Smart Mobile Identity Detection from Captured Images

Murugeswari Kandavel, Ganesan Govindan

Abstract: Most of the cybercrime are originated from abuse of mobile phones. If there is a possibility to identify the persons who abuse mobile phones, then the task of Cybercrime, Information forensic and Defense department is getting easier. Here the authors proposed a technique to identify the International Mobile Equipment Identity (IMEI) number, time stamp and geographical location of the smartphone/mobile. Whenever the mobile camera is used the identity information such as IMEI number, timestamp and geolocation are embedded in the captured image automatically. For that, a mobile application was developed and deployed as a mobile service. By decoding the image, the embedded identity information of that mobile phone is revealed. Using this information it is easy to identify the person/s.

Keywords: Steganography, Cryptography, Cyber Security, Android, Smartphone.

I. INTRODUCTION

According to International Data Corporation (IDC) smartphone shipment in 2016 reaches 359.3 million units. Almost 90% of mobile users had a smartphone. The major reason for this grand success is the faster connectivity, handling the high volume of data, speedy delivery etc. Thus steganography targets smartphones since mostly information hiding techniques were favoured by how people communicate; also the carriers were used for steganography evolved through ages.

are fine and satisfactory. Author (s) can make rectification in the final paper but after the final submission to the journal, rectification is not possible.

II. OBJECTIVES OF THE PROPOSED SCHEME

By having this in mind the authors proposed an android application having three features 1) to identify 2) to locate and 3) to track the timestamp. It will answer the questions raised during investigation Who, When, and Where. Once finding answers for these basic questions then tracing the abusers easily. Also, the proposed application runs on the mobile without the user knowledge. Hence this application planned as a service deployed with mobile services.

Whenever the smartphone is switched on, this application automatically started as a service in that phone. It collects the phone's identity information such as IMEI number, time stamp and Geographical location then embeds into the image which is taken by the camera using steganography.

Revised Manuscript Received on December 15, 2019.

Murugeswari Kandavel, Associate Professor in Kalasalingam Academy of Research and Education, Tamil Nadu, India.

Ganesan Govindan, Associate Professor, Department of Computer Science and Engineering, K.L.N College of Information Technology, Sivagangai, India.

Here imperceptibility of the image must be high, then only the user did not aware of embedding of the identity information. By decoding the captured images of that phone reveals the IMEI number, time stamp and geographical location of the phone. Using this identity information, tracking of the smartphone user is easily found.

A. Related Work

Steganography had its footprints since from 1679, mostly focused on image, audio, and video as cover images. Implementation of steganography started from simple LSB substitution to Matrix Encoding. Imperceptibility of images is maintained hence it defeats human visual/auditory system. Privacy and security of information is one of the main issues in communication. Many methods were used for secret communication. Also, an ample amount of researchers were involved in applying steganography on mobile environment. [1]-[4].

In 2006 onwards researchers started to hide information in SMS. Shirali et al. introduced SMS as a carrier for steganography. She hid the data in a picture and sent it via SMS messages. When the message is received, the hidden data is extracted and the picture is only stored in the phone storage [5]. A new scheme proposed by Shirali et al. in 2007 for exchanging information via SMS secretly, by applying an invented language which is used for SMS texting [6]. Shirali et al introduced a new technique by using SMS as a carrier the mobile software activation code was sent secretly. At the receiver's side the software activation code is extracted and compared with the mobile phone IMEI number. If the comparison succeeds, the software is activated [7]. Rafat et al. used SMS-Texting language for secret communication via SMS [8]. Shirali et al presented a method for hiding data using Sudoku puzzle through SMS. By solving the puzzle the hidden data is extracted [9].

Bhaya [10] suggested a method for hiding the information in the SMS message by altering the font style of each character by 0 (system font) or 1(proportional font). Now the stego message looks like an ordinary one but each character falls in one of these two similarity font style. It was implemented using J2ME in mobile phones. Only one bit is hid in each character at a time.

