Temple University
College of Science and Technology
Computer and Information Sciences

Android-Stego: A Novel Service Provider Imperceptible MMS Steganography Technique Robust to Message Loss

Presenter: Lei Chen

Authors:
Avinash Srinivasan, Jie Wu, and Justin Shi
Temple University
Computer and Information Sciences
Philadelphia – USA

Presentation Roadmap

- Background
- Steganography 101
- Android-Stego
  - Overview, Salient Features, Process
  - Implementation
  - Robust to Operator Manipulation
- Conclusion

Background

- Information hiding (IH) –
  - extensively researched for over two decades
- Steganography –
  - one type of IH
  - yet to be fully explored on smartphones over cellular carrier networks
- Smartphones –
  - epitome of ubiquitous and pervasive computing
  - continue being the locus of *one-device-for-all-needs*
  - make steganography an easily accessible CC channel.

Steganography 101

- The practice of concealing messages or information within other non-secret text or data.
- Simple embedding techniques –
  - data are often hidden through the use of mathematical techniques
  - imperceptible to the naked eye
- Sophisticated embedding techniques –
  - degradation in quality
  - payload change are perceptible

- Steganography + Encryption
  - problem just got harder…..rather lot harder
- Message encryption –
  - substantially harder to detect, extract, and recover message.
  - harder to use entropy-based statistical analysis
  - all encrypted data have very high entropy
    - 7.5 - 8.0 bits-per-byte

- Steganography drawbacks
  - Broad techniques have remained unchanged
  - Offer limited number of possibilities and algorithms

Steganography – Key Requirements

- Cover file should be popular – its usage should not in itself be considered an anomaly.
  - AndroidStego meets this requirement.

- Resultant modifications to the cover file should be imperceptible to a third-party
  - AndroidStego meets this requirement.

Android-Stego Prototype

Assumptions and Threat Model

- Alice (sender) and Bob (receiver) use a PKI-based digital certificate for mutual authentication.

- Alice and Bob can negotiate a shared session key spontaneously over an unsecured communication channel.

- Unsecured channel is a channel that is vulnerable to sniffing/monitoring by – service provider, attacker, etc.

Process Overview

- Splitting and encoding a secret message on the sender side
  - can be multi-part depending on message size; operator restrictions
- Encoded secret message successfully traverses the cellular networks
  - transparent to network restrictions and operator manipulations
- Decoding the received secret message on the receiver side
  - reassembly necessary if it is a multi-part message

