Mobile App

ObscuraCam

In un mondo di video virali e il riconoscimento facciale, ObscuraCam consente di condividere
foto e video, proteggendo la privacy vostra e di coloro che si preoccupano.

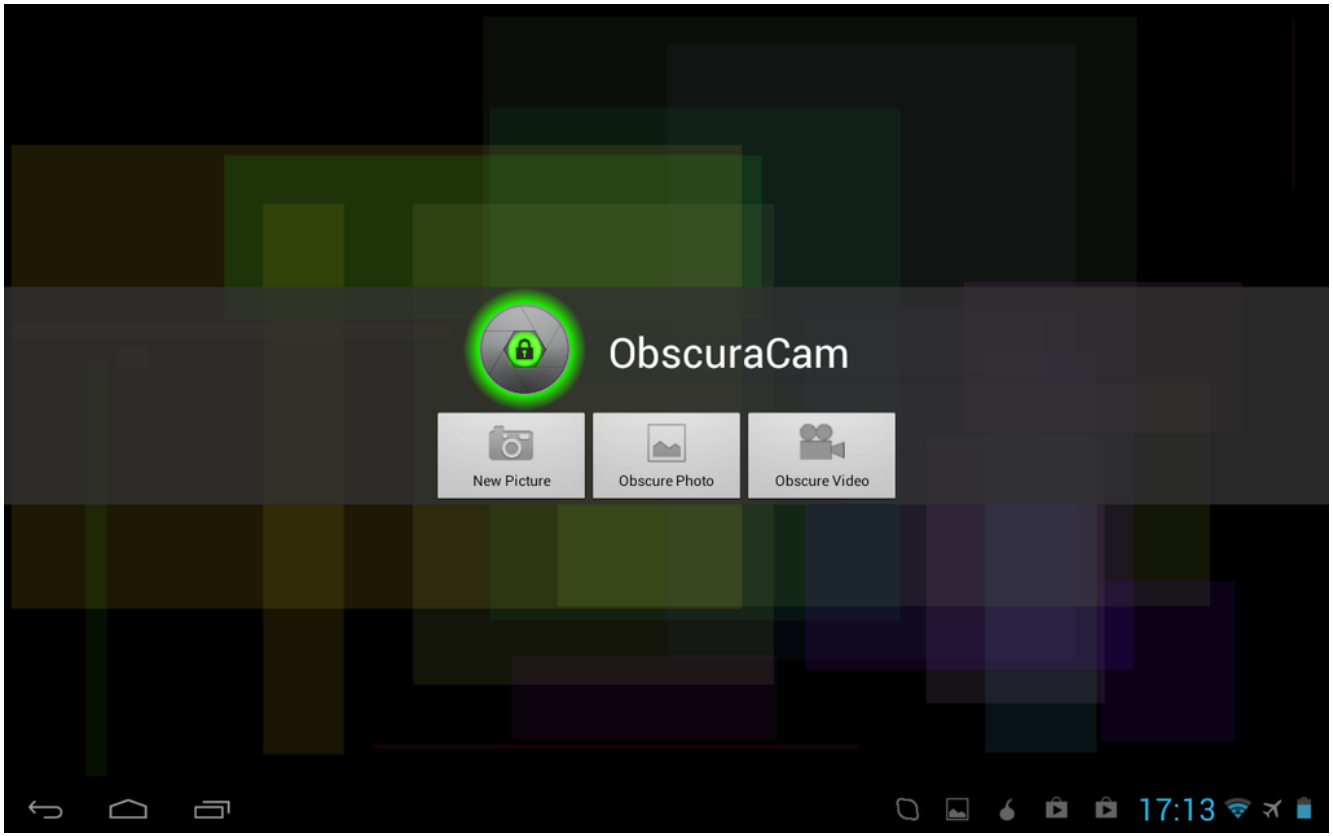
Con ObscuraCam si può offuscare e travisare volti nelle foto e nei video.