Papapanagiotou et al. [11] and Shirali et al.[12] were used MMS messages for hiding secret information. Ritesh et al.[13] used MATLAB program for sent the image with hidden secret data. On the receiver's side also MATLAB program was used to retrieve the secret data from the received image.

Ahmed et al. introduced to hide image/text/voice in images without user's attention [14]. V ahab et al. [15] proposed a new cover for hiding secret is emoticons and lingoes (abbreviation of words normally used in chat and SMS). Based on user defined mapping, emoticons and lingoes were decoded into original information at the receiver end. So far discussed approaches concentrated on hiding any secret message within SMS, MMS and Emoticons or lingoes. All were used for secret communication. The Same idea can be applied for detecting the identity of the mobile user also. Accordingly, a mobile application was developed to hide the identity of the mobile phone in the images captured by its camera automatically. When decoding the images the investigated can easily trace the users.

Gupta et al. thought differently and proposed a novel idea for hiding the mobile phone's identity information such as IMEI [International Mobile Equipment Identity] and IMSI [International Mobile Subscriber Identity] number within the images captured by the device itself [16]. Before the captured images were compressed, identity information was encrypted and hidden into images. He used key based algorithm for hiding the identity numbers randomly within the captured images. The authors claimed that their methodology is feasible and high secure due to the nature of encrypting the numbers before applying the steganography. It is also helpful for identifying the anonymous images which were captured by mobile phones. By having this motivation in mind here the authors proposed an improved technique to hide IMEI Number of the phone, geographical location, date, day and time of the image taken within the images whenever it was captured by the camera without the knowledge of the mobile user/s.

B. Proposed Framework

Hence, the proposed framework, MobiSteg is a steganographic application to hide IMEI Number of the phone, geographical location, date, day and time of the image and they are automatically embedded within the images whenever they are captured by the camera without the knowledge of the mobile user/s. The overview of MobiSteg is given in Figure 1. It is implemented in Moto G Play smartphone with the configuration of Android 6.01 version (OS), 5mp rear camera and 13mp camera.

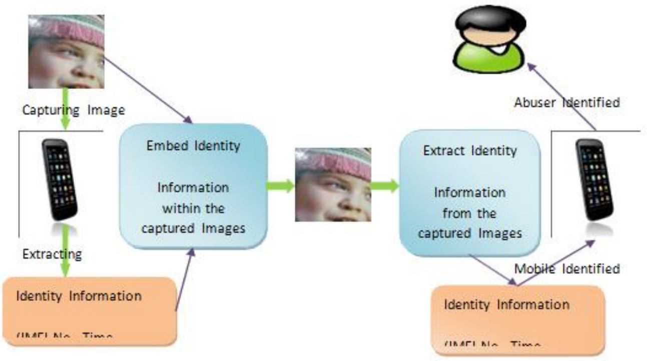


Fig. 1. Architecture of Mobisteg

III. METHODOLOGY

The motivation behind this work is to use steganography in smartphones. So for steganography has been used in smartphones for hiding secret information in SMS, MMS, emoticons and images. The proposed work aims at hiding the identity of the phone into the images which are captured by its camera without the user's knowledge. This application running as a service will embed the identity information of the mobile within the captured images immediately, when it's stored in the gallery. There is no copy of raw image available in the gallery. Hence, it never draws the user's attention. When this embedded image is sent over communication channel either to mobile/computer, decoding using the application will reveal the identity of the mobile.

The major contributions of the proposed work are as follows:

- The identity of the mobile is embedded immediately, whenever the image is captured by its camera.
- Without user's knowledge, the identity is embedded within the images.
- Application which is proposed as a service, automatically starts without user intervention.

The MobiSteg consists of the following four modules which are grouped into two apps and their appearance in the smartphone screen is depicted in Figure 2.

1. Encrypt App. -
   a. Encryption - Mcrypt
   b. Embedding - Mbed
2. MyDecryption App. -
   a. Decoding - Mdcod
   b. Decryption - Mdcryp

Fig. 2. MobiSteg apps and their icons in the mobile phone

Whenever the mobile is switched on, the proposed service is running in the background. Once the image is captured by the camera of the smartphone, the proposed technique starts automatically to get into function as mentioned in the flow diagram given in Figure 3. It accomplishes the following processes one by one.

