Scope International Journal of Science, Humanities, Management and Technology. ISSN : 2455-068X

Vol.3 Issue 4 (2017) 152 - 156. Submitted 25/11/2017. Published 30/12/2017

DATA ASSISTED COMMUNICATION OF MOBILE IMAGE (DAC-MOBI)

[1]E. Madhu Suriya, M.Phil Scholar, Department of Computer Science, Bharathiyar Arts and Science college for Women, Deviyakurichi, Thalaivasal, Salem.

[2]R. Vasugi, Assistant Professor, Department of Computer Science, Bharathiyar Arts and Science college for Women, Deviyakurichi, Thalaivasal, Salem.

Abstract:

Mobile devices perform an array of functions ranging from a simple telephony device to those of a personal computer. Designed for mobility, they are compact in size, battery-powered, and lightweight. Most mobile devices have a basic set of comparable features and capabilities. They house a microprocessor, read only memory (ROM), random access memory (RAM), a radio module, a digital signal processor, a microphone and speaker, a variety of hardware keys and interfaces and a liquid crystal display (LCD). The operating system (OS) of a mobile device may be stored in either NAND or NOR memory while code execution typically occurs in RAM.

Keywords: ROM, RAM, Radio Module, NAND.

1. INTODUCTION

Currently, mobile devices are equipped with system-level microprocessors that reduce the number of supporting chips required and include considerable internal memory capacity currently up to 64GB (e.g., Stacked NAND). Built-in Secure Digital (SD) memory card slots, such as one for the micro Secure Digital eXtended Capacity (microSDXC), may support removable memory with capacities ranging from 64GB to 2TB of storage. Non-cellular wireless communications such as infrared (i.e., IrDA), Bluetooth, Near Field Communication (NFC), and WiFi may also be built into the device and support synchronization protocols to exchange other data (e.g., graphics, audio, and video file formats). Different mobile devices have different technical and physical characteristics (e.g., size, weight, processor speed, memory capacity). Mobile devices may also use different types of expansion capabilities to provide additional functionality. Furthermore, mobile device capabilities sometimes include those of other devices such as handheld Global Positioning Systems (GPS), cameras (still and video) or personal computers. Overall, mobile devices can be classified as feature phones that are primarily simple voice and messaging communication devices or smartphones that offer more advanced capabilities and services for multimedia, similar to those of a personal computer. Both feature phones and smartphones support voice, text messaging, and a set of basic Personal Information Management (PIM) type applications including phonebook and calendar facilities. Smartphones add PC-like capability for running a wide variety of general and special-purpose applications. Smartphones are typically larger than feature phones, support higher video resolutions (e.g., ~300 PPI) and may have an integrated QWERTY keyboard or touch sensitive screen. Smartphones generally support a wide array of applications, available through an application storefront. Table 2 lists the differences in software capabilities found on these device classes.

2. RELATED WORK

Mobile devices contain both non-volatile and volatile memory. Volatile memory (i.e., RAM) is used for dynamic storage and its contents are lost when power is drained from the mobile device. Non-volatile memory is persistent as its contents are not affected by loss of power or overwriting data upon reboot. For example, solid-state drives (SSD) that stores persistent data on solid-state flash memory. Mobile devices typically contain one or two different types of non-volatile flash memory. These types are NAND and NOR. NOR flash has faster read times, slower write times than NAND and is nearly immune to corruption and bad blocks while allowing random access to any memory location.

