International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-4, November 2019

# Iprivacy-Performance Measurement of Encrypted Image Over Mobile Cloud

**M.Sankari, P. Ranjana, D Venkata Subramanian**

***Abstract:*** ***Basically, people can use mobile phones to capture images and upload to cloud storage. While uploaded the data to cloud especially image, untrusted third party cloud vendors may pass to unauthorised users for their profit. And maintaining image Privacy is the major current issue in the cloud storage and resource-limited mobile devices. Due to the overcome of these issues, the proposed work introduced the algorithm Privacy-Preserving algorithm for Image Encryption (PPIE) to secure the encrypted image of mobile on cloud. The proposed architecture is handled by three processes such as Divide, Chunk group and Scramble (DCS) for fast execution. For achieving the high performance of the mobile system, the proposed algorithm reduced the encryption time to speed up the mobile system with limited mobile resources. The main highlights are keeping metadata on mobile rather than cloud. Even cloud service provider cannot able to retain the original image. The performance measures of PPIE, by various JPEG images, are calculated by various metrics such as throughput, Key sensitivity, Low Complexity, Processing Time and Time Consumption. It was proved to be reduced by 50% of time consumption while compared to AES. The proposed work may prevent users from accessing of private images.***

***Keywords: Image Privacy; AES; Python; mobile computing; JPEG; Security.***

## I. INTRODUCTION

Information like image, photo, video and audio is provided to keep secure in any form. Encryption is one of the best method to secure our data in encrypted form. And maintaining privacy is the greatest issue for the resource limited mobile devices. Cloud storage is a storage location where the data are stored. Data are encrypted before store to the cloud. While outsourcing data to the cloud storage, there are two options available for mobile image. First, image data [1] is passed to the cloud for encryption to reduce the mobile computational overhead. Here, maintenance of privacy is not assured.

Manuscript published on November 30, 2019.
* Correspondence Author
**M Sankari***, CSE Dept, Hindustan Institute of Technology and Science, Chennai, India. Email:vpsankarim@gmail.com
**Dr P Ranjana**, CSE Dept, Hindustan Institute of Technology and Science, Chennai, India. Email:pranjana@hindustanuniv.com
**Dr D Venkata Subramanian**, CSE Dept, Velammal Institute of Technology and Science, Chennai, India. Email:bostonvenkat@gmail.com



,[16] like RSA, DES, blowfish , AES [3] has been suitable for text data rather than image processing. These techniques Second, images [2] are encrypted in the mobile itself and encrypted data are moved to the cloud. It is safe for untrusted cloud providers/hackers in the cloud. Privacy assured due to the encrypted image passed. Remembrance of the traditional and past techniques of the encryption [2] are taken high execution time The encryption survey paper [4] deeply explains the various encryption techniques like Cubic squares, XOR, Scrambling and Chaos theory. It is concluded that the chaos technique makes better performance for image encryption. The light weight method [5][13] outlines for storing data to multiple cloud by using PRP(Pseudo random permutation) and chaos theory. It never used the cloud resources for its encryption. A novel privacy scheme of paper [6][18] outsourced the data in Internet of Things to the mobile cloud to assure privacy. It is a light weight data privacy. The DPM parallel Data privacy method paper [7] assures the data privacy and using GPU(Graphic Processing Unit) for parallel processing. GPU used for all kinds of image. The author introduced the data privacy scheme [8] to secure the data on the cloud storage from the untrusted cloud providers. Instead of image [9] applied to light weight encryption, videos are possible to apply for maintaining the sensitive data. In mobile cloud computing [10], data are secured through the data transmission by energy consumption. Based on the visual data image like face recognition, natural images and vehicle identification, the proposed encryption technique [11-13] is designed to prove the minimum execution time to assure privacy/security. The proposed work considers the JPEG image format for testing. When the photo [14] has taken from mobile, images are automatically stored in the JPEG format. It is a standardized image for mobile and the internet. The encryption techniques are described the various survey techniques [15] for image encryption and outsourced encrypted image to cloud and data privacy scheme. The survey paper [16] describes that the symmetric encryption has high security strength and good in speed, time, throughput and avalanche effect. It is a practical and real time usage. The remaining section contains: Section 2 explains the diagram and architecture of proposed PPIE. Section 3 outlines the various metrics to analysis the performance measures of PPIE. Section 4 describes the encipher of the PPIE algorithm. Finally, the proposed work overviews the PPIE method and concludes for future directions.

