively applied to the encrypted images by following the same type of encryption while properties of the homomorphic encryption are still persevered. In this paper, we will take advantage of the HSC

based image scrambling as the encryption algorithm and assert the validity of homomorphic encryption in image encrypted domain.

The HSC is with a fractal structure generated by a recursive production rule which has the property of self-similarity and satisfies IFS system, its dimension is a fraction and it is supported by the fixed-point theory. After several rounds of recursions started from the fractal generator, the curve will fill up a given space recursively. If the curve space comprises of raster grids, the curve is utilized for re-ordering each pixel within the discrete space along the pixel order on the curve.

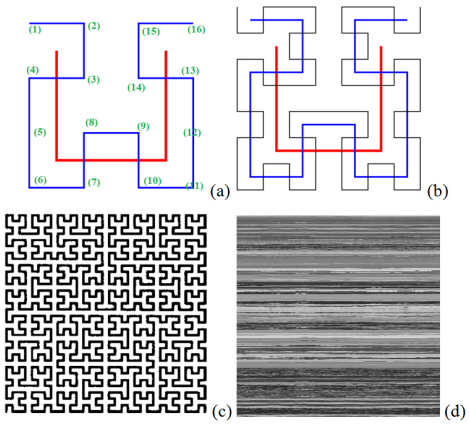

Fig. 2. Generating a HSC curve (a) Fractal generator (b) Generated HSC curve using recursion at resolution 8×8 (c) Generated HSC curve at resolution of 32×32 (d) Scrambled image based on the HSC curve (512×512) in spatial domain.

Generating procedure of a HSC curve is described as Figure 2(a). In figure 2(a), all the pixels on this plane along the HSC curve have been numbered. Figure 2(b) and (c) show the curves at resolutions 8×8 and 32×32 respectively. Figure 2 (d) shows a scrambled image of the Lena (512×512) in spatial domain using the 512×512 HSC curve. In a scrambled image, only the pixel locations have been re-ordered, the pixel color information still holds.

Our contribution in this paper is to search for a given face object in encrypted domain. Amongst the existing work, most of them are related to keyword search, this is based on plaintext encryption and ciphertext decryption in the encrypted domain which was derivative from the traditional cryptography.

In face recognition, eigenvalues and eigenvectors are calculated directly from the encrypted images [7] which is based on traditional PCA algorithm. Eigenfaces based recognition algorithm and a combination of known cryptographic techniques, in particular Homomorphic Encryption and Garbled Circuits (GC) have been employed to improve the computational complexity and server client communications [25].

Holomorphic properties of Paillier Cryptosystem specially for Euclidean distance has been used to calculate the distance between two feature vectors. In Paillier Cryptosystem,

$$[|m_1 + m_2|] = [|m_1|][|m_2|] \tag{5}$$

$$[|\alpha \cdot m|] = [|m|]^{\alpha} \tag{6}$$

Different from those existing work, in this paper our focus is on face object search in encrypted domain. The novelty of this paper lies in that the encryption of digital images is conducted via image scrambling based on the HSC curves; we select mean, variance and histogram as our features and compose them into a feature vector, the distance between feature vectors is calculated by using inner or dot product. We search for the given object in the encrypted domain and evaluate our search results by using precision and recall as well as F-measure.

3 Our Contributions

In image encryption and decryption as well as visual object search, we transform an image from spatial domain to DCT domain first and utilize the DCT coefficients for encryption and decryption. After these operations, we commit inverse DCT / IDCT transforms and transfer the image blocks back to spatial domain for the purpose of displaying. Therefore, in this paper we deal with the DCT transform as our pre-processing, our encryption and decryption are block based scrambling and descrambling. The steps of image search in encryption domain based on HSC curves scrambling are described as below,

Algorithm. Search a given face object in encrypted domain

```
Input: Face image F and image I
Output: Face location in the encrypted image
Step 1. Segment images F and I into the identical size blocks.
Step 2. Use DCT transform on these blocks.
Step 3. Use pseudo random number to select a HSC curve
        for the scrambling
Step 4. Extract the features (mean, variance and histogram)
        from the encrypted image and combine them into a vector
Step 5. Search encrypted image F on encrypted image I by
        calculating the distance between the encrypted F
        and sliding window of I hierarchically
Step 6. Calculate the precision, recall and F-measure for evaluating
        the search results.
```

3.1 Image Encryptions

In this section, we elucidate how digital images are encrypted using HSC curves based image scrambling, we manage the algorithm to serve image encryption and decryption well by adaptively tuning the parameters.