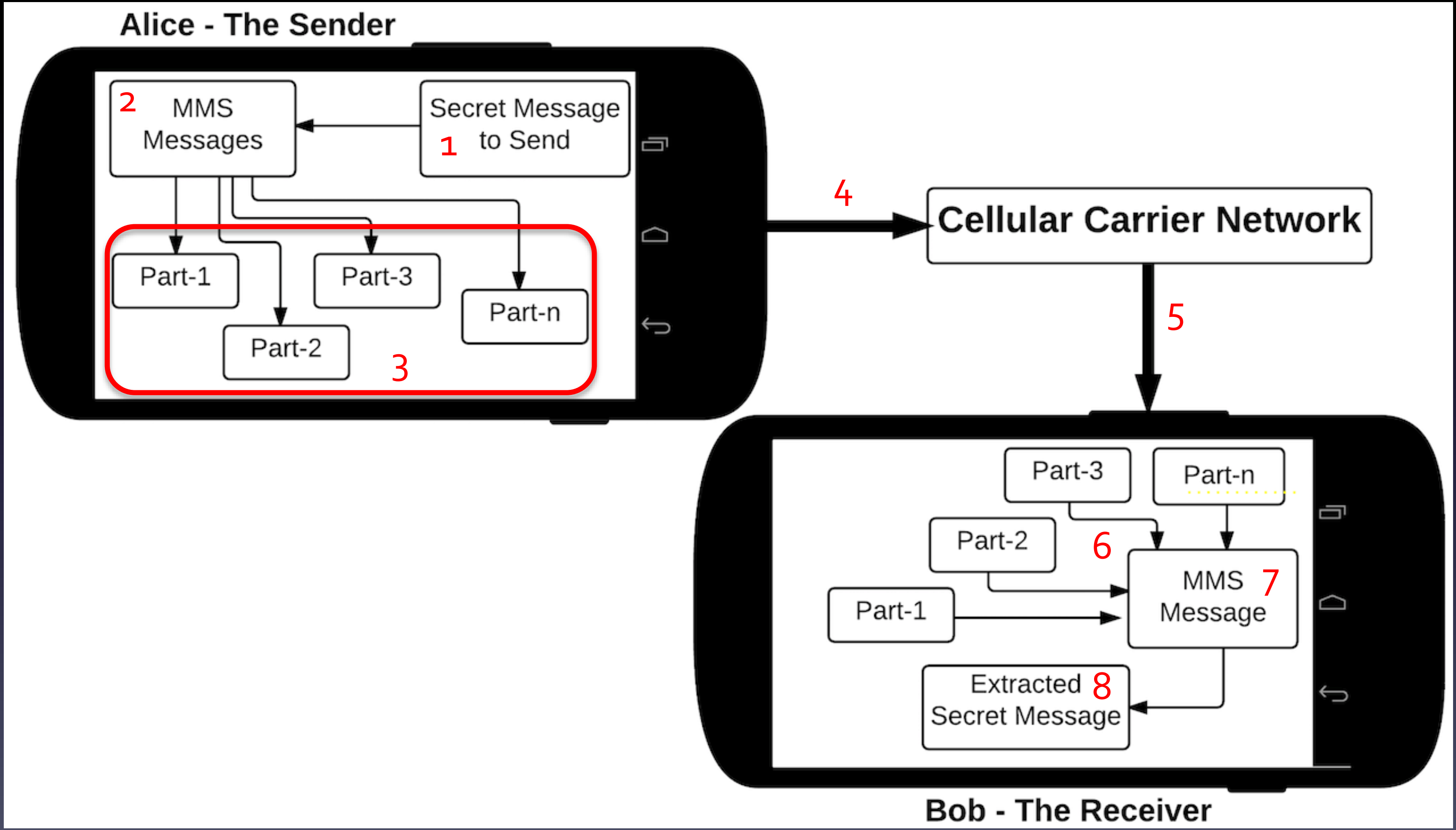
Android-Stego Implementation

- Insertion of a secret message into a single instance of the cover file is upper bound by the imperceptibility threshold (T_{imp}) to modifications.

