Novel Encryption Method of GPS Information in Image File Using Format-preserving Encryption

Changhyun Lee, Yeonju Choi, Hyeongmin Park, Kangbin Yim, and Sun-Young Lee

Soonchunhyang University
IMIS 2019

Presenter: Brandon Falk (上海交大)

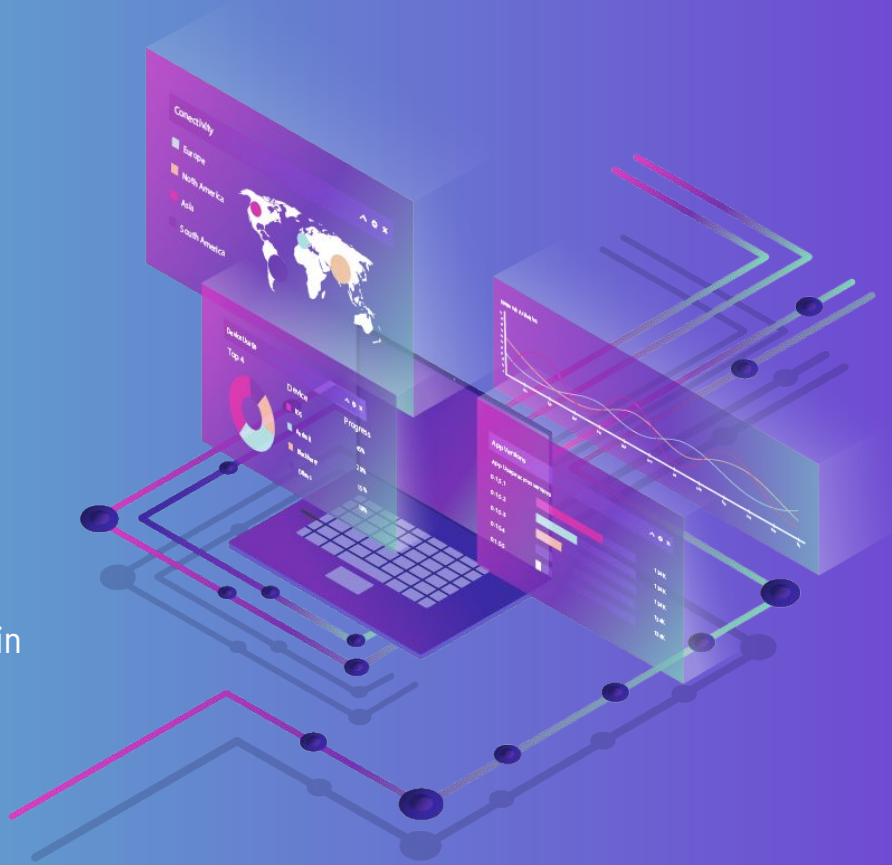
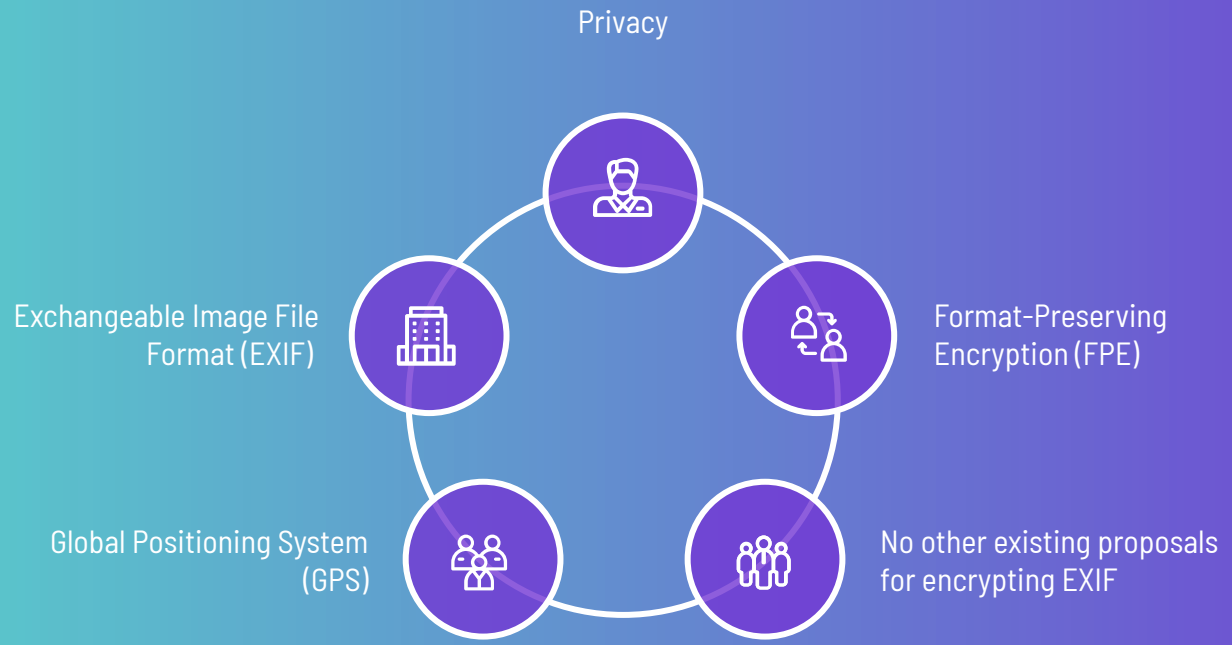


