Private Searching on Encrypted Data in Cloud

Huda M. Saleh
Department of Computer Science, College of Science, university of Basra, IRAQ

Hameed A. Younis
Department of Computer Science, College of Science, University of Basra, IRAQ

ABSTRACT
Cloud computing appeared as the most common paradigm in the time being that provides calculations and storage resources by when used – pay method. Users can exploit cloud resources from anywhere at any time without maintenance cost. Flexibility in resource allocation enabled cloud services to be effective in delivering with reasonable cost. However, transfer data to cloud make it vulnerable to leakage, and loss of privacy. Therefore, data security in cloud considered as the primary hurdle of cloud adoption. Many users prefer prior protection for their data using data encryption, which determine cloud popularity, since most searches process are not carry out on encrypted data directly. This paper build secure and effective system for searching over encrypted images in cloud environment and propose public-key image encryption algorithm from RSA and Paillier algorithms. The proposed image encryption algorithm achieved higher security and appropriate processing time, which evaluated by PSNR, Entropy, NPCR, UACI and processing time. We used Scale Invariant Feature Transform algorithm (SIFT) algorithm for image feature extraction, locality sensitive hashing (LSH) to secure sensitive images and build index, and Eculidean distance as similarity metric.

General Terms
Information Security, cloud computing

Keywords
Cloud Computing, RSA, Paillier, Searchable Encryption, LSH, SIFT

1. INTRODUCTION
Cloud computing paradigm is one of the biggest attractions taking us to the era of new technologies, and great prosperity business. It assists us to dealing with problems as data loosing, and data accessing [1]. The term "cloud", derived from cloud symbol that used to explain the Internet graphs [2]. National Institute of Standard and Technology (NIST) defined Cloud computing as "model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or services provider interaction". This paradigm includes five major characteristics : On-demand self service, broad network access, resource pooling, rapid elasticity, and measured services, three service models: Software as a service (SaaS), Platform as a service (PaaS), and infrastructure as a service (IaaS), and four deployment models: Private cloud, public cloud, community cloud, and hybrid cloud [3]. Virtualization considered as the main driver in cloud paradigm. It provides virtual storage and services to customers that is unthinkable only by virtual technology. Eessentially, it produces virtual image of operating system, devices, servers or network resources, utilized in various machines synchronously. Therefore, it is hardware decreasing, conserve cost and energy [1]. Not long ago, end users and enterprises move personal data, including images, sounds and video files from their PC to the remote servers (cloud storage) reached via a network [2]. The usefulness of cloud paradigm as easy management, cost reduction, uninterrupted services, disaster management, and green computing gave users and enterprises support and confidence to send their data to cloud. On the other hand, it brings big challenges in field of data security and privacy protection [4]. Security concept refers to a particular situation where all of the potential risks either eliminate or bring them to a minimum. In the traditional systems, through effective security rules have been impose security, which dealt with restrictions on procedures and flow between them, on software, and data access by people. In the cloud perimeter, this conception completely muddled, where assigned control to the infrastructure model. In the public cloud, the control is lessen to the owner of the infrastructure for the imposition adequate security policy to ensure that suitable security actions applied, then risk is minimal. This is not different in private model that managed by a private group. Consequent to architectural style and attributes of cloud computing, it impose number of security issues like centralized of security, availableness, data and operations partitioning, Generally, security linked to key aspects as confidentiality, integrity and availableness, which will be the basics of designing and building any safe system. These key aspects of security used on the seeds of system: Data, software and resources tools to be safe [2]. Sending important applications and data to cloud paradigm have a great significance for companies and people, but it is necessary for them to be sure that their data kept safe in every case and where it goes. Therefore, cloud service provider (CSP) in order to encourage them, make sure that clients will get the same security and privacy controls as their data centers do [5]. Because cloud service provider instead of the company or people commonly hosts cloud storage, and cloud infrastructure used by multi users, then data uploaded to the cloud exposed to insider and outsider attacks, especially effect on data privacy [6]. To maintain data privacy and prevent unwanted access, data owner should encrypt these data before submitting to the cloud server. In encryption process, the explicit data converted to non-readable data by anyone except authorized user who owns the decryption key, according to the key used, encryption either symmetric encryption (shared-key) one key used to encrypt and decrypt data, or asymmetric (public-key) where used two different keys one for encryption data and the other for decryption [7]. Encryption achieve confidentiality, integrity and availability for any system but at the same time, reduce the search capabilities, especially in the cloud environment since cloud server (untrusted party) perform search process instead of users. It is not practical for users to download all the encrypted data, and decrypt it before searching process. Therefore, companies and individuals who wished to enjoy cloud services and decrease expenditure should build efficient system able to protect data privacy stored in remote servers and maintain search capabilities.