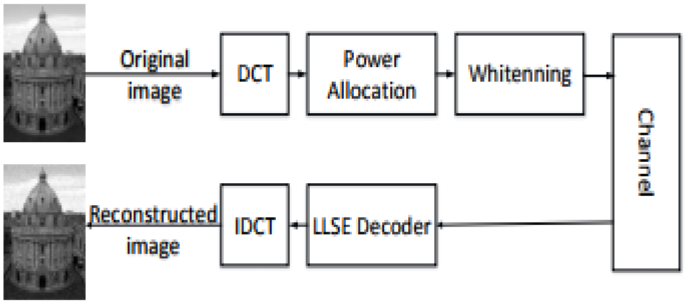

Fig.1.Block Structure

NAND flash offers higher memory storage capacities, is less stable and only allows sequential access. Memory configurations among mobile devices have evolved over time. Feature phones were among the first types of devices that contained NOR flash and RAM memory. System and user data are stored in NOR and copied to RAM upon booting for faster code execution and access. This is known as the first generation of mobile device memory configurations. As smartphones were introduced, memory configurations evolved, adding NAND flash memory. This arrangement of NOR, NAND and RAM memory is referred to as the second generation. This generation of memory configurations stores system files in NOR flash, user files in NAND and RAM is used for code execution. NOR flash memory includes system data such as: operating system code, the kernel, device drivers, system libraries, memory for executing operating system applications and the storage of user application execution instructions. NOR flash will be the best location for data collection for first generation memory configuration devices. NAND flash memory contains: PIM data, graphics, audio, video, and other user files. This type of memory generally provides the examiner with the most useful information in most cases. NAND flash memory may leave multiple copies of transaction-based files (e.g., databases and logs) due to wear leveling algorithms and garbage collection routines. Since NAND flash memory cells can be re-used for only a limited amount of time before they become unreliable, wear leveling algorithms are used to increase the life span of Flash memory storage, by arranging data so that erasures and re-writes are distributed evenly across the SSD.

3. PROPOSED SYSTEM

Identity modules (commonly known as SIM cards) are synonymous with mobile devices that interoperate with GSM cellular networks. Under the GSM framework, a mobile device is referred to as a Mobile Station and is partitioned into two distinct components: the Universal Integrated Circuit Card (UICC) and the Mobile Equipment (ME). A UICC, commonly referred to as an identity module (e.g., Subscriber Identity Module [SIM], Universal Subscriber Identity Module [USIM], CDMA Subscriber Identity Module [CSIM]), is a removable component that contains essential information about the subscriber. The ME and the radio handset portion cannot fully function without a UICC. The UICC's main purpose entails authenticating the user of the mobile device to the network providing access to subscribed services. The UICC also offers storage for personal information, such as phonebook entries, text messages, last numbers dialed (LND) and service-related information. The slot for the UICC card is normally not accessible from the exterior of the mobile device to protect insertion and removal as with a memory card. Instead, it typically is found beneath the battery compartment. When a UICC is inserted into a mobile device handset and pin contact is made, a serial interface is used for communicating between them.

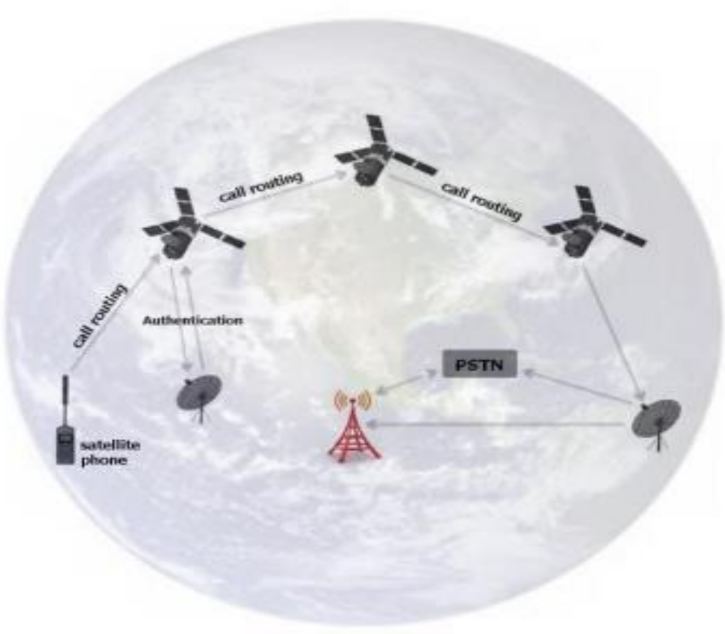

Fig.2.Network

In most cases, the UICC should be removed from the handset first and read using a Personal Computer/Smart Card (PC/SC) reader. Removal of the UICC provides the examiner with ability to read additional data that may be recovered (e.g., deleted text messages). Authenticating a device to a network securely is a vital function performed via the UICC. Cryptographic key information and algorithms within the tamper resistant module provide the means for the device to participate in a challenge-response dialogue with the network and respond correctly, without exposing key material and other information that could be used to clone the UICC and gain access to a subscriber's services. Cryptographic key information in the UICC also supports stream cipher encryption to protect against eavesdropping on the air interface.

4. ANALYSIS

Mobile devices that do not require a UICC are relatively straightforward as the acquisition entails a single device. Mobile devices requiring UICCs are more complex. There are two items that must be examined: the handset and the UICC. Depending on the state of the mobile device (i.e., active, inactive) the handset and UICC may be acquired jointly or separately. It is generally accepted to process the UICC first while the device is in an inactive state.

If the mobile device is active, a joint acquisition of the handset and UICC contents should be acquired first. A direct acquisition recovers deleted messages present on a UICC, while an indirect acquisition via the handset does not. The UICC must be removed from the mobile device and inserted into an appropriate reader for direct acquisition. When data protection is active, the file key is obliterated when the file is deleted, leaving encrypted and generally unrecoverable file contents in unallocated space, which render traditional carving techniques for deleted files useless.