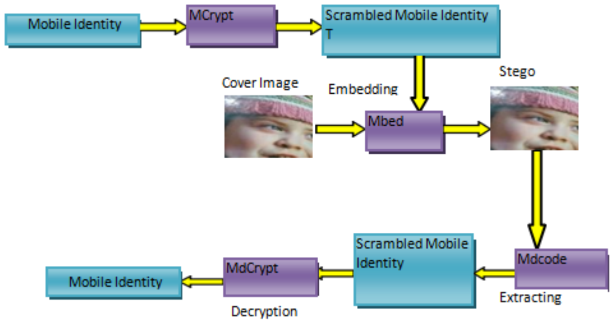


Fig. 3. Flow diagram of mobisteg processes

A. *MCrypt:* Using the proposed encryption technique – Mcrypt, the process is carried out. First, the IMEI number, time stamp and geolocation of the smartphone are retrieved and are concatenated then to form a single string called as Mobile Identity (MI). Then, it is transformed by using the steps given in the flowchart as depicted in Figure 4 and results into scrambled mobile identity (MI’).

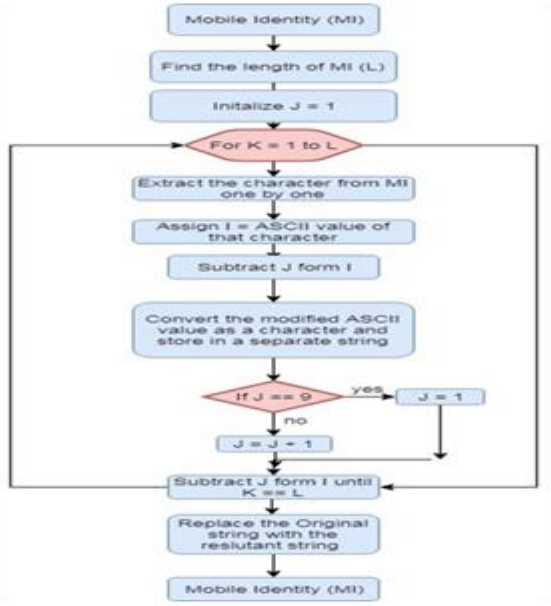

Mobile Identity (MI)
Find the length of MI (L)
Initalize J = 1
For K = 1 to L
Extract the character from MI one by one
Assign I = ASCII value of that character
Subtract J form I
Convert the modified ASCII value as a character and store in a separate string
If J == 9
yes
J = 1
no
J = J + 1
Subtract J form I until K == L
Replace the Original string with the reslutant string
Mobile Identity (MI)

Fig. 4. Mcrypt flow chart

B. *Mbed:* For embedding, simple LSB 2 bit substitution is used. All the smartphones are handling only color images. Hence, the proposed work focuses on only color images. Mbed consists of two phases; pixel selection and LSB substitution.

Pixel Selection

Normally in steganography algorithms, the choice for hiding secret information is only in the sequential pixels. Hence, anybody who has the knowledge of the algorithm, can extract the hidden secret from the image. Here, the proposed approach selects the pixels in a random manner; and therefore, it is difficult to extract the hidden secret.

LSB substitution

- The first RGB value of the captured image (JPEG only) is taken.
- Each of the three color palettes (red, green, blue) of the image is separated.
- Each pixel is represented as eight bits per color palette and totally, single pixel in a color image has 24 bits (3 × 8).
- The resultant string of Mcrypt i.e., scrambled Mobile Identity (MI’) is converted into binary form.

- Pictorial representation of Mbed process is shown in Figure 5.
- Finally, all the three palettes are combined and the stege image is now ready with embedded MI’.