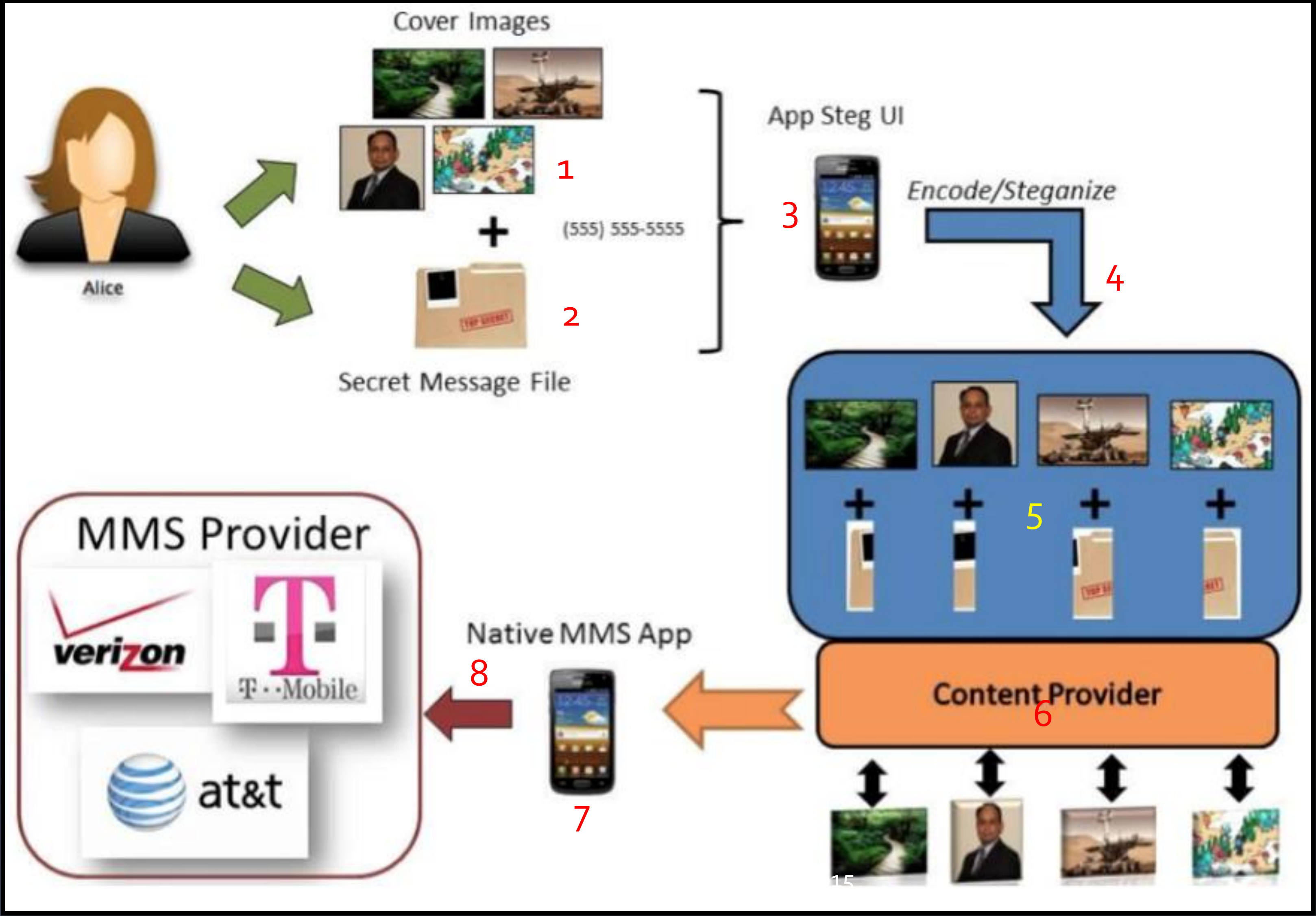
- AndroidStego meets this requirement by incorporating:
  - multi-part, segmented, and distributed capabilities into the LSB encoding algorithm.
  - can hide arbitrary binary data of arbitrary length – additional cover file instances are used if the secret message size > T_{imp}

- Prototype is features:
  - robust to message loss resulting from cellular operator manipulations of MMS messages.
  - a segmented and distributed implementation built with LSB as the core encoding technique.
- Prototype implementation-
  - real world working prototype – custom LSB implementation
  - modular, built with existing Android APIs
  - new features can be easily introduced, making it more capable in hiding, as well as robust to detection