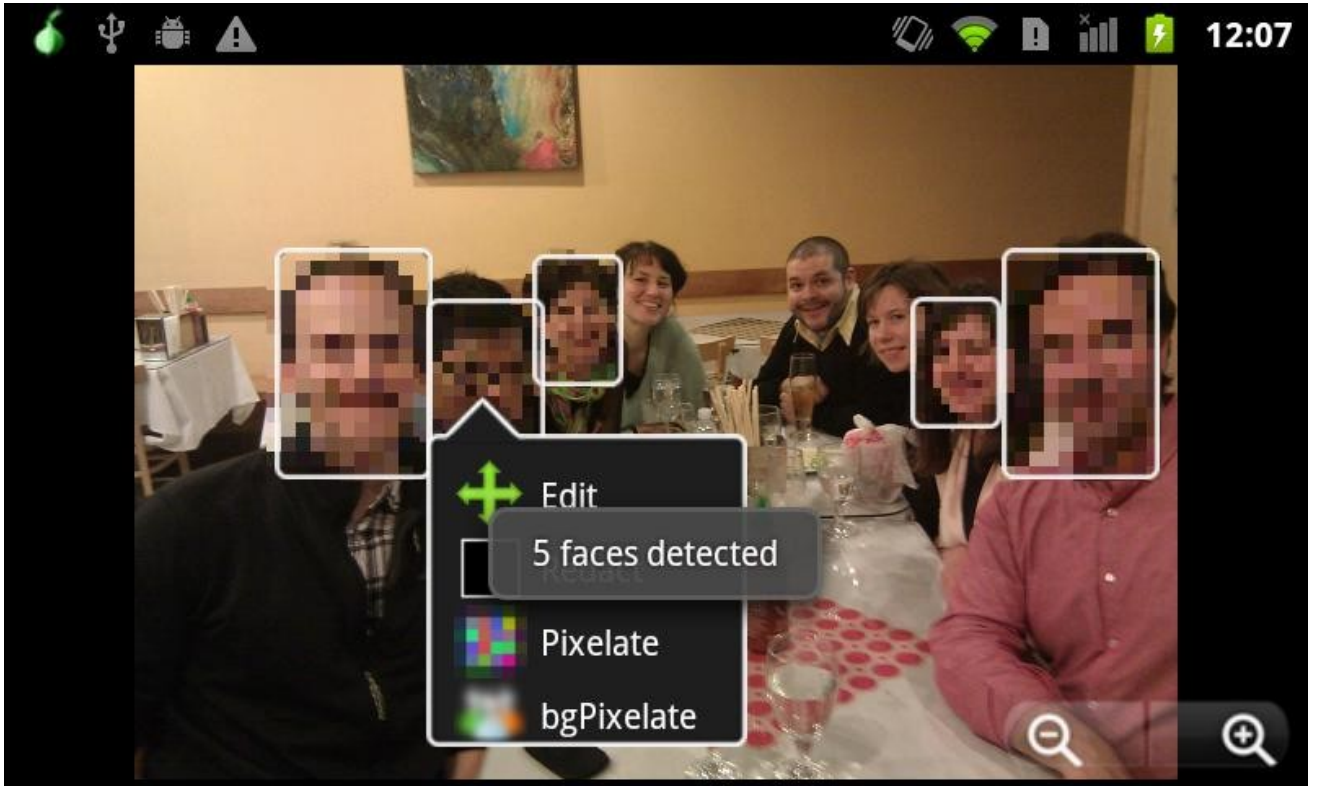
Le informazioni che potrebbero identificare l'utente come cameraman (METADATI) vengono rimosse dal file per una maggiore sicurezza.

★ PRIVACY PER LE TUE FOTO: ObscuraCam può essere usato come una macchina fotografica per scattare foto, o per anonimizzare foto e video che hai effettuato precedentemente.

★ TRAVISAMENTO: Copertura delle facce con pixel, oscurare o possibilità di aggiunta di altri effetti.

★ RILEVAMENTO AUTOMATICO VOLTI: ObscuraCam rileva automaticamente i volti in foto e video, in modo da poter essere anonimi rapidamente e facilmente in una folla o un video lungo.