Procedure. As shown in the algorithm, in image encryption we import images in spatial domain and segment them into blocks having identical size, for each block we recursively generate a corresponding HSC curve using the generator presented in Figure 2(a), the curve starts from very beginning shown in red color, its mouth points in upward.

In the second iteration, for each turning point at start or end, we generate the same shape however the size and orientation will be changed. At the starting point, we rotate the generator for 90 degrees toward the left (anti-clockwise); at the end point, we turn the generator to right for 90 degrees (clockwise), at the other two turning points, the orientations of the generators are the same. We link these generated shapes together and yield the blue curve in Figure 2(a).

We repeat this step and acquire the black curve shown in Figure 2(b). If the end resolution is 32×32, we take use of the same way to generate Figure 2(c). The procedure is described as eq.(7),

$$p_{n+1}(x, y) = HSC(p_n(x, y)), n = 1, 2, \cdots \tag{7}$$

where HSC$(\cdot)$ is the iterative function, $p(x, y)$ is the turning point on the curve, the stop condition for this recursion is the final resolution reached so as to fully fill the given plane, the Hausdorff dimension of this fractal curve is 2.00. [17] The image scrambling procedure is described as,

$$I' = HSC(I) \ mod \ W \tag{8}$$

where I is the previous image without scrambling, I' is the scrambled image, W is the image width. After generated this HSC curve, we sort the pixel order according to the pixel sequence on the HSC curve shown as eq.(8). The eq.(8) first converts points on 2D plane to 1D curve order, then the 1D sequence will be used to fill up the image space line by line from top to bottom, consequently the image is fully scrambled shown as Figure 2(d) which is exported as the encrypted image.

Figure 3 shows the scrambled images of Lena in different resolutions of the HSC curves. In Fig. 3(a), we scramble each 16×16 image blocks in DCT domain using the generated 16×16 HSC curve, Fig. 3(b) is based on 32×32 blocks meanwhile the Fig 3(c) is based on 64×64 blocks of image scrambling. From our observations, we find that Lena's faces are gradually becoming tougher to be perceived from left to right. From the trade-off perspective, this means that it will be much harder to find a face from Fig. 3(c) than from Fig. 3(a).

The encryption using HSC based image scrambling in DCT domain changes the pixel sequence spatially, but does not alter color information of image pixels. Figure 3 shows one of results of image scrambling using the HSC curves based image scrambling in DCT domain with different resolutions.

Security. The security of this encryption is ensured by the key and the scrambling algorithm. This is because the HSC generator has multiple choices, and could be rotated along the clockwise and anti-clockwise directions, the generator has four orientations. Based on different generators, the HSC curves will be

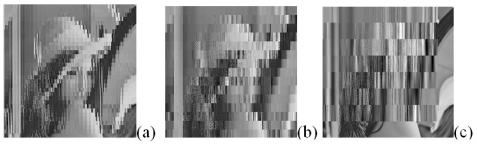

Fig. 3. Image encryption for Lena (512×512) in DCT domain using HSC for the blocks with different size (a) block size: 16×16 (b) block size: 32×32 (c) block size: 64×64

completely different. Meanwhile, the image block has multiple choices with various resolutions, the scrambling based on different block sizes will lead to image encryption with different strengths. Larger the bock size, stronger the encryption. Therefore, which HSC curve will be selected at what resolution will be the unique key of the encryption algorithm.

The HSC based image scrambling is different from the traditional encryption algorithms such as RSA, ECC and secret sharing, etc. The reason is that the scrambling completely destroys the order of pixel locations in the image, therefore the pixel neighborhood operations such as edge extraction, SIFT and others, are not possible anymore, especially in the DCT domain. However these geometric information could be detected from those encrypted images using RSA or ECC algorithms sometimes.

3.2 Face Object Search

In this section, we search for a given face object in encrypted domain. Our goal is to find the matched coefficients of the given face object in DCT domain after encryption. Therefore, we seek the face object using a sliding window. We keep the encrypted image at its given size but vary the face object size in a hierarchical multi-resolution search.

The window is initially defined for one face image size. For each window, we traverse the input image completely in scanline order from top to bottom and left to right, calculate the distance between feature vectors of the face image and regions of the encrypted image. When arriving the right-bottom corner of the image, we modify the face image size and search it starting from the left-up corner again, till scanned all sizes of encrypted face image, the procedure is shown as Fig. 4.