- First two bits in the MI’ (resultant string of Mcrypt) are embedded in the Red palette pixel
MI = 1 0 1 1 0 0
Red - 1 1 0 1 0 1 X X
First two bits of MI’ 1 1 0 1 0 1 **1 0**

- Next two bits in the MI’ in green palette pixel
Green – 0 1 0 0 1 1 X X
Second two bits of MI’ 0 1 0 0 1 1 **1 1**

- Next adjacent two bits are embedded in blue palette pixel
Blue – 1 0 0 1 0 0 X X
Third two bits of MI’ 1 0 0 1 0 0 **0 0**

Fig. 5. Pixel Selection of Mbed Process

C. *Mdcode:*The reverse process of Mbed is carried out and it is depicted in Figure 6. Finally, all the extracted values (binary form) are converted into ASCII values and again converted into their equivalents characters. That is the scrambled Mobile Identity (MI’).

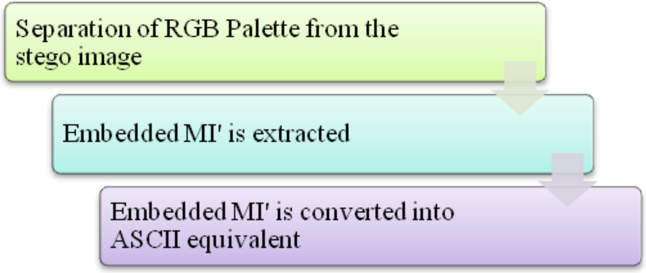

Separation of RGB Palette from the stego image
Embedded MI' is extracted
Embedded MI' is converted into ASCII equivalent

Fig. 6. Processes of Mdcode

D. *Mdcrypt:*The reverse process of Mcrypt has been carried out and it is depicted in Figure 7. The resultant value of Mdcode is transformed into original values. That is nothing but 15 digit IMEI number, day, month, date, time, year and Geolocation (longitude and latitude) of the smartphone.

E.

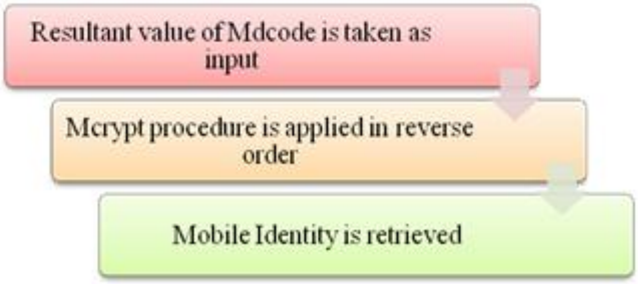
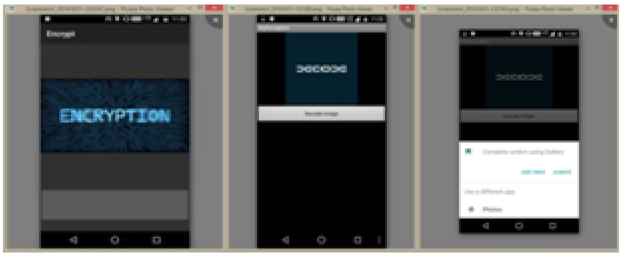

Resultant value of Mdcode is taken as input
Mcrypt procedure is applied in reverse order
Mobile Identity is retrieved

Fig.7. Processes of Mdcrypt

IV. EXPERIMENTAL RESULTS

The proposed application has been implemented as a service in MotoG Play Android version
6.01 smartphones which has 2GB ROM, 16GB RAM, 5MP rear camera and 13MP camera. The application is developed in Android Studio and the database is SQLite. This application is compatible with Android Version 5.0 and above. For testing, the images captured by the front camera of the mobile are used. Hence, the dataset is prepared by the mobile only. The following screen shots have shown the entire process.
For visualizing purpose, the proposed MobiSteg is running as an application and the screen shots are captured. Then, they are displayed using the Picasa Photo Viewer. MobiSteg has two apps, one is for encryption, named as Encrypt and the other one is for decryption named as MyDecryption as shown in Figure 2. Figures 8.a, b and c show the smartphone screenshots while an encryption, decoding and opening the embedded image are running respectively.

