Digital Media Steganography Approach to Modern Smartphone

Nilam Kishor Mahajan.
Student (BE), Department Of Computer Science & Engineering,
Shri Sant Gadge Baba college of engineering, Bhusawal, North Maharashtra University,
Jalgaon,Maharashtra, India.

Abstract: By means of donation sophisticated services and centralize a huge degree of special data, modern smartphones changed the technique we mix divert and vocation. To this aim, they rely upon complex hardware/software frameworks leading to a digit of vulnerabilities, attack and hazard to side view individuals or gather sensitive information. However, the bulk of machinery evaluate the safekeeping degree of smartphones neglects steganography, which can be mainly used to: i) exfiltrate private facts by camouflage methods, and ii) conceal valuable or personal information into innocent looking carriers.

Keywords: Steganography, Smartphones, Covert Channels, Information Hiding, Security.

I. INTRODUCTION

The fast technical advance of software and hardware lead to mobile phones offering capabilities previously achievable only for desktop computers or laptops. The increasing convergence of network services, computing/storage functionalities, and complicated Graphical User Interfaces (GUIs) culminate interested in fresh policy called smartphones, which are quickly becoming the first choice to access the Internet, and for entertainment. but, the Bring Your Own Device (BYOD) example make them center tools in the daily working routine.

This popularity is mainly driven by a multi-functional flavor combine lots of skin texture, such as a high-resolution camera, unlike air interfaces (e.g., Bluetooth, 3G and IEEE 802.11),with Global Positioning System (GPS) addicted to a unique device. To lever the hardware, the characteristic in service scheme (OS) has planning exceptionally lock to the one old on top of desktops [4]. Then, the resulting vast user base ignited the expansion of numerous application deliver from online stores, or through specialized sources on the Web. Even if parallel hardware/software platform be at the base of a extra general class of smart devices (e.g., tablets), to keep away from cannibalization of advertise shares, many products do not implement the 3G/telephony sub-system. Yet, for the sake of cleanness, we make use of smartphone as an sunshade term, despite when doubts arise.

II. LITERATURE SURVEY

Chung et al. [1] is propose to transform secret data into a QR code, and then embed it in a digital image by performing the Discrete Cosine Transform (DCT) which is a normally old method to decor relate the image data.A. Choche and H. R. Arabnia [2] are also proposed similar approaches the former utilized QR code encryption using 3 DES (Data Encryption Standard) for superior protection and next the LSB to set in resultant data into a covert image. Wu et al. [3],is proposed by where author rely happening steganography near secrete the presence of the QR code for aesthetic purposes.

In this perspective, Bao and Xiao Hu [4] discuss an mp3-resistant method to protect the secret data by means of a well-suited a-priori treatment of the dynamic range of the uncompressed auditory entity.Mozo et al. [5]

investigate the alteration of Flash Videos (.flv), which are appropriate general remaining toward the status among users of sites like YouTube.

III. STEGANOGRAPHY BASICS AND ITS EVALUAION

A. Definitions and Goals

Steganography is the process of embedding secret messages into an not guilty look delivery service, definite as Steganographic or else hidden data carrier. Its importance increases with the ubiquitous availability of digital in order, because the process to bring in information is unfair by how communication methods evolve, e.g., as of mail on paper through concerned ink, to computer networks.

B. Fundamental Properties

All Steganographic methods exchanging data among two endpoints canister be there characterize by the following properties (also obvious as show index):

- Steganographic bandwidth (before aptitude): it is the volume of secret data sent per time unit by using a given method;
- detectability (or security): it is the inability to detect a steganogram within a certain carrier (e.g., by comparing the statistical properties of the captured data with the typical known values for the carrier);
- robustness: it is the amount of alterations a steganogram can with stand without destroying the embedded secret data.

IV. SMARTPHONE OBJECTS METHODS

since discuss, current plans can liberate and control audio plus video, take high-resolution pictures and create transcript by full-featured speech processors. in addition, the Software as a Service (SaaS) paradigm allows editing contents even in presence of resource limited devices. As briefly introduced in Section IV-D, smartphones offer a range of carrier to push in covert data, being a relevant platform for exploiting the so called digital media steganography.
a multiplicity of Methodsimagery, QR system, audio, video, text.

V. MITIGATION TECHNIQUES

As said, steganography leads to multifaceted privacy and security implications, thus a part of the research is de-voted to reveal or prevent covert communications. Generally, steganography mitigation techniques aim at: i) detecting, ii) eliminating, and iii) limiting the Steganographic bandwidth (or capacity) of a covert channel. Especially, for i) there is a well-defined research area called steganalysis, while for ii) and iii) the lack of universal solutions stems countermeasures tightly coupled with the specific information hiding technique.

CONCLUSION

Modern smartphones are an excellent playground for the development of new steganographic methods, and also, as a consequence of their importance, they will be likely to become one of the most targeted platforms for data exfiltration. To classify the work done, we developed taxonomy to partition methods in three covert channels, and we also evaluated possible countermeasures.

ACKNOWLEDGEMENT

I feel great pleasure in submitting this Paper on "Steganography in Modern Smartphones and Mitigation Technique"**.** I wish to express true sense of gratitude towards my H.O.D., Prof. D. D. Patil. I also wish to thank my teacher Prof. R.R.Singh who at very discrete step in preparation of this Paper contributed his valuable guidance and help to solve every problem that arose.

Also, most likely I would like to express my sincere gratitude towards my family for always being there when I need them the most. With all respect and gratitude, I would like to

thank all the people, who have helped me directly or indirectly. I owe my all success to them.

REFERENCES

[1] C. H. Chung, W. Y. Chen, C.-M. Tu, "Image Hidden Technique Using QR Barcode", in Proceedings of Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 522 – 525, Kyoto, Japan, Sept. 2009.

[2] A. Choche and H. R. Arabnia, "A Methodology to Conceal QR Codes for Security Applications", in Proceedings of International Conference on Information and Knowledge Engineering (IKE'11), Las Vegas, USA, July 2011.

[3] W. -C. Wu, Z. -W. Lin and W. -T.. Wong, "Application of QR-Code Steganography Using Data Embedding Technique", in J. J. Hyuk Park et al. (Eds.), Information Technology Convergence, Lecture Notes in Electrical Engineering, vol. 253, pp. 597-605, DOI: 10.1007978-94-007-6996-0_63, 2013.