Feature Selection. Since the images have been encrypted based on DCT domain, the features are used for searching in encryption domain including mean, variance, entropy, etc. The visual features therefore are combined such as eq.(9) and eq. (10),

$$V_O = [f_{O1} \quad f_{O2} \quad \cdots \quad f_{Om}] \tag{9}$$

$$V_\Omega = [f_{\Omega 1} \quad f_{\Omega 2} \quad \cdots \quad f_{\Omega m}] \tag{10}$$

where V_O and V_Ω are the relevant features from face object O and sliding window Ω.

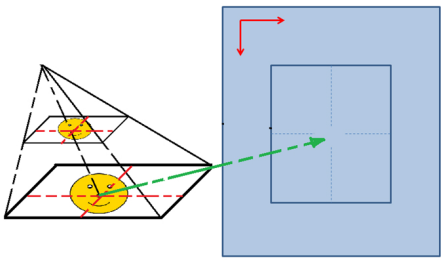

Fig. 4. Sliding windows search for a face object

Distance Calculation. The feature vectors are employed for the face object search, equation for calculating the distance between feature vectors is shown in eq.(11) and eq.(12) which are applied to the cases having invariance in encrypted domain such as rotating, scaling and filliping. After histogram equalization, it is able to be applied to the images having various lighting conditions,

$$\Omega = \arg\min_{\Omega}\{|V_{\Omega}(f_1, f_2, \cdots, f_m) - V_O(f_1, f_2, \cdots, f_m)|\} \tag{11}$$

where I_O is the image having face object, V_O is its feature vector; I_Ω is sliding window of the encrypted image for searching, its feature vector is V_Ω. What we like to emphasize in this paper is that the histograms, means and variances are all normalized.

$$\Omega = \arg\max_{\Omega} \frac{V_O(f_1, f_2, \cdots, f_m) \cdot V_{\Omega}(f_1, f_2, \cdots, f_m)}{|V_O(f_1, f_2, \cdots, f_m)| \cdot |V_{\Omega}(f_1, f_2, \cdots, f_m)|} \tag{12}$$

For an example, we search the given object in encrypted domain by using the inner or dot product between two feature vectors first shown as eq.(12); later we calculate the EMD (Earth Movers Distance) shown as eq.(13), which is used to refine the image distance for the search in encrypted domain [24].

$$\Omega = \arg\min_{\Omega} EMD(O, \Omega) = \arg\min_{\Omega} \frac{\Sigma_i \Sigma_j d_O(i,j) d_{\Omega}(i,j)}{\min(\Sigma_i w_{pi}, \Sigma_j w_{qj})} \tag{13}$$

where $w_{pi} \geq \Sigma f(i,j)(m \geq i \geq 1)$ and $w_{qj} \geq \Sigma f(i,j)(n \geq j \geq 1)$, $f(i,j) \geq 0$, $d(i,j) \geq 0$.

Multi-resolution Search. While conducting face search in encrypted domain, we have three down-sampling operations: original, half and quarter. The search results '1' or '0' will be merged together using 'or' operations. The finally found region will be generated by merging the detected regions in different resolution together.

3.3 Search Evaluations

In this section, we will detail on how to evaluate search results. Suppose an encrypted face object has been traversed from a large number of encrypted pictures. From the results, we need find true positive tp, true negative tn; false positive fp and false negative fn. Based on these parameters, we objectively evaluate our search by using precision, recall and F-measure.

In the context of this paper, when a face object is found, we usually refer to search region A and the image region B having intersection, $A \cap B \neq \emptyset$. The corresponding mathematical description is shown as eq. (14).

$$p = \frac{\Lambda(A \cap B)}{\Lambda(A \cup B)} \cdot 100\% \tag{14}$$

where $\Lambda(\cdot)$ is the area of the specific regions, $p \in [0, 1]$. Eq.(14) shows how many percent of the face image has been found in the search. If $A \cap B = \emptyset$, that means the search is a failure, we could not get the face object from this image, so $p = 0$.

After we have received the search results, we calculate the recall and precision as well as F-measure utilizing our ground truth. The ground truth tells us whether an image has the designated face or not, it is '0' or '1'. Our results reveal from multi-resolution viewpoint whether we have successfully found the face or not.