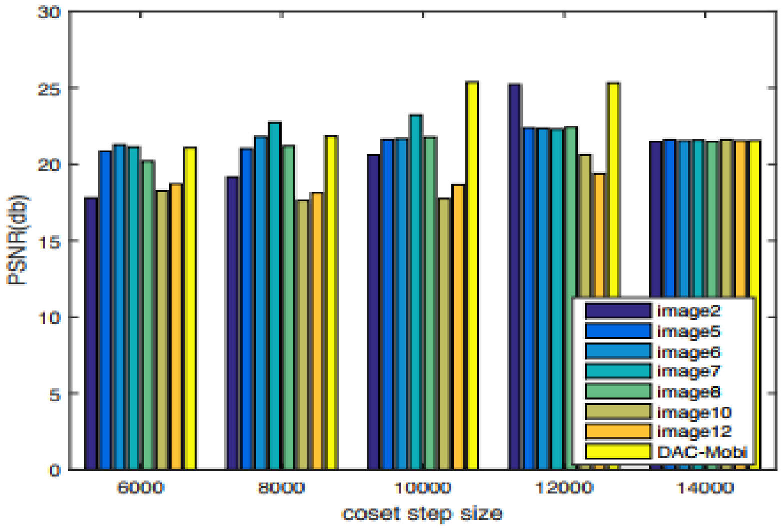

Fig.2.Output

Data however can often be found residing inside allocated data containers (i.e., SQLite Tables) and should not be discounted or ignored as part of any examination. Recovery of such data can be challenging as SQLite data recovery may be somewhat automated (e.g., epilog), often manual recovery may be the only option. Fortunately for the forensic investigator, a significant portion of user data is stored within allocated data containers and garbage collection is not generally performed on these containers. Many tools are able to parse much of the information presented in the Android OS however all tools suffer the same problem as iOS based devices -- multitudes of applications. Hundreds of applications are added every week. Understanding and reverse engineering each one of them one-at-a-time is a time consuming process. Many vendors have chosen to focus on parsing the data from the more popular communication applications (e.g., WhatsApp, FaceBook, etc.). The more advanced examiner should be aware of this shortcoming and be prepared to perform testing and reverse engineering for some cases where support for specific applications may not yet exist.

CONCLUSION

In this paper, a novel data-assisted communication of mobile image (DAC-Mobi) framework is proposed, Dis- tributed Source Coding (DSC) and denoising are explored as two key techniques to exploit cloud information in this framework. In the proposed scheme, the DSC divides the image to be transmitted into three layer bit planes, the MSB of partial low frequency DCT coefficients are sent in digital modulation, the remaining MSB and all middle bit plane are discarded to save transmission power, the LSB are transmitted in pseudo analog modulation. The receiver uses digitally decoded MSB and analog demodulated LSB to recover a small down-sampled image, then extracts features, and retrieves correlated (similar) image in cloud. The retrieved images are used for DSC decoding and denosing. We further analyse how to select Coset coding parameter, and coordinate the power allocation and external denosing.

REFERENCES

[1] X. Liu, L. Wan, Y. Qu, T.T. Wong, S. Lin, C.S. Leung, and P.A. Heng. Intrinsic Colorization. ACM Trans. Graph., 27(5):152:1–152:9, Dec. 2008.

[2] J. Sivic O. Whyte and A. Zisserman. Get Out of my Picture! Internet-based Inpainting. British Machine Vision Conference, 2009.

[3] J. Hays and A. A. Efros. Scene Completion Using Millions of Photographs. ACM Trans. Graph., 26(3), Jul. 2007.

[4] T. Chen, M.M. Cheng, P. Tan, A. Shamir, and S.M. Hu. Sketch2Photo: Internet Image Montage. ACM Trans. Graph., 28(5):124:1– 124:10, Dec. 2009.

[5] M. Eitz, R. Richter, K. Hildebrand, T. Boubekeur, and M. Alexa. Photosketcher: Interactive Sketch-Based Image Synthesis. Computer Graphics and Applications, IEEE, 31(6):56–66, Nov. 2011.

[6] M.K. Johnson, K. Dale, S. Avidan, H. Pfister, W.T. Freeman, and W. Matusik. CG2Real: Improving the Realism of Computer Generated Images Using a Large Collection of Photographs. IEEE Trans. Vis. Comput. Graphics, 17(9):1273–1285, Sept. 2011.

[7] S. Jakubczak and D. Katabi. A Cross-Layer Design for Scalable Mobile Video. In Proc. 17th Annu. ACM Int. Conf. Mobile Comput. and Netw. (MobiCom'11), pages 289–300. ACM, 2011.