TABLE OF CONTENTS

01 BACKGROUND

Background


Privacy
Format-Preserving Encryption (FPE)
No other existing proposals for encrypting EXIF
Global Positioning System (GPS)
Exchangeable Image File Format (EXIF)

INTRODUCTION 02

Measuring GPS in Smartphones

A-GPS

Synchronize GPS satellite position and current time by 3G or 4G communication networks

Cell-ID

3G or 4G signals received from base station

Wi-Fi

Signal of wireless router identifying location

P-Cell

Builds database based on information in surrounding environment and compares to information received from device

EXIF

How
smartphone, camera, etc

When
date time stamps

Data Travels
Across devices, software, etc

Where
longitude / latitude / direction / altitude

Photo storage services
Google images, WeChat Moments, Weibo, Facebook, Instagram
(Some services strip EXIF data)

“Can be a gold mine of information”

—SOMEONE FAMOUS

Format-Preserving Encryption

- Encrypt plaintext with values of same format
  - Vulnerable to codebook attack if plaintext is short
- Defense
  - Tweaking, Cycle-walking, Ranking
    - Tweak is additional input values to make up for short plaintext
    - Cycle-walking is Vulnerable to side-channel attacks
    - P-NP problems can't efficiently apply Ranking
- **Thus, FPE is not used in this paper's proposal**