If the search results are known, we have,

$$Pr = \frac{Tp}{Tp + Fp} \tag{15}$$

$$Rc = \frac{Tp}{Tp + Fn} \tag{16}$$

where Pr And Rc refer to precision and recall, respectively. Tp, Fp, Fn, and Tn are the true positive, false positive, false negative and true negative in the search. The Tp, Fp, Fn, and Tn show amongst the search results how many search results reflect the ground truth exactly. Furthermore, F-measure is calculated by, Eq.(17),

$$F_m = 2 \cdot \frac{Pr \cdot Rc}{Pr + Rc} \tag{17}$$

4 Results and Analysis

We implement our search algorithm using Matlab platform and encrypted images in DCT domain. Our search results are shown in Fig. 5, Fig. 6 and Fig. 7 marked with red rectangles.

In Table 1, we encrypt the Lena 512×512 image in blocks using 4 resolutions of HSC curves (resolution 1: 8×8, resolution 2: 16×16, resolution 3: 32×32, resolution 4: 64×64). Table 1 shows that there is a trade-off between the quality of image encryption algorithm and the quality of search. The higher encryption

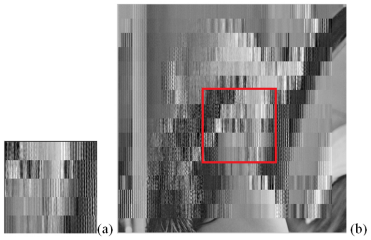

Fig. 5. Searching Lena's face on the scrambled images by using the HSC curve based scrambling (a) Lena's face (164×164) in encrypted domain using HSC scrambling after DCT transform; (b) Image Lena (512×512) in encrypted domain using HSC scrambling after DCT transform, the red rectangle shows the found region of the visual object.

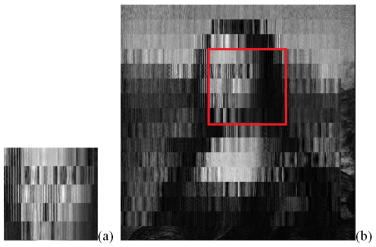

Fig. 6. Searching Mona Lisa's face on the scrambled images by using the HSC curve based scrambling (a) Mona Lisas face (164×164) in encrypted domain using HSC scrambling after DCT transform; (b) Image Mona lisa (512×512) in encrypted domain using HSC scrambling after DCT transform, the red rectangle shows the found region of the visual object.

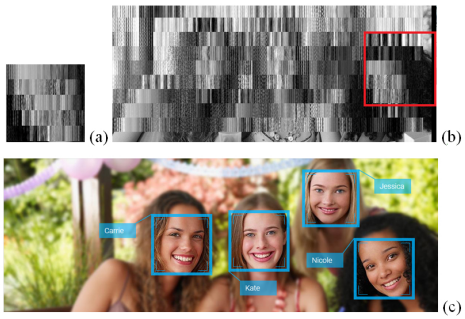

Fig. 7. Searching Nicole's face on the scrambled images by using the HSC curve based scrambling (a) Nicoles face (164×164) in encrypted domain using HSC scrambling after DCT transform; (b) Nicole (724×314) in encrypted domain using HSC scrambling after DCT transform, the red rectangle shows the found region of the visual object (c) Nicoles face on the original color image.

Table 1. Comparisons of HSC encryption in encrypted domain

Resolutions	Block Size	SSIM	DSSIM	NCC	EMD
Resolution 1	8×8	0.8227	0.0887	388.1511	0.9811
Resolution 2	16×16	0.8340	0.0830	480.3705	2.0861
Resolution 3	32×32	0.8618	0.0691	428.1592	3.2792
Resolution 4	64×64	0.8631	0.0685	907.2569	5.8470

that means the search is more difficult since the visual information has been scrambled using the HSC curves.

Table 2. Comparisons of search results after transforms

Transforms	SSIM	DSSIM	NCC	EMD
Scaling	0.8047	0.0977	42.9602	11.7442
Rotating	0.8407	0.0797	291.8372	8.1224
H-flipping	0.8394	0.0803	922.3983	1.9938
V-flipping	0.8805	0.0598	430.1192	2.4320

Table 2 shows search results that we use the Lena face images (512×512) after 4 Affine transformations (scaling, rotating, horizontal filliping, and vertical flipping). It discovers the scaling and flipping transforms did affect the search quality, but the rotating does not affect the result too much, this may be related to the fact that the image size is not changed too much.