Many schemes built to make search on encrypted data possible, Kuzu M., et.al. [8] Proposed an effective scheme for similarity searchable symmetric encryption in high dimensional spaces, used locality sensitive hashing (LSH) algorithm to secure sensitive data and build index, Jaccard distance as similarity metric and Advanced Encryption Standard (AES) in CTR (Counter Mode) for data encryption. Xia Z., et al. [9] proposed scheme for similarity searching using secure transformation method to protect the confidentiality of images database, histogram for features extraction then used to build inverted index, which outsourced along with the encrypted images to cloud server. The scheme suffered from statistic attacks and required O(n) time complexity. Zhu Y., et.al. [10] Proposed an effective scheme for searching on encrypted cloud images. Used p-stable LSH algorithm for index building by extract global features from images database, under Euclidean metric. LSH enables efficient similarity image search and less time consuming compared to direct search scheme. Hwang R. J., et.al. [11] Present a system model comprising a cloud user and a cloud server. Scheme support ranked multi-keyword search, which tolerate queries involving incorrect keywords. Used ranked function to evaluate the correlation between a keyword and a specific file. This paper focuses on achieving data security in cloud environment by proposing encryption algorithm to encrypt images in terms of strength and time it takes to encrypt and decrypt images. Consequently, convince users to upload their sensitive images to cloud servers and exploit the economic benefits of cloud computing by providing high level of security for their data; reduce effort on users by assigning all searching processes to cloud server, then used appropriate technique for searching on encrypted data without influencing on searching time and results. This paper summarized as follow: Section II describes framework background. Section III present the problem statement. Section IV present the proposed scheme. Section V gives the experimental results of the proposed scheme, and finally, Section VI gives conclusions.

2. FRAMEWORK BACKGROUND

2.1 Public-key Algorithm

Before discovering public key cryptography, ensured path was only way for users to concur on a secret key. In 1967, Diffie and Hellman [12] completely changed secret key agreement over public channel, they use multiplicative group of integers modulo p (integer number) and a generator g (integer number) for key exchange protocol. Public-key algorithms depend on two keys, which are different from each other, but related mathematically, one for encryption and the other for decryption [7]. Knowing encryption algorithm and the public key not lead to deduce the private key. Public key algorithms owns six basic components, Plaintext (M) the original data. Encryption algorithm (E): Sequential procedures to transform plaintext to unclear text. Public and private keys: Pair of keys already selected one for encryption, which published to other users and second kept secret for decryption. Cipher text (C): Unclear message created as output of (E) algorithm that transmitted over insecure channel. In addition, Decryption algorithm (D): Recover the plaintext (M) using private key and ciphertext (C).

RSA Algorithm: In 1977, Rivest R. L., Shamir A., & Adleman (RSA) [13], proved that the announcement of the encryption-key does not lead to the decryption key disclosure. This led to the creation of new encryption method called RSA cryptosystem, which utilized computation in $\mathbb{Z}^*n$. RSA security depend on decomposition n to its factors ($n=p\times q$). Factoring n by adversary, will be able to getting Ø(n) and d, thus, breaking system. The current factoring algorithms capable of analyzing the numbers that length of more than 512 bits, choosing both p and q must have at least 512 bits length, so, n=1024 bits, factoring this number appears very difficult. Before the encryption and decryption procedures, the sender and receiver should generate their key pairs (public, private).