Whenever the camera is used for capturing images/photos, Encrypt app starts and its home screen is shown in Figure 8.a. This app immediately hides the mobile identity within the image which is currently captured by the camera and stored in the gallery. Figure 8.b shows the MyDecryption app home screen. When this app is clicked, it decodes the image currently stored in the gallery and reveals the mobile identity. This identity is again stored as an image and displayed through Picasa photo viewer. The opening request is shown in Figure 8.c.



a. b. c.

Fig. 8. Screen shots of
a) Mcrypt screenshot b) Mdcrypt
c) Opening the stego image

The scrambled revealed identity is displayed in Figure 9. Decrypted version of IMEI number, timestamp, and geolocation of the smartphone are also displayed in Figure 9. This App was tested on Oct 31 2016 Monday (shown in Figure 9). The exact geographical location is identified (using the website www.latlong.net) using the latitude and longitude values of the revealed MI and they are shown in Figure 10. By using the revealed identity information of the mobile from the captured image, the investigation department can easily trace out the abusers.

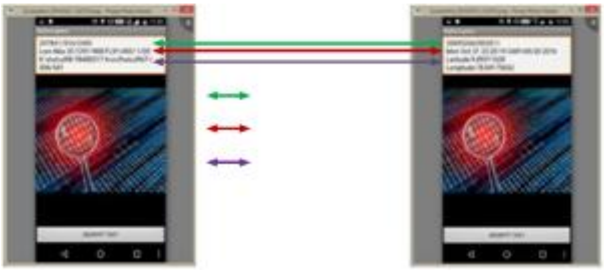
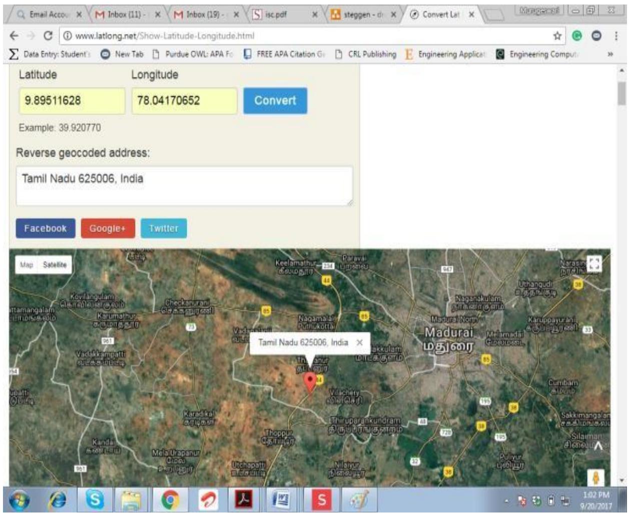


Fig. 9. Screenshot of Mdcode and Mdcrypt output



www.latlong.net/Show-Latitude-Longitude.html

Latitude: 9.89511628
Longitude: 78.04170652
Convert

Example: 39.920770

Reverse geocoded address:
Tamil Nadu 625006, India

Fig. 10. Location identified using latitude and longitude

V. PERFORMANCE EVALUATION OF THE PROPOSED SCHEME

For comparing the performance of the proposed scheme, the Peak Signal to Noise Ratio (PSNR) and Histogram are calculated. PSNR is the accurate metrics used to judge the imperceptibility of stego images. The histogram shows the frequency distribution of a set of continuous data used to inspect the underlying distribution. It also shows the changes made during the embedding process.