## II. PPIE METHOD

PPIE technique has taken the digital image from camera and converted to the binary form which is unreadable format.

It has applied three processes such as DIVIDE, CHUNK GROUP and SCRAMBLE to reduce the processing time to maintain image privacy. The encrypted data are stored to the cloud storage. In cloud storage, encrypted data are encrypted again before it gets stored into the cloud server.

The architecture of the proposed PPIE model is in Fig 1. Indep_file represents the different files formed from the chunk group.

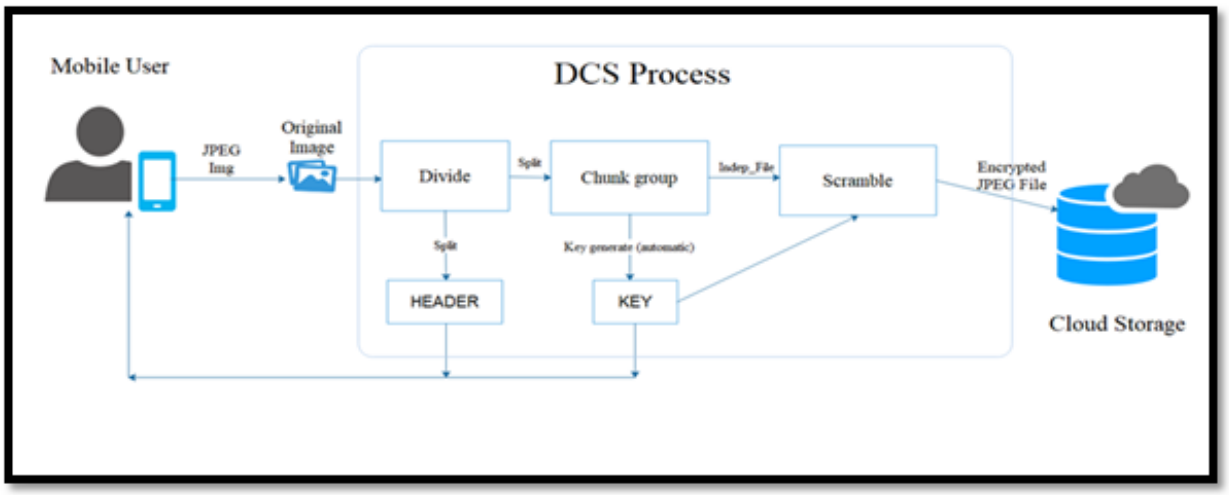


**Fig 1 Architecture of Proposed PPIE Model**

### A. Three basic Processes(DCS)

There are mainly three basic and major processes such as DIVIDE, CHUNK GROUP and SCRAMBLE available in the proposed PPIE method to improve the efficiency and high performance of resource-limited devices.

DIVIDE: The original image data is divided into two section. One section acts as a header and other section acts as a content. Header section contains the privacy data that is called meta data such as created date, size of the file, size of chunk formation and bytes occupied for image. The next section acts as the remaining part of the file. It is split into the different chunks based on the division. Division may be 1,2,3 or more byte/s of chunks. The DIVIDE process is as follows

DIVIDE=Header+Content (1)

where Header = {Metadata of the image} and Content={Group of Chunks split from the image}

The content of each file is as follows

Content= C(i,k) (2)

Where 'i' represents the position Bin(image), 'k' is the positon from 1 to m.