★ MODALITÀ PRIVACY MULTIPLE: Le facce possono essere pixelate, completamente rimosse o camuffate. Si può anche offuscare tutto tranne una piccola porzione di un'immagine.

★ CONDIVIDERE IN MODO SICURO: Obscuracam rimuove tutti i dati identificativi memorizzati nella foto, tra cui dati di localizzazione GPS e telefono (marca e modello) in modo da poter salvare la foto protetta nella Galleria, o condividerla direttamente su Facebook, Twitter o qualsiasi altra app abilitata tramite il tasto "Condividi" .

★ PROTEGGE L'IDENTITÀ DELLA FOTOGRAFO: Gli smartphone allegano le informazioni per ogni foto che scattano(quando, dove, modello del telefono ecc…).
ObscuraCam rimuove tutte queste informazioni (METADATI).

PixelKnot: Hidden Messages

Hai un testo che non vuoi facilmente condividere? Perché non nasconderlo in una foto?

Con PixelKnot, solo i tuoi destinatari, con la password, saranno in grado di sbloccare il vostro messaggio testuale.

Tutti gli altri vedranno solo un’immagine.

E 'un modo divertente e facile per condividere i messaggi nascosti senza che nessuno lo sappia.
Prendete quei pixel, li torcete in un nodo, e vedrete di persona!

★ MASCHERARE I MESSAGGI: Le immagini sono pubbliche, il testo è nascosto dentro. Anche un occhio esperto penserà che l'immagine sia pulita.

★ PER VISUALIZZARE IL TESTO NASCOSTO: Mettere una password sul messaggio segreto per fare in modo che nessuno possa leggerlo, tranne il destinatario al quale avrai comunicato la pswd da usare per visualizzare il testo.

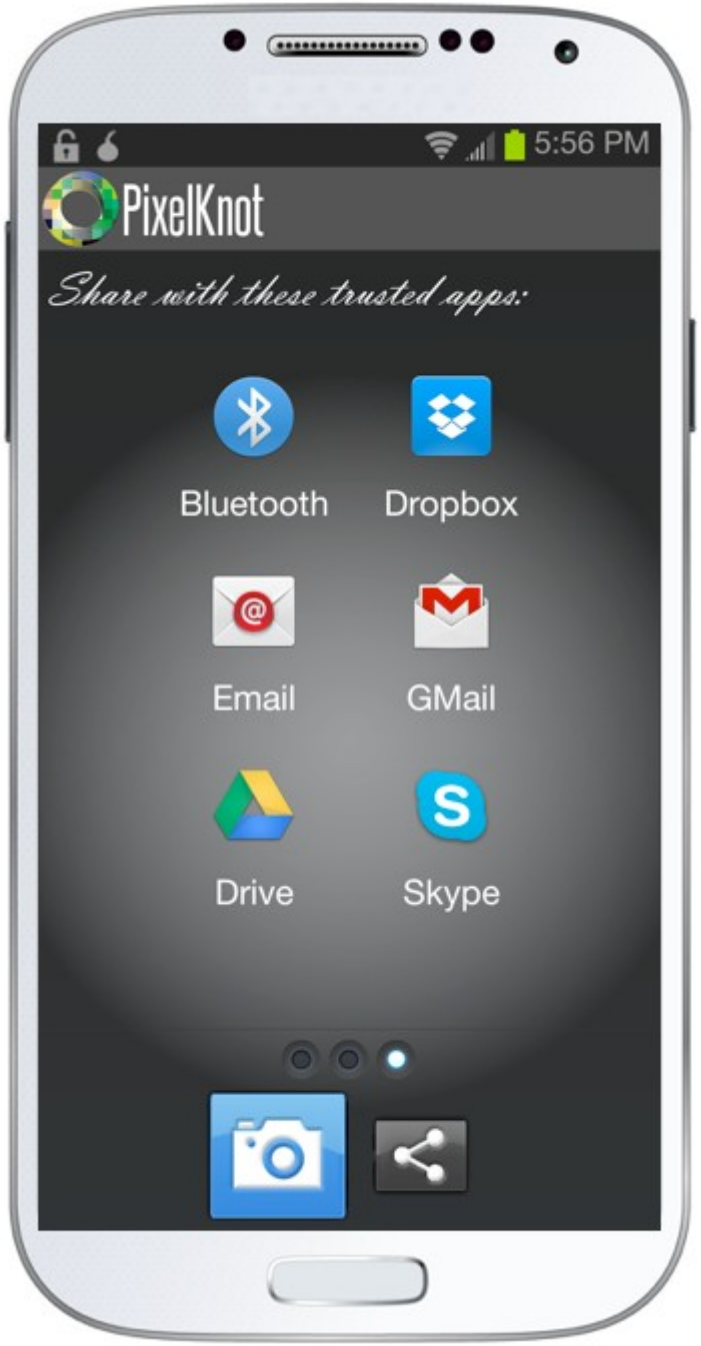
★ SCEGLI LA TUA IMMAGINE: è possibile utilizzare la fotocamera per scattare foto, o semplicemente utilizzare le foto che hai già preso.