Generating MMS Stego



Embedding Secret Message



Extracting Secret Message

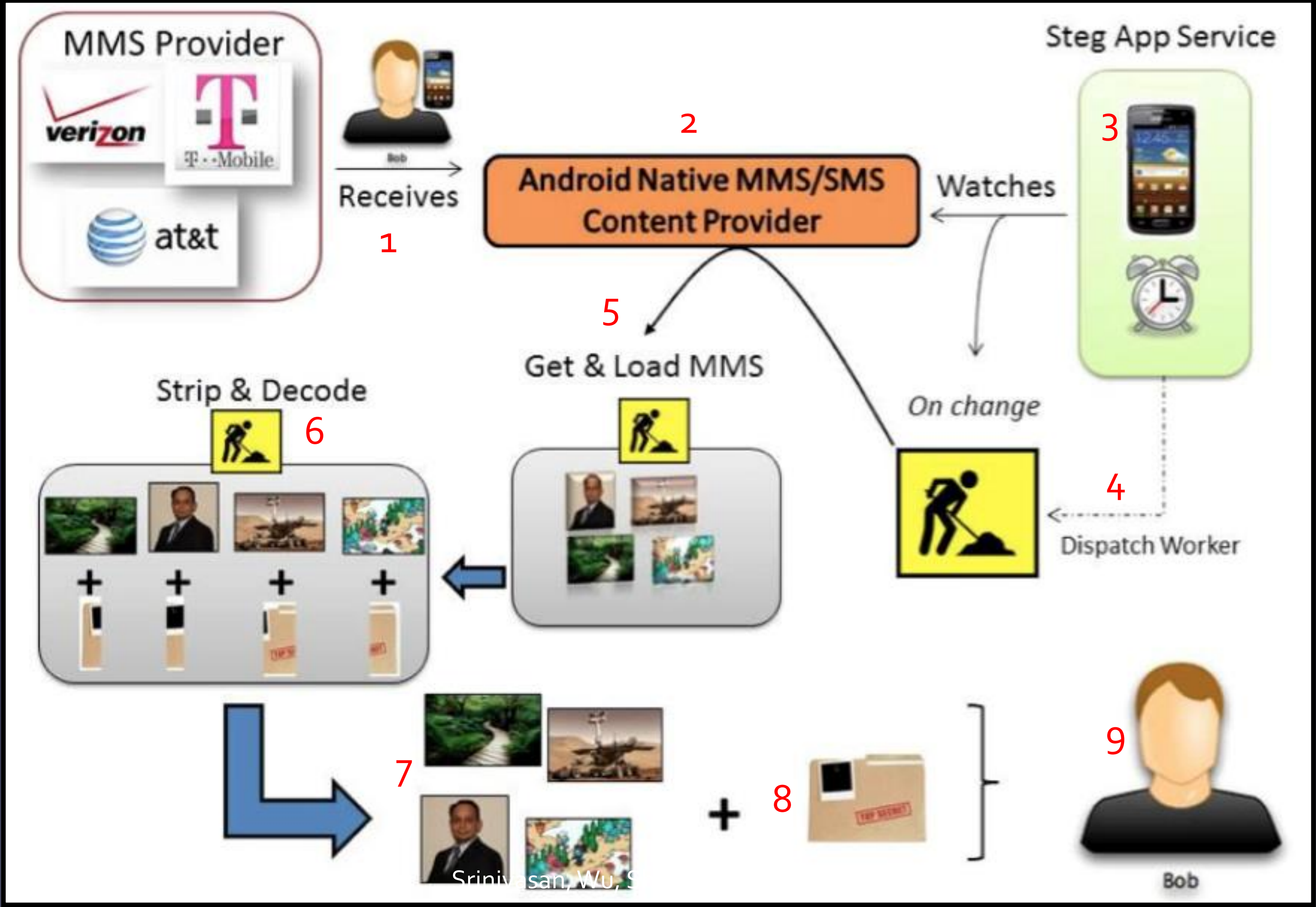
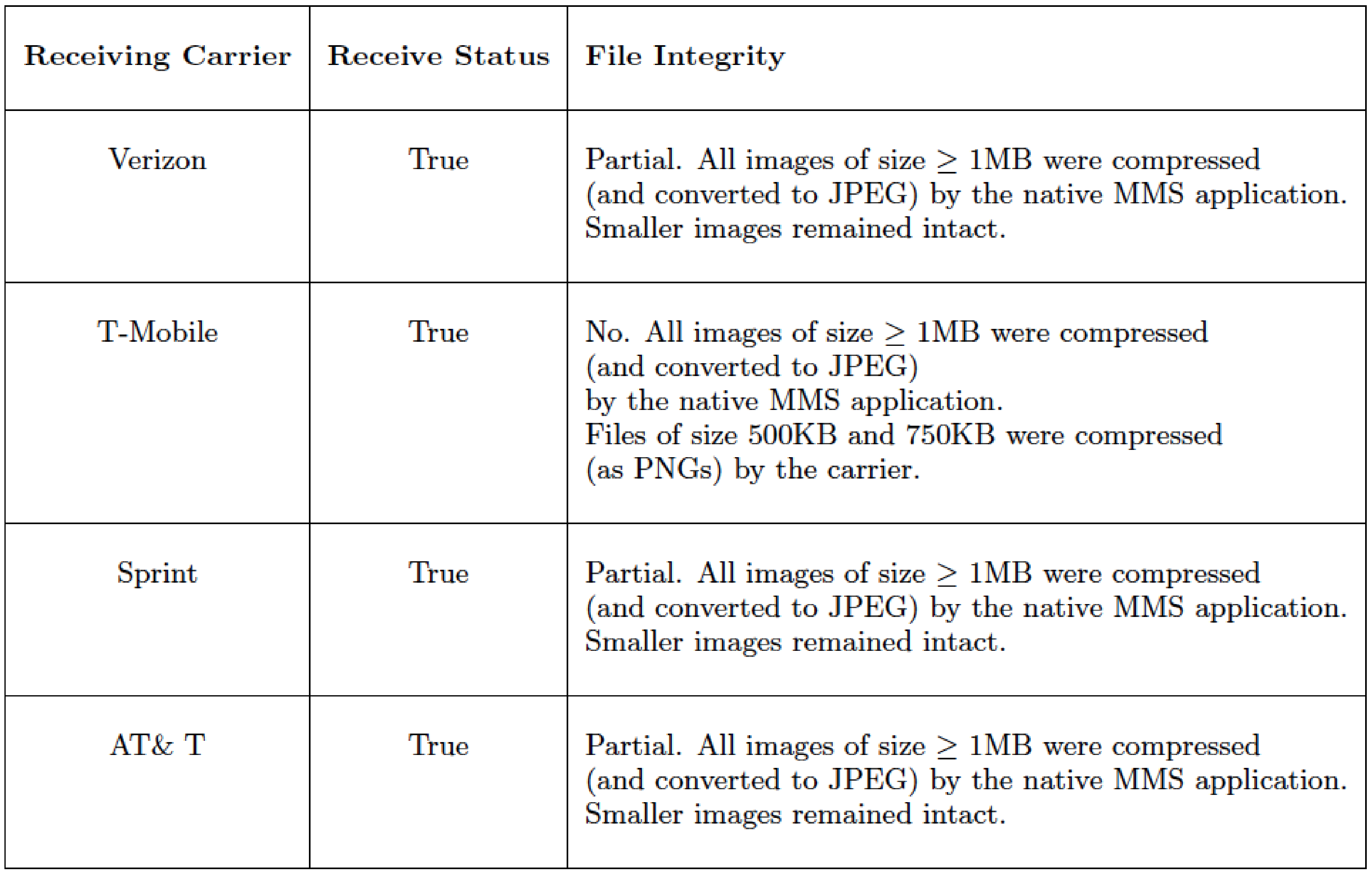


Table 2: Summary of cellular carrier restriction on in-coming MMS message size for four major cellular service providers in North America.



Receiving Carrier	Receive Status	File Integrity
Verizon	True	Partial. All images of size ≥ 1MB were compressed (and converted to JPEG) by the native MMS application. Smaller images remained intact.
T-Mobile	True	No. All images of size ≥ 1MB were compressed (and converted to JPEG) by the native MMS application. Files of size 500KB and 750KB were compressed (as PNGs) by the carrier.
Sprint	True	Partial. All images of size ≥ 1MB were compressed (and converted to JPEG) by the native MMS application. Smaller images remained intact.
AT& T	True	Partial. All images of size ≥ 1MB were compressed (and converted to JPEG) by the native MMS application. Smaller images remained intact.

Conclusion(s)

- Smartphones will increasingly be the locus of *one-device-for-all-needs.*
- Steganography most easily accessible alternative for covert communication over smartphones.
- Built a real-world working prototype – robust to cellular operator manipulations of MMS messages – results of of our prototype's survival over four major cellular operators in North America has been analyzed and presented.