B. PSNR Measurement

PSNR is used as a quality measurement between the cover (captured image) and stego (embedded image) images. Here, both cover (X) and stego (Y) images are colorful and JPEG images. The quality of the image is acceptable, if the PSNR value is higher than 30dB. To measure PSNR for color images, the formula given in Equation (1) is used.

$$\mathrm{PSNR}\,(X, Y) = 10\log_{10}\left[\frac{R^2}{MSE}\right] \quad \text{— Eq.1}$$

$$\text{Where, } MSE = \frac{\sum_{M,N}[X(M,N)-Y(M,N)]^2}{M*N} \quad \text{and}$$

$$R = \max\,(\max(X), \max(Y))$$

R is the maximum fluctuation in the input image data type. For example, if the input image has a double-precision floating point data type, then *R* is 1. If it has an 8-bit unsigned integer data type, *R* is 255. Here, R is 255. *M* and *N* are the number of rows and columns in the input images such as cover image (X) and stego image (Y). The MSE represents the cumulative squared error between the stego and the cover image, whereas PSNR represents a meter of the elevation error. The more depressed the value of MSE, the lower the error. If the PSNR is higher, the quality of the stego image is more honest.

For testing purpose, 50 images (taken by Front camera of the mobile) of cover and stego are taken. Once the images are captured, immediately they are embedded with the mobile identity using the proposed MobiSteg. The Captured images are cover images and the images embedded with MI are stego images. Each sample has a pair of one cover and one stego image. images must be in the same size.
For a sample, only the PSNR values for 3 images are calculated as per equation 1 and are recorded in Table 1.

As per the Table 1 for all samples, the PSNR value will be higher (greater than 38 dB) and it is stated that the difference between cover and stego images is too low which will not be noticed by the human eye. Hence, robustness and imperceptibility are maintained between original and embedded images.

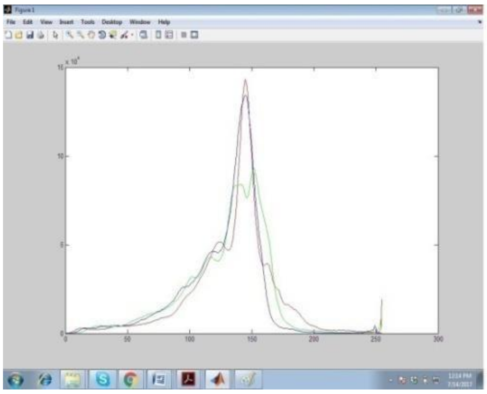
Table 1 PSNR values for the captured images

Samples	Cover Images	Stego Images	PSNR
Sample 1			38.2840
Sample 2			41.9637
Sample 3			46.2824

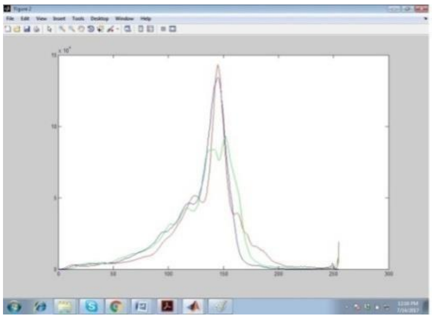
C. Histogram Measurement

Histogram of the color images is measured and plotted in the graph as three curves, that is the red curve for the frequency distribution of red color palette, green curve for the frequency distribution of green color palette and blue curve for the frequency distribution of blue color palette. X axis reflects the range of pixel values of the image and the Y axis shows the number of pixels falls within each range of X; the Y-axis ranges from 0 to the greatest number of pixels deposited in any range. Each one of the sample images has different ranges of color pixels. Hence, the histogram curve of the three samples shows (as shown in Figures 11, 12 and 13) different variations of red, green and blue color frequencies.

Figure 11.a & 11.b shows the histogram measurements for sample 1 of the cover and stego images, respectively. Both the histograms show small curve variation between red, green and blue color pixels and they are almost similar to each other. Hence, embedding has no distortion effect in the cover image.