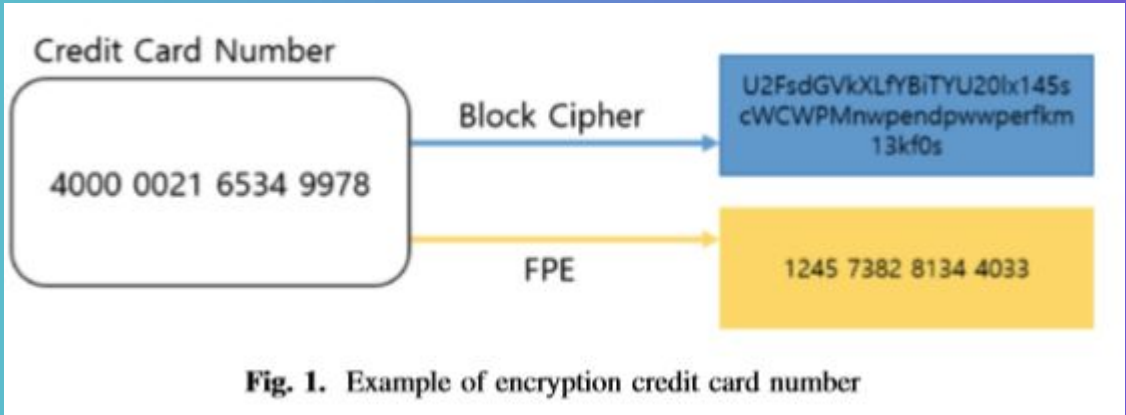


Fig. 1. Example of encryption credit card number

03 STATE OF THE ART

FE1 Algorithm

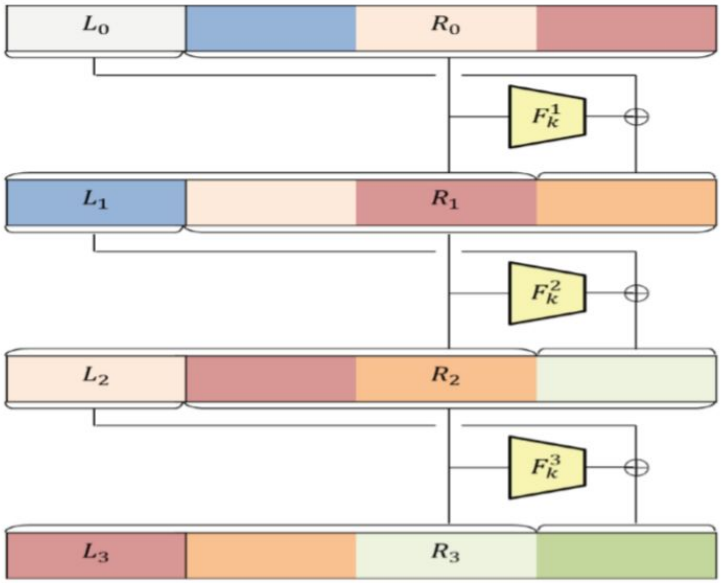
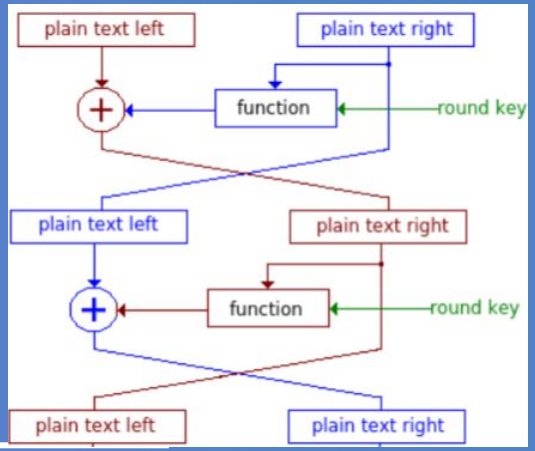


Fig. 2. Structure of FE1 algorithm [7]