★ CAMBIAMENTI INVISIBILI: Anche un’analista esperto non dovrebbe essere in grado di rilevare qualsiasi tipo di messaggio.

★ CONDIVISIONE TRA PIATTAFORME: Vuoi condividere le immagini tramite posta elettronica, strumenti di file sharing (come Dropbox e SparkleShare), social media (come Google e Flickr) o direttamente tramite Bluetooth o NFC? Non è un problema! I messaggi sono ancora recuperabili sull'altro lato. Avremo presto anche altri strumenti (come Facebook), quindi rimanete sintonizzati!

★ MATEMATICAMENTE SICURO: Usa il recente algoritmo di steganografia F5

★ ATTACK RESISTENT: Abbiamo lanciato attacchi contro le immagini con messaggi nascosti al loro interno utilizzando una versione specializzata di stegdetect, uno strumento automatico per la rilevazione di contenuti steganografia nelle immagini. Nella maggior parte dei casi, le immagini sono state inattaccabili.



CameraV: Secure Visual Proof

CameraV è il modo più semplice per catturare e condividere foto e video su smartphone o tablet, il tutto mantenendoli interamente sicuri e privati.

CameraV è facile da imparare e semplice da usare.
Tutte le foto e i video realizzati sono protetti da password e al 100% crittografati sul dispositivo. È inoltre possibile aggiungere note private e tag di una foto o un video, e scegliere con chi condividerli.

NoteCipher

Tutte le note create e memorizzate da quest’applicazione vengono salvate e crittografate in sicurezza. Garantite con lo standard di crittografia AES a 256 bit.

SQLCipher è un'estensione SQLite che fornisce crittografia AES a 256 bit di file di database. Ad oggi, la libreria di base è open-source, promosso e gestito da Zetetic LLC, ed è stato portato su Android nel 2011 dal progetto TheGuardianProject.

Signal Private Messenger

La privacy è possibile e Signal la rende facile.

Utilizzando Signal, è possibile comunicare istantaneamente, evitando costi di SMS, creare gruppi in modo da poter chattare in tempo reale con tutti i tuoi amici in una sola volta, e condividere i media o gli allegati, tutto con completa privacy.

Parlare liberamente: Effettua telefonate cristalline a persone che vivono in città, o a lunga distanza.

Il server non ha accesso a qualsiasi della vostra comunicazione e non memorizza alcun dato.

Surespot Encrypted Messenger

Ogni cosa inviata con surespot viene crittografata da estremo a estremo con crittografia simmetrica (AES-GCM a 256 bit) e chiavi create con ECDH a 521 bit.

Puoi inviare informazioni e immagini private con sicurezza, hai il controllo sui tuoi messaggi, quando cancelli un messaggio viene cancellato anche nel telefono del destinatario, e le immagini possono essere condivise solo su richiesta.