Table 3. Comparisons of search results of various samples

Pictures	PSNR	SSIM	DSSIM	NCC	EMD
Lena	39.3324	0.8210	0.0895	518.8758	2.3660
Mona Lisa	39.8592	0.8353	0.0823	969.1637	1.4657
Nicola	39.3715	0.8241	0.0879	1578.1183	1.1955

Table 3 demonstrates what are the differences between the given human faces and found regions. We calculate the differences using the metrics SSIM(Structural similarity), DSSIM(Structural Dissimilarity), NCC (Normalized Cross Correlation) and EMD (The Earth Mover's Distanc).

Table 4 shows the corpus of our search related to famous figures. We search the given faces within the encrypted domain, and compare the found face location and the ground truth. From the results, we calculate precision and recall as well as F-measure.

We adopted the LFW Face Database as corpus for searching human faces in encrypted domain, the database of face photographs was designed for studying

Table 4. Face search in encrypted domain using the Wild dataset

Face Data	Samples	Precision	Recall	F-Measure
Putin	115	0.825	0.3548	0.4962
Agassi	115	0.722	0.2921	0.4629
Clinton	115	0.690	0.2020	0.3125

the problem of unconstrained face recognition. We select 3 figures with a total of 115 images for the algorithm testing (Putin: 40, Agassi: 36, Clinton: 29). The results are shown in Table 4. The precisions of our search are acceptable.

The corresponding images are shown in Figure 8, Figure 9 and Figure 10.

Fig. 8. Precision of face search in encrypted domain: 82.5% (Putin)

5 Conclusion

In this paper, we search for face objects in encrypted domain. The main purpose is to reuse the encrypted data and save the computation time by directly manipulating on the encrypted data. Our results show the superiority of face object search in encrypted domain. Our contributions are: 1) Image encryption using

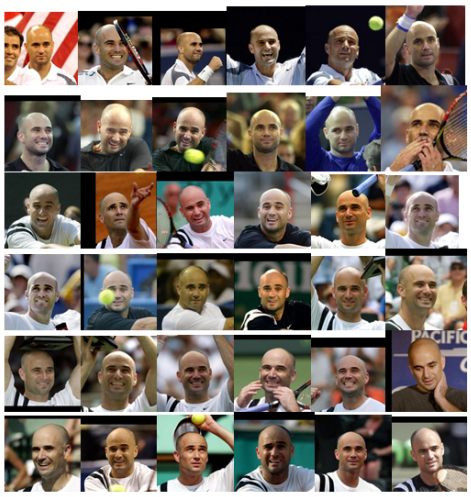

Fig. 9. Precision of face search in encrypted domain: 72.22% (Agassi)

Fig. 10. Precision of face search in encrypted domain: 69% (Clinton)

HSC based image scrambling; 2) Face object search within the given encrypted images; 3) Search evaluation in encrypted domain. In future, we will further investigate the relative issues in encrypted domain, especially for the security and privacy preservation problems in big data associated with social media.