The maximum number(m) of Chunks formation is

$$m=[[\frac{Size\_Image}{Size\_Chunk}]\text{-}Header\_size]$$

where Size_image refers to the original image size(bytes), Size_Chunk refers to the chunk size in bytes and Header_size refers the header of the original image(bytes).

CHUNK GROUP: The pattern acts as a key or predefined function created by the user. The divided chunks are combined to make independent files according to the decision of the pattern selection. In proposed work, pattern decides as an odd and even format.

File 1← Formation of odd chunks

File 2← Formation of even chunks

The Pattern of chunk formation are as follows in Fig 2.

**File2(Odd)**

| | | |
|---|---|---|
| 1 | 3 | 5 |
| 7 | 9 | 11 |
| 13 | 15 | 17.. |

**File1(Even)**

| | | |
|---|---|---|
| 2 | 4 | 6 |
| 8 | 10 | 12 |
| 14 | 16 | 19.. |

**Fig 2 Example of Pattern Format**

SCRAMBLE: Each different file is scrambled themselves by using the key. The key is generated automatically by the first row of each file. The Key is stored in the client database. The Key representation is as follows

$Key_j$=First_row($File_j$) (3)

where $Key_j$ refers to the $j^{th}$ file of the key, First_row ($File_j$) refers to the first row of the $j^{th}$ file.

### B. PPIE Algorithm

***Input***

The Image Matrix 'Img',
Total number of pixels in image 'n',
Maximum Number of Chunk Formation 'm'

***Outcome***

The encrypted image Enc(Img), keys, H(i) are stored in mobile database.

***Process***

Img=" *.jpeg"
Bin(Img)←Img
**Divide:**
for every pixel at position (i, n-1) do
for each pixel at position (k, m)
do
Split the image as header H(i) and content C (i, k)
Bin(img)=H(i)+C (i, k)
end for
end for
**Chunk Group:**
Distribute C (i, k) as different file
by grouping of chunks based on pattern File1
File1←Formation of odd chunks(C(i,k[odd])
File2←Formation of even chunks(C(i,k[even])
**Scramble:**
for each row at file(j,2)
Generate $Key_j$=first row($file_j$)
Scramble files by keys
$File_j$←$key_j$+$file_j$
End for
Enc(img)← Combine($File_i$)
Return Enc(img)
Enc(img)→ cloud storage

## III. PERFORMANCE MEASURES OF PPIE

For considering the 10 JPEG image as a grey scale image with 256*256 pixels, calculate the encryption time of the proposed PPIE method with standard algorithm AES. The proposed work is implemented in PYTHON [11], which is an open source, high level language and includes the library module like pycrypto for execution. It is a scripting language and simpler code to execute. The configuration of LENOVO YOGA 520 system, Intel core i3 processor with 8GB RAM are used for implementation. The proposed work [18] considers the chunk size as 16 bits/2 bytes, size of Key in AES as 2 bytes. The PPIE key size is automatically taken from the first row of each file. The Pattern are considered as odd/even chunks. The following measurement considers the reduction of Encryption time, Iteration calculation, Low complexity, Key sensitivity and Throughput to be evaluated to express the performance of the PPIE method to ensure security/privacy.

### A Reduction of Encryption Time

The Proposed work has been taken the three processes to execute the algorithm. By splitting, image data are divided to run parallel for fast execution. Key can be generated automatically. So the encryption time are reduced to run parallel and less time to generate the key. But in AES, image data are processed by four rounds sequentially and higher time taken for key generation. Therefore, the usage of CPU and memory are maximized. The encryption time of standard AES and effective proposed PPIE method are in Table I.