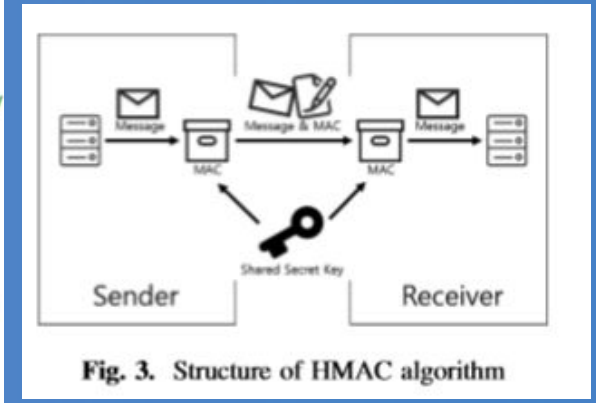
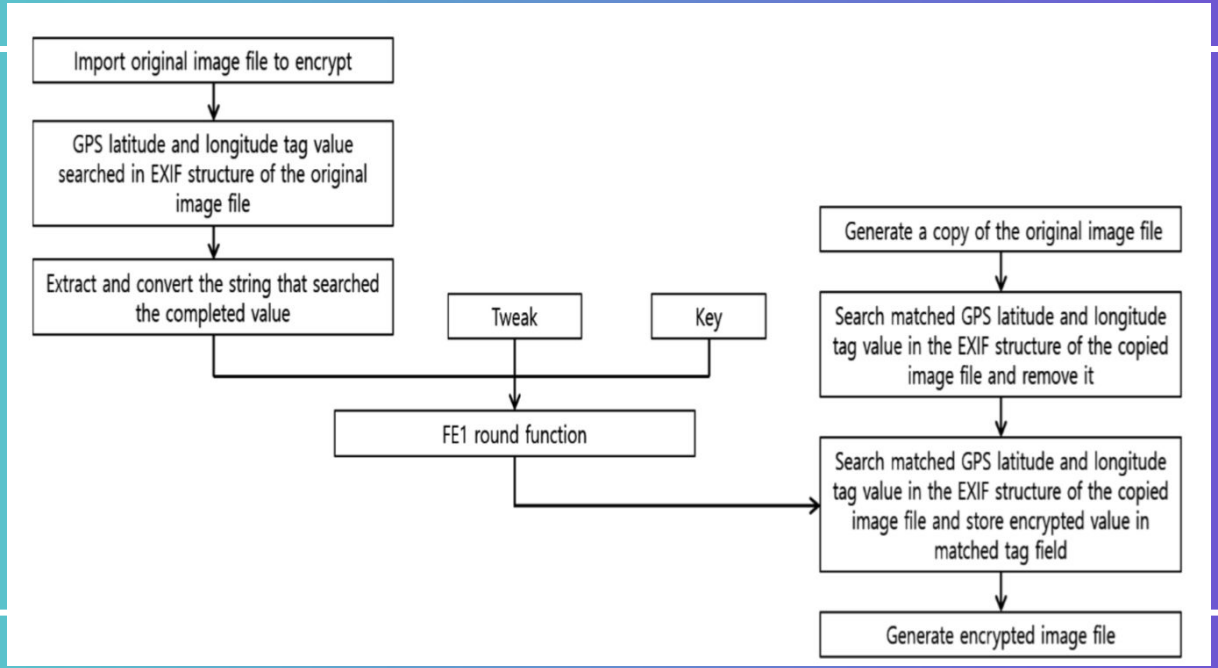


Fig. 3. Structure of HMAC algorithm

- Unbalanced Feistel Network - divide plain into unequal lengths
- Calculation of L and R values - R is entered in round function along with key, tweak, and corresponding # of rounds
- Round function algorithms: HMAC and AES. Calculate XOR with L. Then attach to existing value R.