References

1. Bianchi, T., Piva, A., and Barni, M.: Composite Signal Representation for Fast and Storage-Efficient Processing of Encrypted Signals. IEEE Transactions on Information Forensics and Security, 5, 1, 180– 187(2010)
2. Breinholt, G. and Schierz, C.: Algorithm 781: Generating Hilberts Space-Filling Curve by Recursion. ACM Transactions on Mathematical Software, 24, 2, 184–189 (1998)
3. Cao, N., Wang, C., Li, M. Ren, K., Lou, W.: Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data. IEEE Transactions on Parallel and Distributed Systems, 25, 1, 222–233 (2014)
4. Czajkowski, K., Fitzgerald, S., Foster, I., Kesselman, C.: Grid Information Services for Distributed Resource Sharing. In: 10th IEEE International Symposium on High Performance Distributed Computing, pp. 181–184. IEEE Press, New York (2001)
5. Cheon, J., Lee, H., and Seo, J.: A New Additive Homomorphic Encryption based on the co-ACD Problem. In: ACM CCS14, USA, pp. 287–298, ACM Press, USA (2014)
6. El-Deen, A., El-Badawy, E., Gobran, S.:Digital Image Encryption Based on RSA Algorithm. Journal of Electronics and Communication Engineering, 9, 1, 69–73 (2014)
7. Ergun, O. Q.: Privacy preserving face recognition in encrypted domain. In: IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), pp. 643–646 (2014)
8. Gentry, C.: A Fully Homomorphic Encryption Scheme. PhD Thesis, Stanford University. (2009)
9. Hsu, C. Y., Lu, C. S. and Pei, S. C.: Image Feature Extraction in Encrypted Domain With Privacy-Preserving SIFT. IEEE Transactions on Image Processing, 21(11): 4593–4607 (2012)
10. Iftene, S.: General Secret Sharing Based on the Chinese Remainder Theorem with Applications in e-Voting. Electronic Notes in Theoretical Computer Science 186, 67–84 (2007)
11. Kamara, S., Papamanthou, C., and Roeder, T.: Dynamic Searchable Symmetric Encryption. In: ACM CCS 12, USA, pp. 965–976. (2012)
12. Klette, R.: Concise Computer Vision. Springer, London. (2014)
13. Lia, L., Abd El-Latif, A., and Niu X.: Elliptic curve ElGamal based homomorphic image encryption scheme for sharing secret images. Signal Processing, 92, 4, 1069–1078 (2011)
14. Lathey, A. and Atrey, P. K.: Image enhancement in encrypted domain over cloud. ACM Transactions on Multimedia Computing, Communications and Applications, 11, 3. (2015)
15. Lu, L., Perdisci, R., and Lee, W.: SURF: Detecting and Measuring Search Poisoning. In: ACM CCS11, USA, pp. 467–476 (2011)
16. Lu, W., Swaminathan, A., Varna, A., and Wu, M.: Enabling Search over Encrypted Multimedia Databases. In: Proc. of SPIE 7254, Media Forensics and Security (2009)

17. Matias, Y., and Shamir, A.: A video scrambling technique based on space filling curves. In: Advances in Cryptology (CRYPTO 87), pp. 398–416 (1988)
18. Mood, B., Gupta, D., Butler, K., Feigenbaum, J.: Reuse It Or Lose It: More Efficient Secure Computation Through Reuse of Encrypted Values. In: ACM CCS14, USA, pp. 282–296 (2014)
19. Naveed, M., Agrawal, S.Prabhakaran1, M. Wang, X., Ayday, E., Hubaux, J., and Gunter, C.: Controlled Functional Encryption. In: ACM CCS14, USA, pp. 1280–1291 (2014)
20. Naor, M., Shamir, A.: Visual cryptography. In: Advances in Cryptology (EUROCRYPT'94), pp. 1–12. Springer Berlin Heidelberg (1995)
21. Qin, Z., Yan, J., Ren, K., Chen, C. W., and Wang, C.: Towards Efficient Privacy-preserving Image Feature Extraction in Cloud Computing. In: ACM MM14, Orlando, Florida, USA (2014)
22. Rahulamathavan, Y., Phan, R., Jonathon, A., Parish, D.: Facial Expression Recognition in the Encrypted Domain Based on Local Fisher Discriminant Analysis. IEEE Transactions on Affective Computing, 4, 1, 83–92 (2013)
23. Rouselakis, Y., and Waters. B.: Practical Constructions and New Proof Methods for Large Universe Attribute-Based Encryption. In: ACM CCS13, Germany, pp. 463–474 (2013)
24. Rubner, Y., Tomasi, C., Guibas. L.: The Earth Mover's Distance as a Metric for Image Retrieval. International Journal of Computer Vision, 40, 2, 99–121 (2000)
25. Sadeghi, A., Schneider, T., Wehrenberg, I.: Efficient privacy-preserving face recognition. In: International Conference on Information Security and Cryptology, pp. 229–244 (2009)
26. Shyu, S.J. and Chen, Y. R.: Threshold secret image sharing by Chinese Remainder Theorem. In: IEEE Asia-Pacific Services Computing Conference, pp. 1332–1337 (2008)
27. Suresh, V. and Madhavan, C.: Image Encryption with Space-filling Curves. Defence Science, 62, 1, 46–50 (2012)
28. Song, X., Wagner, D., and Perrig, A.: Practical techniques for searches on encrypted data. IEEE Symposium on Security and Privacy, pp. 44–55 (2000)
29. Wang, G., Liu, Q., and Wu, J.: Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services. ACM CCS10, USA, pp. 735–737 (2010)
30. Wong, W., Cheung, D., Kao, B., Mamoulis, N.: Secure $k - NN$ computation on encrypted databases. In: ACM International Conference on Management of data, pp. 139–152 (2009)