Paillier Algorithm: In 1999, Paillier P. [14], tested new computation problem based on "composite residuosity class" known as Paillier cryptosystem, which considered randomizing asymmetric algorithm for public-key cryptography. The security of Paillier cryptosystem based on the difficulty of discrimination nth-residues modulo n2 from non-nth-residues, since the rigidness of the computational problem of determine nth-residues is extremely powerful than factorization problem for RSA algorithm. Before the encryption and decryption, the sender should generate key pairs (public, private).

2.2 Searchable Encryption (SE)

In 2000, Song et.al [15] proposed the first general model of Searchable encryption (SE), as a technique for searching on encrypted data stored in remote untrusted server, server performs searching and sending search results to the user in encryption form without any leakage of original data. SE is safe; keep planned search and query segregation, straightforward and high speed. Information retrieval is one of the more frequent services provided by the network. All network users have already searching for specific words in Google drive, amazon or any search engine, after typing keywords. Google will retrieve results related to search words. All of these actions carried out on the plaintext, and then any attacker can easily learn search data and search results. If the research data have private and important information for user, user's privacy had penetrated. To solve this security issue, Song searchable encryption introduces as cryptosystem whose cipher text is searchable. It composed of three objects, cloud server provider ('CSP'), person owns data (data owner 'DO'), and person use data (data user 'DU'). DO encrypt the data files and uploading them to the cloud server, DU have search request and want to acquire results from CSP, and CSP stores the data uploaded by DO and perform the searching algorithm, then send search results to data user, as explain in Figure (1) [16].

Index is the main component in searchable encryption, which built on original data. Build secure index able to search quickly for the required data and ensures the security requirements as data privacy, search pattern and access pattern is a very important task for data owner, because perfect construction of index significantly reduces search complication, thus increase search effectiveness [15, 17].

Fig 1: Searchable Encryption Basic Entities

The Nearest Neighbor Search (NNS) or similarity search is very important in several fields as "image and video databases", "information retrieval", and "data mining"...etc. NNS include set of objects (database) that can described by a group of features in $\Re d$, a distance metric used to measure similarity of query object and database objects. In image retrieval application, image assign into high dimensional feature vectors. To avoid obstacle of searching in high-dimensional space problem, results of c-Approximate Nearest Neighbor search (c-ANN) considered very close as the exact search. c-ANN search problem, include set of points p within $\Re d$ d-dimensional space, to inquire about a given point q, and an approximation ratio c>one, the c-ANN search build a data structure which finds points closest to q, in distance more than the distance from q to p, that equivalent to c.

LSH: Locality-Sensitive Hashing is the approximation version of the NN search, which based on hashing, give answer with height likelihood that it right answer or near to it instead of exact answer. Underlying principles of LSH algorithm, for any two points, the chance of collision, is tightly linked to the distance among them, large distance means low collision probability and vis versa. LSH index database by employ group of hash functions to map database objects into several buckets [18, 9, 19, and 20].

2.3 Content based Image Retrieval (CBIR)

Is a technique for searching of digital images in a large database based on the content or features of the images instead of the descriptions associated as keyword and tags. CBIR system include many methods at different levels of indexing and retrieval, the most difficult task is feature extraction [21, 22].

SIFT: Scale Invariant Feature Transform algorithm is a greatly used algorithm for feature extraction in computer vision, since it detects and extracts features of an image in a steady way regardless of image "rotation, scaling, illumination and camera viewpoint". In addition, the individual feature give correct matching against large database of features, detect the same points despite changes in viewing conditions, close to real time performance and can generate many features from even small object. SIFT takes (N×N) image as input and produce (1×128) features vector. SIFT converts image data into local features through four important procedures: "Scale-space extrema detection, keypoints localization, orientation assignment, and keypoints descriptor" [23, 24].