**Table I Encryption Time AES vs PPIE**

| Image type(JPEG) | Image Size(kb) | Average Encryption time(milli sec.) | |
|---|---|---|---|
| | | AES | PLIE |
| camera | 4.64 | 1.8 | 0.25 |
| dots | 3.88 | 1.13 | 0.23 |
| earth | 5.59 | 1.14 | 0.25 |
| leaf | 5.83 | 1.21 | 0.45 |
| letter | 12.9 | 1.39 | 0.45 |
| people | 3.93 | 1.63 | 0.29 |
| right | 6.41 | 1.2 | 0.28 |
| s_letter | 4.70 | 1.6 | 0.33 |
| w_letter | 6.36 | 1.18 | 0.28 |
| wheel | 6.84 | 1.5 | 0.4 |
| Average Time Duration | | **1.37** | **0.32** |

Consider the example as "earth" jpeg image has taken the encryption time of AES as 1.14millisec and PLIE as 0.25 millisec and the proposed average time duration was 1.37 millisec and AES was 0.32. The conclusion of PPIE was reduced more than half of AES. It is designed in python language and demonstrated clearly in Fig 3 by using bar chart.

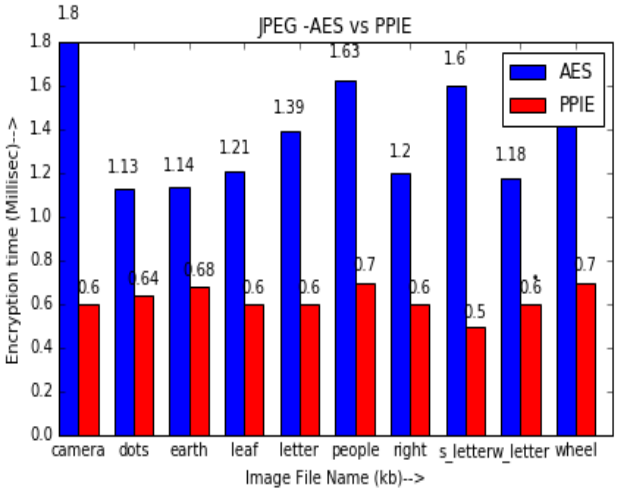


**Fig 3 Encryption Time AES vs PPIE**

### B Iteration Calculation

As the above proposed work discussed, minimization of encryption time while running parallel to reduce the number of loops formed. But in standard AES[4], large number of loop is generated due to the non-splitting data to maximize the encryption time. While compared to AES, PPIE method has less iteration to achieve the superior performance of speedup and security. The iteration calculation of AES and PPIE method is in Table II.

**Table II Iteration calculation of AES vs PPIE**

| Image Type(JPEG) | Image size(kb) | Iteration Calculation(Number of loops) | |
|---|---|---|---|
| | | AES | PPIE |
| camera | 6.84 | 438 | 19 |
| dots | 4.64 | 298 | 22 |
| earth | 3.88 | 249 | 12 |
| leaf | 5.59 | 359 | 45 |
| letter | 5.83 | 374 | 25 |
| people | 12.9 | 830 | 44 |
| right | 3.93 | 253 | 7 |
| s_letter | 6.41 | 414 | 27 |
| w_letter | 4.70 | 306 | 22 |
| wheel | 6.36 | 408 | 18 |

For the observation of the iteration calculation, the proposed work PPIE has minimized the number of loops for execution while compared to standard AES. It makes to improve the speed and security.

### *C Low* Complexity

The proposed work of low complexity is calculated on three factors. (a)Splitting (b)Iteration calculation (c)Encryption time measurement. For referring the Fig 2, Splitting can be done by the pattern to run parallel. For Referring the Table 2, Calculate the iteration and improve the speed performance of the mobile. Encryption time are calculated in Table 1. Thus, the complexity of the mobile are reduced by parallel processing, improve the execution time based on reduced iteration loop. It is represented in Fig 4.


**Fig 4 Calculation of Low Complexity**

### D Key Sensitivity

It is a major metric for cryptography to understand the strength of the algorithm. A longer key has high security but the smaller key has less security. It takes high execution time to complete the algorithm. But the smaller key takes less execution time, less resource with better security. The proposed algorithm PPIE has taken the key automatically generated from the first line of the file while keys are never passed to cloud to maintain privacy.