Le identità multiple ti permettono di essere chi vuoi con chi vuoi, e puoi sempre bloccare chi diventa fastidioso.

Surespot non richiede né salva il tuo numero di telefono o email e non mettiamo a rischio i tuoi dati, e non ci sono pubblicità!

ChatSecure

ChatSecure è un app di messaggistica libera e open source che dispone di crittografia OTR su XMPP. È possibile collegare account esistenti su Google, creare nuovi account sul server XMPP (anche via Tor), o anche connettersi al proprio server per una maggiore sicurezza.

ChatSecure è completamente interoperabile con altri client che supportano OTR e XMPP, come Xabber, Adium, Jitsi, Zom, Pidgin, e altro ancora.

* XMPP

* OTR

* Tor

* SQLCipher

Orbot: Proxy with Tor
Orfox: Tor Browser for Android

Orbot usa Tor per cifrare il traffico Internet e poi lo nasconde facendo rimbalzare attraverso una serie di computer in tutto il mondo. Tor è un software libero e una rete aperta che ci consente di difenderci contro alcune forme di sorveglianza della rete che minacciano la libertà personale e la privacy.

Orfox è costruito dallo stesso codice sorgente Tor Browser (che è costruito su Firefox), ma con alcune modifiche minori sulle caratteristiche per renderlo compatibile con Firefox per Android e il sistema operativo Android.

Include NoScript e HTTPSEverywhere add-on

Orbot: Proxy with Tor

*** UTENTI Samsung Galaxy ***

Su alcuni dispositivi, l’applicazione aSamsung è in ascolto sulla stessa porta di rete che Orbot utilizza.

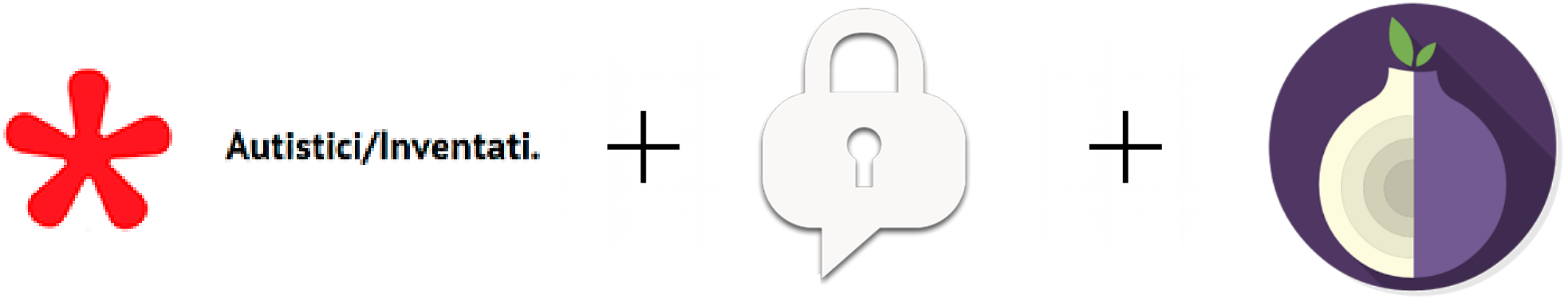
Cosa fare?
Scaricare 'SockStat' da Google Play.
Cercare l'applicazione sulla porta 9050.
Arresto forzato e Disabilitare tale app.

Si può anche provare a cambiare "Tor SOCKS" di Orbot nelle impostazioni della sezione di debug a 9051 o AUTO.

Si può vedere la correzione in questo video:
https://www.youtube.com/watch?v=yK-nK4F67_g

*****

La combo consigliata



http://lab61.info/wp/wordpress/index.php/materiali/

Ripple - BETA

Ripple è un “panic button" che può inviare il messaggio di “trigger” per qualsiasi applicazione che è un "panic responder". Tali applicazioni possono fare cose come blocco, mascherarsi, cancellare i dati privati, inviare un messaggio di emergenza, e altro ancora.