3. PROBLEM STATEMENT

Searching on encrypted data stored in cloud include three basic components, which works together:

1. Data owner *DO* have *n* number of images D_{Img} = {Img_1, Img_2,…, Img_n} that he want to send to CS. To keep image privacy, *DO* should : Encrypt all images, ED_{Img} = Encryption (D_{Img}, key), extract features from images, FeD_{Img} = feature extraction algorithm (D_{Img}), and build index from images features I= Build index (FeD_{Img}), then send encrypted images (ED_{Img}) and index (I) to cloud server.
2. Data user *DU* authorized user, have query image and ask cloud server to search in *DO* database and retrieve similar images to his query image, he should extract features from query image (q), f_q = feature extraction algorithm(q), generate trapdoor TD(f_q), and send TD(f_q) to cloud server.

Cloud server *CS* accurately track the particular procedures. At the same time, try to know additional information about the images received, it consider" honest but curious". *CS* should store encrypted images and index from data owner, start searching in index, when received TD(f_q) from data user, and compare query vector fq with the items in index and return k number of nearest images in encrypted form to data user. Data user can use the retrieved image after decryption.

Each of these three components have responsibilities to ensure security.

4. PROPOSED SCHEME FOR SEARCHING ON ENCRYPTED IMAGES IN CLOUD

The proposed scheme consist of three components: Data owner (DO), Cloud Server (CS), and Data User (DU) and three phases: The uploading phase, querying phase, and search and retrieve phase. Figure (2) and Figure (3) shows the proposed scheme components and phases, which explain the key steps for each phase. First phase include four steps:

Fig 1: If Necessary, the Images can be Extended both Columns

Key generation, images encryption, feature extraction, building secure index and sending (encrypted images and index) to the CS. The second phase consist of three steps: feature extraction from query image, trapdoor generation, and then, sending it to the CS. The third phase have three steps: index searching, retrieve similar images in encrypted form and, sending back to the DU. Figure, (3) explain the whole steps of the proposed scheme. We suppose using private cloud in our proposed scheme, which provide easy management, maintenance and update. Private cloud designed to serve a single organization include a specific number of users. DO in private cloud, is the only one who knows the original data, therefore can determine security level for data.

Uploading phase	Querying phase by (DU)	Search and Retrieve phase by (CS)
1-Key-generation	1-Query image Feature extraction	1-Index searching
2-Image	2-Trapdoor Generation Vq	Retrieve similar images
3-Feature extraction		
4-Index	3-Send (Vq) to CS	2-Send to DU
5-Send encrypted images and		

Fig 3: Main Phases of the Proposed Scheme

1. The Uploading Phase by DO

Data owner have database, set of images, and wants to outsource them to CS, The uploading phase encompass of four steps: key generation, image encryption using proposed image encryption algorithm, feature extraction using scale invariant feature transform (SIFT), and build secure index using Locality sensitive hashing (LSH). Then send encrypted images and index to CS. DO send output of Algorithm (2) and Algorithm (4) to CS.

Algorithm (1): Keys-Generation

Input: Select randomly two primes, great size, different values, p and q, which kept secret.

- Compute RSA public-key (e) and RSA private key (d).
- Compute Paillier public-key (g) and Paillier private key (μ).
- Compute secret matrix M (129×129).

Algorithm (2): Images encryption

Input: Original image (I_{mg}).

- Select pixels to encrypt using RSA.
- Select pixels to encrypt using Paillier.
- Output: Cipher image (C).

Algorithm (3): Feature extraction.

Input: Original image (Img).

Output: Feature vector (1×128) of input image.

Algorithm (4): Index building.

Input: Matrix of images features vectors.

Output: Index (I).

2. The Querying Phase by DU

DU is an authorized user want to search in database and retrieve images similar to his query image, the querying phase encompass of two steps: query feature extraction, query trapdoor generation. *DU* used SIFT algorithm to extract feature vector of his image, then send query trapdoor (Tq) to *CS*.

Algorithm (5): Trapdoor Generation

- Input: Query image q. Extract feature vector from query image using Algorithm (3).
- Extend to (1×129), using random value [0, 1].
- Multiply with inverse matrix (M×M).

Output: Query trapdoor (Tq).