Design of GPS Encryption using FE1

Encryption Process shown below is the same as Decryption Process



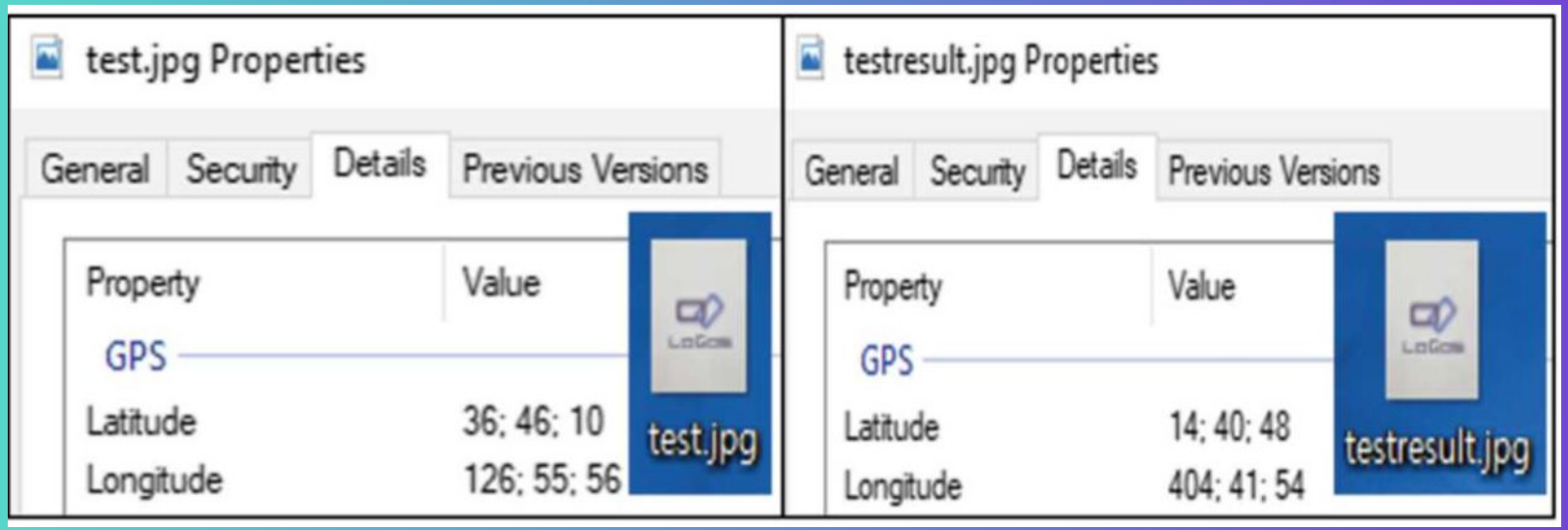
EXPERIMENTS 04

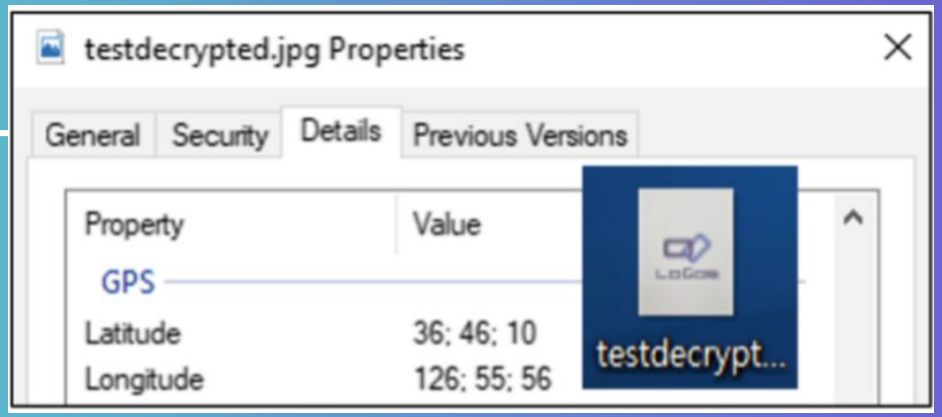
```
1. encrypt   2. decrypt
Choose the number you want : 1

Image Latitude : 36,46,10
Image Longitude : 126,55,56

Encrypted Image Latitude : 14,40,48
Encrypted Image Longitude : 404,41,54

Edit Complete
```

〈Encrypt〉

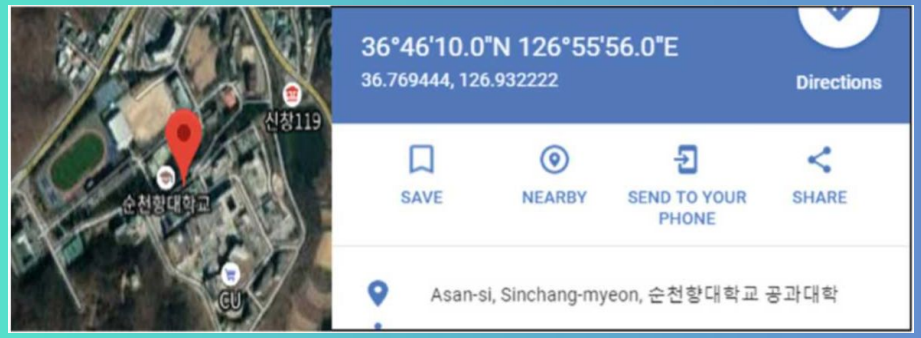
```
1. encrypt   2. decrypt
Choose the number you want : 2

Image Latitude : 14,40,48
Image Longitude : 404,41,54

Decrypted Image Latitude : 36,46,10
Decrypted Image Longitude : 126,55,56

Edit Complete
```