### E Throughput

Basically, Throughput [16] explains the number of encrypted data by the specified unit time. Throughput is directly proportional to the speed. So, Speed up the process is mainly base on the throughput of the algorithm. Assume that the Image_size represents the size of the image file and $Enc\_time_i$ as the time taken calculation for the encryption. Our proposed work has calculated the throughput of two algorithms such as AES and PPIE method. It is to explains how much of data can be passed per unit time and clearly declared the speed of the algorithm.

$$\textbf{Throughput(AES)} = \sum_{i=1}^{n} \frac{Image\ size_i}{Enc\ time[i](AES)}$$

=

[((4.64+3.88+5.59+5.83+12.9+3.93+6.41+4.70+6.36+6.84)/ 10)/ ((1.8+1.13+1.14+1.21+1.39+1.63+1.2 +1.6+1.18+1.5)/10)]

**Ω 4 Mbps**

$$\textbf{Throughput(PPIE)} = \sum_{i=1}^{n} \frac{Image\ size_i}{Enc\ time[i](PPIE)}$$

=

[((4.64+3.88+5.59+5.83+12.9+3.93+6.41+4.70+6.36+6. 84)/10)/ ((0.25+0.23+0.25+0.45+0.45+0.29+0.28+ 0.33+0.28+0.4)/10)]

**Ω 17.19 Mbps.**

For these observation, throughput of proposed work is increased four times of the AES. So, it improves the speed of the image encryption and the power consumption.

## IV. DECRYPTION

Basically, cloud server encrypts the encrypted binary data from PPIE algorithm. While the process of decryption, retrieve only the encrypted data (PPIE) from cloud. The proposed work descrambled the files with the automatically generated keys. Then merging the files by using the odd/even pattern. After the collection of chunks with chunk size, retain the original JPEG image. Finally, mobile image is regained from cloud.

## V. CONCLUSION

This proposed work proved that the high performance of mobile system can be achieved by various performance measures such as low complexity, throughput, speed and time consumption. Without trust of the unauthorized cloud vendors/hackers, the proposed work holds the privacy information like secret key, pattern and the header in mobile system itself. Non sensitive encrypted image is passed to the cloud. Python Language was used to implement the algorithm. The proposed algorithm proved that the encryption time is minimized by 50% than AES. Therefore, it automatically improves the overall performance of the system. The future direction will be tested with different patterns, chunks and various file formats. And measure with the various factors to ensure security and privacy.

## REFERENCES

1. M. Sankari and D. P. Ranjana, “Privacy-Preserving light weight image Encryption in mobile cloud,” in Advances in Intelligent Systems and Computing, Bangalore, Springer, 2018, pp. 404-414.