3. The Search and Retrieve Phase by *CS*

CS responsible of searching in index (I) and retrieve similar images to *DU* query image in encrypted form. This phase have three steps: searching in index, retrieve similar image and send back to *DU* without knowing any information about the query image or retrieved images since it in encrypted form. *CS* used LSH algorithm for searching process, when received *DU* trapdoor.

Algorithm (6): Searching in index (I)

Input: Query trapdoor (Tq).

- Mapping Tq to index (I) buckets.
- Find common buckets in index (I).
- Compute Euclidean distance (buckets of (I), Tq buckets).
- Send encrypted images to DU.

Output: k similar images in encrypted form.

4. The Decryption of Retrieved Images by *DU*

DU received k similar images from CS in encrypted form. In order to be used. It must be decrypted using proposed image decryption algorithm. Since *DU* consider authorized user, *DO* can send decryption keys.

Algorithm (7): Image decryption

Input: Encrypted image (C).

- Select pixels to decrypt using RSA.
- Select pixels to decrypt using Paillier.

Output: Original image (I_{mg}).

5. EXPERIMENTAL RESULTS

This section present the experimental results of the proposed scheme using new image encryption algorithm. We used database of GroundTruth image database [25], contain 1000 color images in jpg format, which converted to gray level with (256×256). The framework of the research designed by MATLAB R2015a software in 64 -bit system with 2.40 GHz core i5 processor and 8 GB of RAM, run with MS Windows 10 operating system.

5.1 Encryption Results

The heading of subsections should be in Times New Roman 12-point bold with only the initial letters capitalized. (Note: For subsections and subsubsections, a word like *the* or *a* is not capitalized unless it is the first word of the header.)

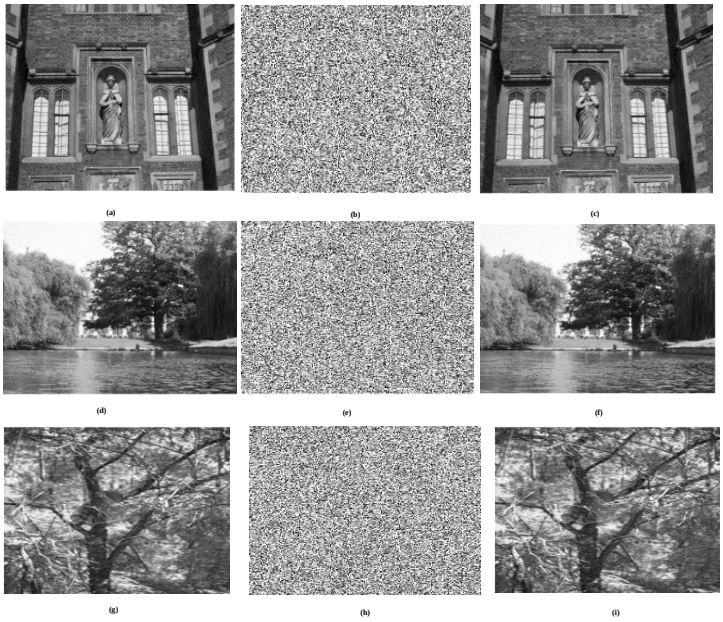

Fig 4: (a), (d), (g) original images; (b), (e), (h) Encrypted images using proposed algorithm; (c), (f), (i) Decrypted Images, Respectively

Security Analysis We evaluate the performance of the proposed image encryption algorithm according to [26, 27, and 28]:

1. Gray Histogram Analysis: Refer to the pixel intensity values that can reflect the distribution of pixel information. Figure (5b) shows the histogram of original image and, Figure (5c) shows the histogram of cipher image. We can see the histogram of cipher image shows linearly distributed of pixel values. This make difficult for attackers to deduce useful information.