〈Decrypt〉

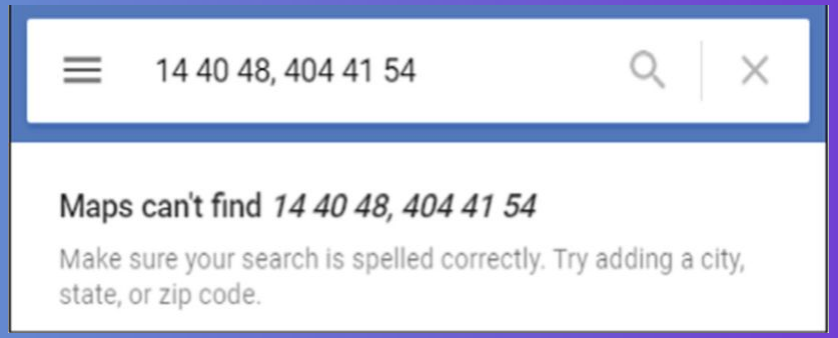




Real Location Searched on Google Maps



Exceed Google Map Range Value (Intended)



05 RESULTS

Here you could describe the topic of the section

Discussion of Results

SPECS: CPU I5-8500
Windows 10

Time Complexity: n^2

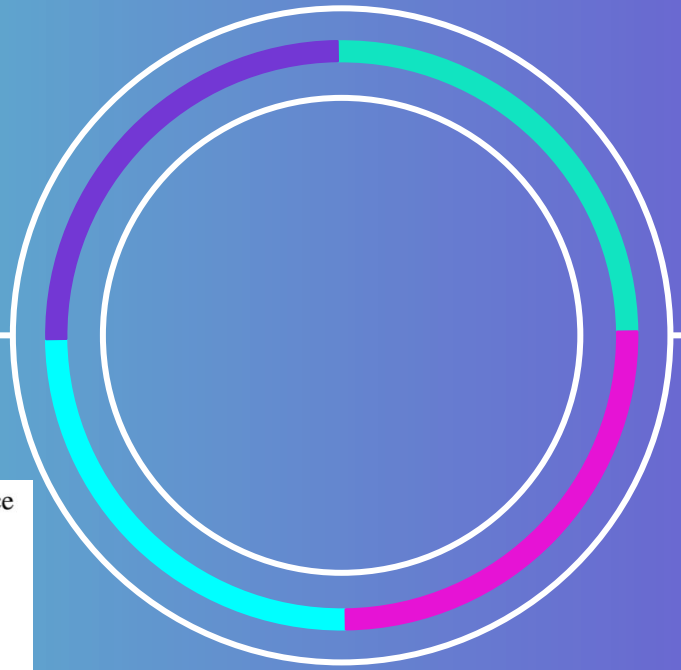


Table 1. Result of proposed encryption method performance

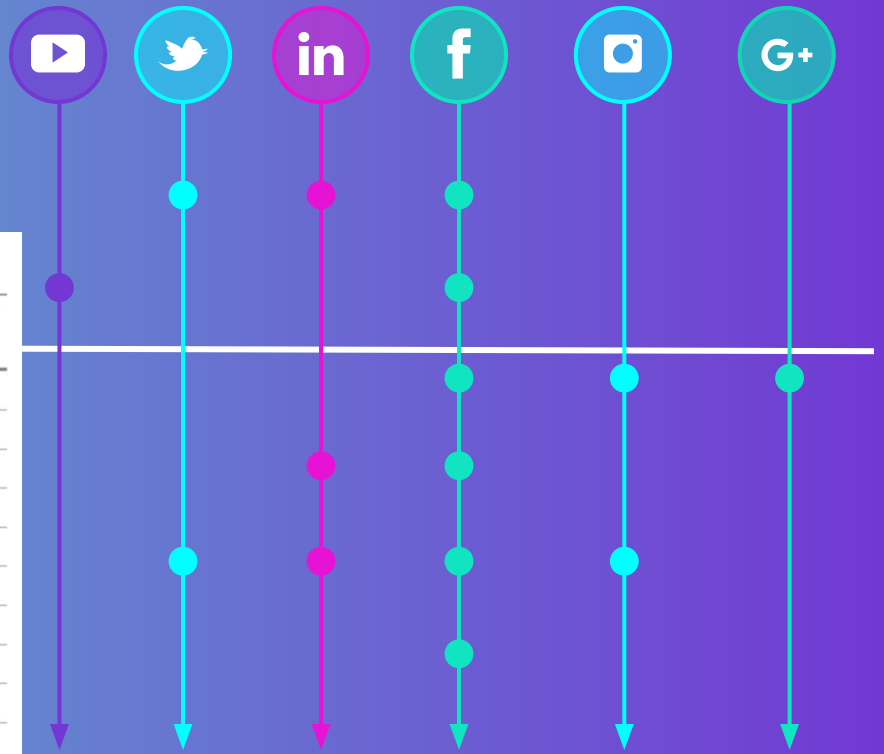
	Time (s)	Volume (MB)
Image 1	0.009	3.09
Image 2	0.01	3.55
Image 3	0.025	8.28
Image 4	0.01	3.45
Image 5	0.009	3.26
Image 6	0.013	4.09

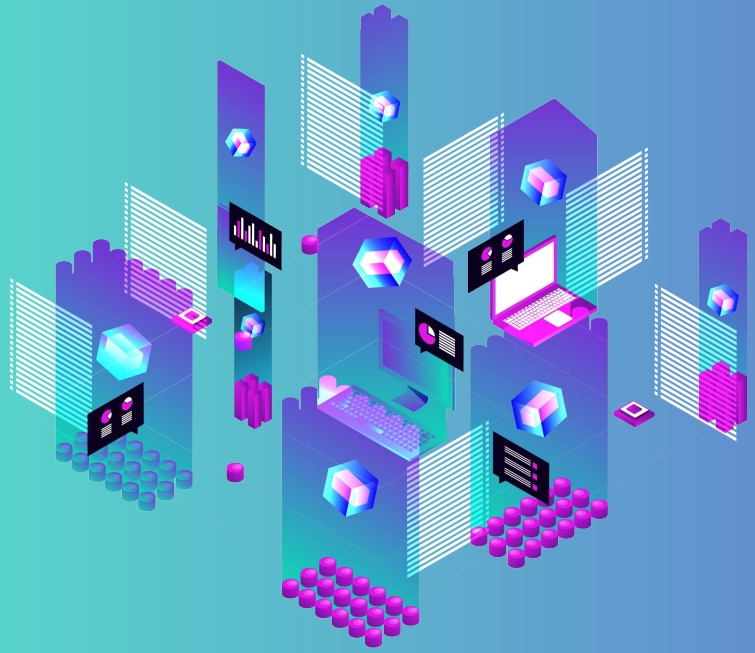
Discussion of Results

Triangle = EXIF GPS data **found**
Circle = EXIF GPS data **not found**

Table 2. Search the GPS information where it is remain

	PC → Mobile	PC → PC	Mobile → PC	Android → iOS	iOS → Android
Cloud Service 1	○	○	○	○	○
Cloud Service 2	○	○	○	○	○
Cloud Service 3	○	○	○	○	○
Messenger Application	○	○	△	○	X
Text Messenger	–	–	–	○	X
SNS 1	X	X	X	X	X
SNS 2	X	X	X	X	X
SNS 3	○	○	○	○	○
SNS 4	○	○	○	○	○
E-Mail	○	○	○	○	○





CONCLUSION 06

Conclusion and Potential

5,408 Followers	5,408 Followers	5,608 Views	608 Followers	5,608 Likes	5,608 Followers

- **Novel Encryption Approach**
  - Lack of Defense
  - Lack of Significant Experimentation
  - Area is capable for further research
- **EXIF GPS implications**
  - Treasure cove of data is stored in photos
    - If a photo service is hacked, a lot of personal information can be more exposed than intended

谢谢~