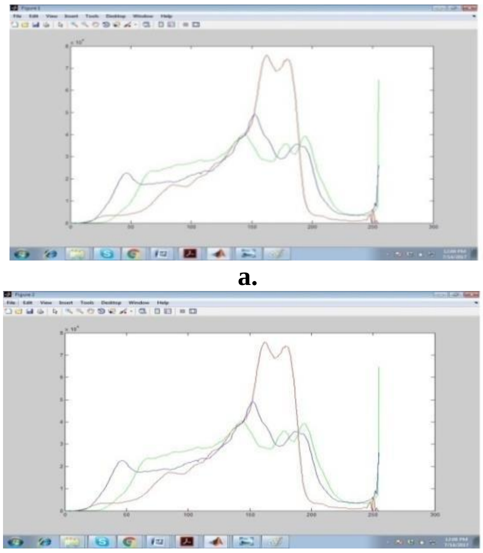
a.



b.

Fig. 11. Histogram Measurement of (a) Cover and (b) Stego of sample 1image

Figure 12.a & 12.b shows the histogram measurements for sample 2 of the cover and stego images, respectively. Both the histograms show small curve variation between green and blue color pixels and there is a large variation in red color pixels. They are almost similar to each other. Hence, embedding has no distortion effect in the cover image.

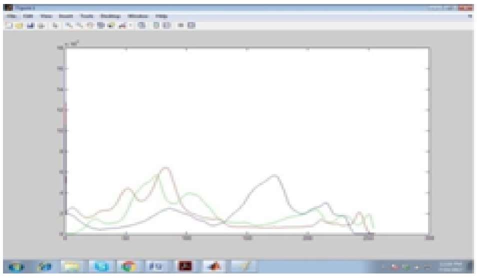


a.

b.

Fig.12. Histogram Measurement of (a) Cover and (b) Stego of sample 2 image

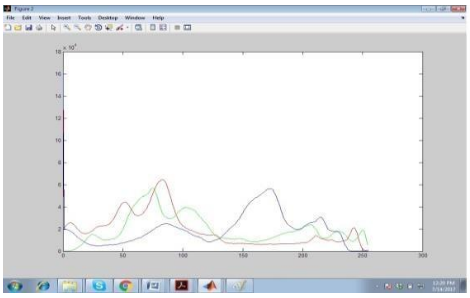
Figure 13.a & 13.b shows the histogram measurements for sample 3 of the cover and stego images, respectively. Both the histograms show small curve variation between green and blue color pixels and there is a large variation in red color pixels. They are almost similar to each other. Hence, embedding has no distortion effect in the cover image.



a.

Retrieval Number: D11261284S219/2019©BEIESP
DOI:10.35940/ijrte.D1126.1284S219

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication



b.

Fig. 13. Histogram Measurement of (a) Cover and (b) Stego of sample 3 image

VI. CONCLUSION

This proposed work is a steganographic application to hide the smartphone identity information in its captured images. By revealing the identity of the mobile, it helps the Information Forensics/Cyber Crime department to track the mobile users easily. Here, the proposed framework MobiSteg runs as a service on the smartphone. Hence, the mobile users don't aware of the running service. Once the mobile is switched on, the proposed service starts automatically.

Images taken for experiments are real time images captured by the front camera of the mobile device only. The proposed work satisfies all the three challenges (security, robustness and payload) of steganography (proved by the experiments) and it can be the best one. If the smartphone industries come forward to implement this feature in their products, then the mobile abusers can be easily identified.

The proposed application runs only on Android OS, and can handle images captured only by front camera. It can be extended in future for video and audio whenever they are captured by the smartphone. It can also be extended for higher version of Android and higher megapixels smartphone cameras.