2. S. Garg.P, "An efficient and secure data storage in Mobile Cloud Computing through RSA and Hash function," Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014 International Conference on IEEE Society., 2014.
3. D. Kumar, D. A.R.Reddy and Dr.S.A.K.Jilani, "Implementation of 128-bit AES algorithm in MATLAB," International Journal of Engineering Trends and Technology (IJETT), vol. 33, no. 3, 2016.
4. P. M. Modak and D. V. Pawar, "A Comprehensive Survey on Image Scrambling Techniques," International Journal of Science and Research (IJSR), vol. 4, 2015.
5. M. Bahrami and M. Singhal, "A Light Weight Permutation Based Method for Data Privacy in Mobile CloudComputing," in 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)., 2015.
6. M. Bahrami, A. Khan and M. Singhal, "An Energy Efficient Data Privacy Scheme for IoT Devices in Mobile Cloud Computing," IEEE International Conference on Mobile Services., 2016.
7. m. Bahrami, D. Li, M. Singhal and A. Kundu, "An Efficient Parallel Implementation of a Light-weight Data Privacy Method for Mobile Cloud Users," Seventh International Workshop on Data-Intensive Computing in the Clouds (DataCloud), 2016.
8. M. Bahrami and M. Singhal, " cloudPDB:A light-weight data privacy schema for cloud-based databases," International Conference on Computing, Networking and Communications, Cloud Computing and Big Data., 2016.
9. X. Zhang, S.-H. Seo and C. Wang, "A Lightweight Encryption Method for Privacy Protection in SurveillanceVideos"Volume: 6 Pages:18074-87.," IEEE Journals & Magazines, vol. 6, pp. 18074-87, 2018.
10. J. S. S. K. N. &. L. B. Hong, " A study of secure data transmissions in mobile cloud computing from the energy consumption side," in International Conference on Information Networking (ICOIN), 2013.
11. K rasool reddy et al., " GUI implementation of image encryption and decryption using Open CV-Python script on secured TFTP protocol," in AI Conference, 2018.
12. H.C.A. Tilborg and S. Jajodia (eds.), Encyclopedia of Cryptography and Security, Springer, 2011.
13. C. Shannon, "A Mathematical Theory of Communication," The Bell System Technical Journal, vol. 27, no. 3, pp. 379-423, 1948.
14. J. W. Y. C. K. R. Zhan Qin and Jian, "Privacy-preserving Image Processing in the Cloud," IEEE Journals & Magazines, vol. 5, no. 2, pp. 48-57, 2018.
15. G. Singh and Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security," International Journal of Computer Applications , vol. 67, no. 19, pp. 33-38, 2013.
16. R Arivukarasi et al., "A Comprehensive survey of deceiful conclusion and counteractive action in multimodel datasets utilizing data mining and machine learning," Journal of Advanced Research in dyanamical and control systems, 2019.
17. M. Sankari and P. Ranjana, "PLIE- A Light-weight Image Encryption for data Privacy in mobile cloud storage," International journal of engineering and technology(UAE), vol. 7, pp. 368-72, 2019.
18. Z. A. Balouch, M. I. Aslam and I. ahmed, "Energy efficient image encryption algorithm," International Conference on Innovations in Electrical Engineering and Computational Technologies (ICIEECT)., 2017.

## AUTHOR PROFILE

**Sankari M ,** doing her Ph.d in Hindustan Institute of Technology and Science, Chennai, Tamilnadu. She has completed B.E in computer Science and Engineering from Bharat Niketan Engineering College , under Anna University, 2006.She did her Master degree M.E in Computer Science and Engineering from Hindustan Institute of Technology and Science under Anna University,Chennai,2009. She was worked in Engineering College, under Jawaharlal Nehru Technical University, Hyderabad. She has published five international conference papers and two international journals and three national conferences. She conducted presentation Lab and mentors for engineering students. She attended many workshop and handled many research field seminars. She is interested in the field of image processing, cloud storage, security and networks.

**Ranjana P**, is a Professor in Hindustan Institute of Technology and Science, Chennai. She received her Ph.d in computer science from Hindustan University, Chennai,2017. She received M.E in Computer Science and Engineering from Anna university, Chennai,2005. She received MCA from Madurai Kamaraj university, Madurai,1998. She is conducted many conference, seminars and workshops. She is an coordinator of a NBA, NAAC, UGC-CSE and PG students. She has published papers in 25 international Conferences and 50 international journals. Her area of interests includes image processing, cloud, network and security.

**Dr D Venkata Subramanian**, is an adjunct professor in Velammal Institute of Technology, Chennai. He received his Ph.d in B.S Abdul Rahman University,Chennai in the year 2014. He did his Masters in M.S. in Computer Systems Engineering with specialization in software engineering design from School of Engineering, Northeastern University, Boston, USA in the year 2002. He received B.E. degree in Computer Science and Engineering from Bharathidasan University, Tamilnadu, in the year 1992. He has published more than 50 papers in the international journals and more than 50 papers in the international conferences. His area of interests includes Databases, Knowledge Management, Data Mining, Security and Image Processing.