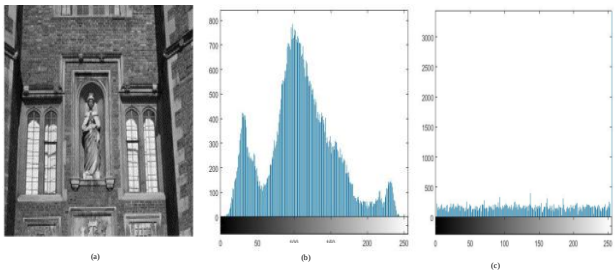

Fig 5: (a) Original Image; (b) Histogram of Image (a); (c) Histogram of Cipher Image using Proposed Encryption Algorithm

2. Entropy Analysis: Gives idea about real information. The concept of entropy is very important for analyzing an encryption scheme. The ideal entropy for original image with 256 gray level is eight. If entropy is less than eight, then there exists a certain degree of predictability. For cryptosystem to resist the entropy attacks, the entropy value should close to ideal value. The entropy, H(m) of source can be calculated as:

$$H(m) = \sum_{i=0}^{2^N-1} p(mi) \times \log 2 \frac{1}{p(mi)} \quad (1)$$

p(mi): The probability of symbol *mi*.

Table 1. Results of Information Entropy Analysis

Entropy	Images 1	Images 2	Images 3
Plain	7.4609	7.5859	7.5580
Cipher	6.1473	6.1499	6.1545

3. Peak Signal-to-Noise Ratio (PSNR): The term PSNR indicate the ratio between the maximum possible value of a signal and the power of distortion noise that effects the quality of it is representation, which used to evaluate an encryption scheme. It is a measurement of changes in pixel values between original image and the encrypted image. The lower value of PSNR represents better encryption quality.

$$PSNR = 10 \times \log 10 \left[\frac{M \times N \times 255^2}{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (P(i,j) - C(i,j))2}\right] \quad (2)$$

M: width of digital image.
N: height of digital image.

P (i, j) is pixel value of the original image.

C (i, j) is pixel value of the cipher image.

Table 2. Results of PSNR Analysis

PSNR (dB)	Image3	Image2	Image1
(original image, cipher image)	7.5282	6.9395	7.0194
(original image, retrieved image)	Inf.	Inf.	Inf.

4. Number of Pixel Change rate (NPCR) and Unified average Changing Intensity (UACI) can used to describe the ability to resist the differential attack. A secure image encryption must be sensitive to the original image change; any small change in an original image pixel can cause big change in cipher image. The ideal values of NPCR and UACI, are 99.61% and 33.46%, respectively.

Table 3. Results of NPCR and UACI for Cipher Image

	Image1	Image2	Image3
NPCR	0.9322	0.9292	0.9258
UACI	0.3739	0.3690	0.3519

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%$$

$$UACI = \frac{1}{M \times N}\left[\sum_{i,j} \frac{|C(i,j) - c`(i,j)|}{255}\right] \times 100\%$$

M: Width of image, N: Height of image.

C (i, j) and C`(i, j) are the corresponding pixels of two images.

If C (i, j) = C`(i, j), then D(i, j) = 0, otherwise D(i, j) = 1.

5. Time for Encryption and Decryption: The time needed by algorithm (measured in seconds) for complete the encryption and decryption steps is important measure to evaluate the encryption algorithm. It is supposed to be short time especially in the decryption steps by DU.

Table 4. Processing Time to Encrypt and Decrypt Images

Time for Encryption and Decryption(Sec)	**Image**2	**Image**2	**Image**1
	397.1405	344.3505	208.2161

Compared PSNR, entropy, and processing time of proposed image encryption algorithm with RSA and Paillier algorithms.

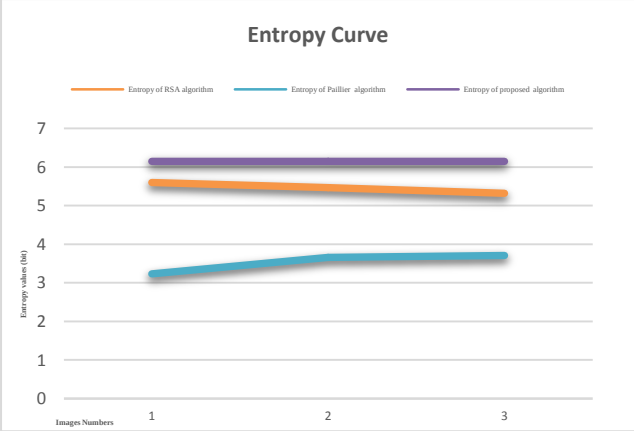

Fig 6. Entropy curve of algorithms RSA, Paillier, and the proposed image encryption algorithm

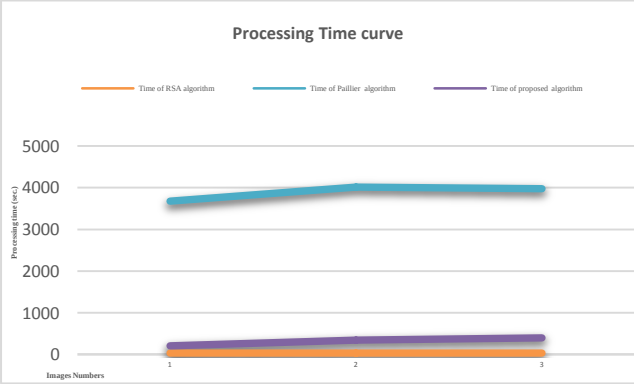

Fig 7. PSNR Curve of algorithms RSA, Paillier, and the Proposed Image Encryption Algorithm

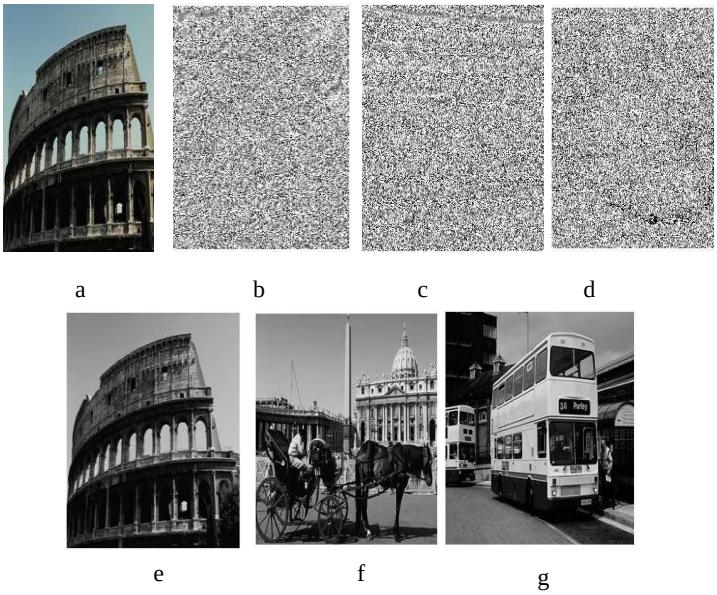

Figure 8. Processing time of algorithms RSA, Paillier, and the proposed image encryption algorithm

6. CONCLUSIONS

In this paper, we address and solve the problem of searching on encrypted images in cloud environment with preserving images privacy, by proposed image encryption algorithm based on two public-key algorithms, RSA, and Paillier. The proposed algorithm combine RSA fast encryption and Paillier strength encryption, through select specific pixels from original image according to data owner precondition. The speed of encryption algorithm is significant criterion of any system especially in real time application. Time to encrypt and decrypt one image by proposed image encryption algorithm consider reasonable time almost five minutes, compared to Paillier time approximately one hour. From the results of our work, some suggestions for future works as develop mechanisms of pixels selection for encryption process as Discrete Wavelet Transform (DWT) or linking chosen pixels with the image characteristics may increase the encryption quality, and using color images (3-D array) instead of gray-scale images (2-D array) in the proposed image encryption algorithm.

7. REFERENCES

[1] Malhotra, L. A. K. S. H. A. Y., Agarwal, D., & Jaiswal, A. (2014). Virtualization in cloud computing. J Inform Tech Softw Eng, 4(2), 136.

[2] Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation computer systems, 28(3), 583-592.

[3] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.

[4] Cao, N. (2012). Secure and Reliable Data Outsourcing in Cloud Computing (Doctoral dissertation, Worcester Polytechnic Institute in Electrical and Computer Engineering).

[5] Popović, K., & Hocenski, Ž. (2010). Cloud computing security issues and challenges. In MIPRO, 2010 proceedings of the 33rd international convention (pp. 344-349). IEEE.

[6] Ho, K. H. (2013). Semantic Search over Encrypted Data in Cloud Computing. (Master of Computer Science in San José State University)

[7] Stallings, W. (2006). Cryptography and network security: principles and practices. Pearson Education India.

[8] Xia, Z., Zhu, Y., Sun, X., & Wang, J. (2013). A similarity search scheme over encrypted cloud images based on secure transformation. International Journal of Future Generation Communication and Networking, 6(6), 71-80.

[9] Kuzu, M., Islam, M. S., & Kantarcioglu, M. (2012). Efficient similarity search over encrypted data. In Data Engineering (ICDE), 2012 IEEE 28th International Conference on (pp. 1156-1167). IEEE.

[10] Zhu, Y., Sun, X., Xia, Z., Chen, L., Li, T., & Zhang, D. (2014). Enabling Similarity Search over Encrypted Images in Cloud. Information Technology Journal, 13(5), 824.

[11] Hwang, R. J., Lu, C. C., & Wu, J. S. (2014). Searchable Encryption in Cloud Storage. World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering, 8(7), 1080-1083.

[12] Smart, N. P. (2003). Cryptography: an introduction (Vol. 5). New York: McGraw-Hill.

[13] Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key

cryptosystems. Communications of the ACM, 21(2), 120-126.

[14] Paillier, P. (1999). Public-key cryptosystems based on composite degree residuosity classes. In International Conference on the Theory and Applications of Cryptographic Techniques (pp. 223-238).

[15] Song, D. X., Wagner, D., & Perrig, A. (2000). Practical techniques for searches on encrypted data. In Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on (pp. 44-55). IEEE.

[16] Han, F., Qin, J., & Hu, J. (2016). Secure searches in the cloud: a survey. Future Generation Computer Systems, 62, 66-75.

[17] Bösch, C., Hartel, P., Jonker, W., & Peter, A. (2015). A survey of provably secure searchable encryption. ACM Computing Surveys (CSUR), 47(2), 18.

[18] Gionis, A., Indyk, P., & Motwani, R. (1999). Similarity search in high dimensions via hashing. In VLDB (Vol. 99, No. 6, pp. 518-529).

[19] Slaney, M., & Casey, M. (2008). Locality-sensitive hashing for finding nearest neighbors [lecture notes]. IEEE Signal Processing Magazine, 25(2), 128-131.

[20] Wang, J., Shen, H. T., Song, J., & Ji, J. (2014). Hashing for similarity search: A survey. arXiv preprint arXiv:1408.2927.

[21] Dongaonkar, A. D. (2013). Private Content Based Image Information Retrieval using Map-Reduce (Doctoral dissertation, Department of computer engineering and information technology, college of engineering, Pune).

[22] Humadi, A. M., & Younis, H. A. (2014). Application of the Fuzzy Logic in Content Based Image Retrieval using Color Feature. Int. J. Comput. Sci. Mob. Comput, 3(2), 170-180.

[23] Lowe, D. G. (1999). Object recognition from local scale-invariant features. In Computer vision, 1999. The proceedings of the seventh IEEE international conference on (Vol. 2, pp. 1150-1157). IEEE.

[24] Lowe, D. G. (2004). Distinctive image features from scale-invariant keypoints. International journal of computer vision, 60(2), 91-110.

[25] http://imagedatabase.cs.washington.edu/groundtruth/

[26] Solomon, C., & Breckon, T. (2011). Fundamentals of Digital Image Processing: A practical approach with examples in Matlab. John Wiley & Sons.

[27] Ahmad, J., & Ahmed, F. (2010). Efficiency analysis and security evaluation of image encryption schemes. Computing, 23, 25.

[28] Song, C., & Qiao, Y. (2015). A novel image encryption algorithm based on DNA encoding and spatiotemporal chaos. entropy, 17(10), 6954-6968.