REFERENCES

1. C. Danuputri, T. Mantoro and M. Hardjianto, Data Security Using LSB Steganography and Vigenere Chiper in an Android Environment, Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensics(CyberSec 2015), Jakarta, Indonesia, 2015,pp. 22-27.
2. S. Dhanawe and S. Doshi, Hiding file on Android mobile and sending APK file through Whats app using steganography and compression techniques, International Conference on Signal Processing, Communication, Power and Embedded System, Paralakhemundi, India, 2016, pp. 106 - 110.
3. T. Mantoro, D. Permadi and A. Abubakar,Stegano-image as a digital signature to improve security authentication system in mobile computing, International Conference on Informatics and Computing, Mataram, Indonesia, 2016,pp. 158-163.
   S. Majumdar, A. Maiti and A. Nath, New Secured Steganography Algorithm using Encrypted Secret Message inside QRTM Code: System Implemented in Android Phone, International Conference on Computational Intelligence and communication Networks, Jabalpur, India, 2015, pp. 1130 - 113.
4. M. Shirali-Shahreza, Stealth steganography in SMS, IFIP International Conference on Wireless and Optical Communications Networks, Bangalore, India, 2006, pp. 1–5.
5. M. Shirali-Shahreza and M. Hassan Shirali-Shahreza, Text steganography in SMS, International Conference on Convergence Information Technology, Gyeongju, Korea, 2007, pp. 2260–2265.
6. M. Hassan Shirali-Shahreza and M. Shirali-Shahreza, Sending mobile software activation code by SMS using steganography, Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Kaohsiung, Taiwan, 2007, pp. 554–557.
7. K. Farhan Rafat, Enhanced text steganography in SMS, Second International Conference on Computer, Control and Communication, Karachi, Pakistan, 2009, pp. 1–6.
8. M. Hassan Shirali-Shahreza and M. Shirali-Shahreza, Steganography in SMS by Sudoku puzzle, IEEE/ACS International Conference on Computer Systems and Applications, Doha, Qatar, 2008, pp. 844–847.
9. Wesam S. Bhaya, Text Hiding in Mobile Phone Simple Message Service Using Fonts, Journal of Computer Science, Vol.7 (11), pp. 1626-1628, November 2011.
10. K. Papapanagiotou, E. Kellinis, G. F. Marias, and P. Georgiadis, Alternatives for multimedia messaging system steganography, In: Hao Y. et al. (eds) Computational Intelligence and Security. Lecture Notes in Computer Science, Vol. 3802, pp. 589-596, Springer, Berlin, Heidelberg, December 2005.
11. M. Shirali-Shahreza, Steganography in MMS, IEEE International Multitopic Conference, Lahore, Pakistan, 2007, pp.1–4.
12. R. P. Singh, M. A. Alam Khan, M. Khan and N. Singh, Spread spectrum image steganography in multimedia messaging service of mobile phones, International Journal of Electronics Engineering, Vol. 2(2), pp. 365–369, December 2010.
13. A. S. Nori and S. A. Baker, Data Hiding over Mobile Phones using Socket Network Communication, International Journal of Computer Science Issues, Vol. 10, Issue 6, No 1, pp. 201-208,November 2013.
14. V. Iranmanesh, H. J. Wei, S. L. Dao-Ming and O. A. Arigbabu, On using Emoticons and Lingoes for Hiding Data in SMS, in International Symposium on Technology Management and Emerging Technologies, Langkawi, Kedah, Malaysia,2015, pp. 103-107.
15. A. Gupta, A. Dadlani, R. Malhotra and Y. Bansal, A novel scheme to hide identity information in mobile captured images, In: D. Wyld, J. Zizka, D. Nagamalai (eds) Advances in Computer Science, Engineering & Applications. Advances in Intelligent and Soft Computing, Vol. 166, pp. 403-411, Springer, Berlin, Heidelberg, May 2012.

AUTHORS PROFILE

Murugeswari Kandavel received her BE in Computer Science and Engineering and MTech in Information Technology in 1996 and 2003, respectively, from Madurai Kamaraj University and University of Punjab. She started her carrier as a Lecturer in 1997 and continues her service in teaching field. Currently, she is working as an Associate Professor in Kalasalingam Academy of Research and Education, Tamil Nadu,India.

Ganesan Govindan is an Associate Professor in Computer Science and Engineering Department, K.L.N College of Information Technology, Sivagangai. He obtained his BE degree in Computer Science and Engineering from Madurai Kamaraj University and ME degree in Computer Science and Engineering from Anna University, Chennai in the year 1990 and 2005, respectively. His research interests include cloud computing, information security, steganalysis and soft computing techniques. He had published more than 15 publications in the area of grid computing and information security.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication