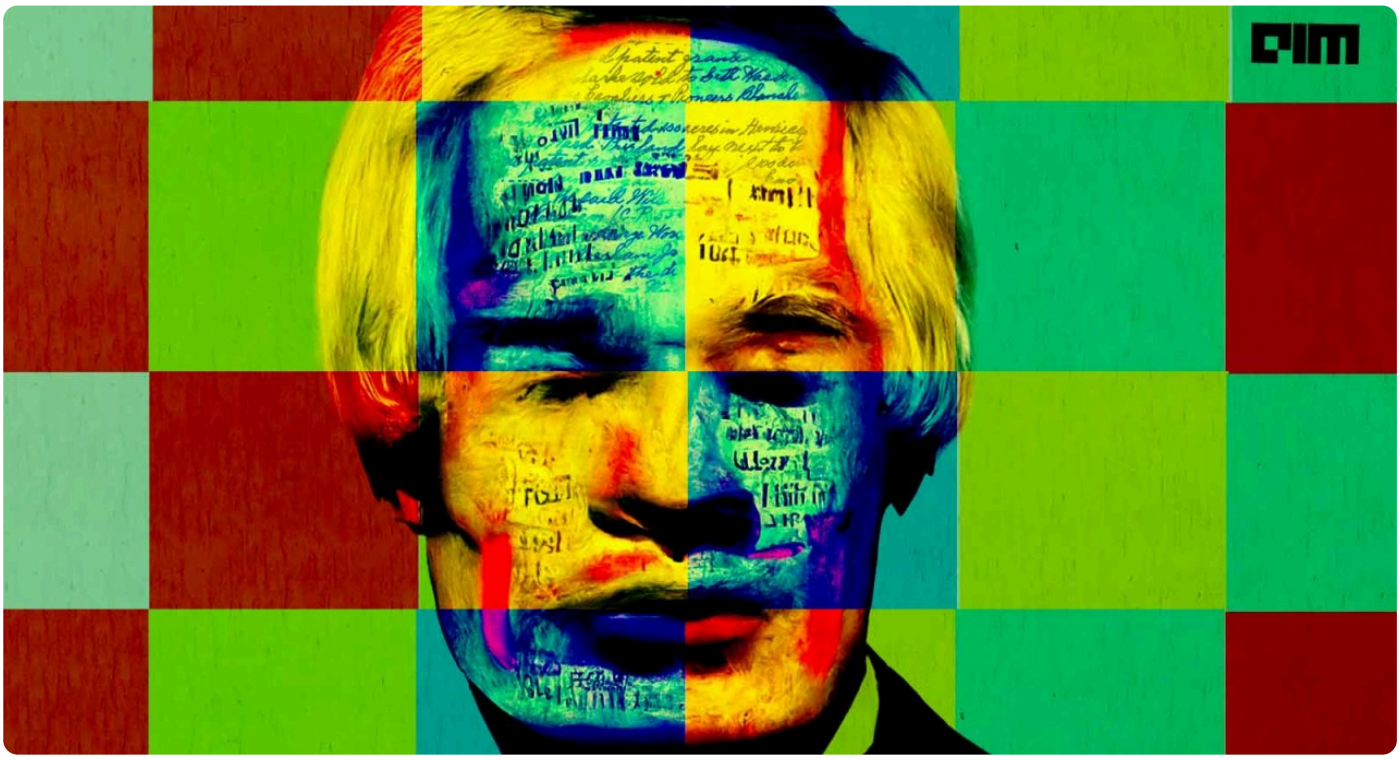

La steganografia e le sue possibili implementazioni

Roberto A. Foglietta
GNU/Linux Expert and Innovation Supporter

Published Mar 26, 2023

+ Follow

LA STEGANOGRAFIA E LE SUE POSSIBILI IMPLEMENTAZIONI

Qui il progetto che genera dei tipo di video affinché si possa salvare dati codificati su youtube godendo di storage teoricamente infinito.

- **Infinite-Storage-Glitch** su Github

Il progetto non si pone un obbiettivo pratico ma è più che altro un PoC goliardico, però molto interessante.

Altri esempi più classici sono la filigrana nelle JPG e gli ultimi 2 bits meno significativi nelle PNG (e altri formati loss-less) che sono da tempo usati per la stganografia, non di rado combinata con altre tecniche come la crittografia che rende le informazioni steganografate non intelligibili e la compressione che ne aumenta l'entropia ad un livello molto simile a un rumore bianco.

In entemrambi i casi quando un'immagine presenta artefatti da compressione JPG oppure rumore di fondo nelle PNG, in teoria potrebbe esserci nascosto un messaggio cifrato.

Al netto di header e metadati legati al formato dell'immagine, il rapporto fra volume trasmesso e dato steganografato è il 25% considerando un rapporto di compressione di 2:1, si arriva al 50%.

Sembra un sistema inefficiente ma sarebbbe la stessa dimenesione del messaggio veicolato segretamente se esso fosse stato trasferito in chiaro e senza compressione.

Le cose si fanno ancora più interessanti quando il sistema di crittografia e la chiave, l'header rimosso che identifica l'algoritmo di decompressione, il formato di steganografia, l'alfabeto del messaggio, e l'ordine delle operazioni sono determinate dal contenuto presentato visualmente dall'immagine.

Perché in questo modo nessun algoritmo deterministico e nessuna analisi statistica ne la ricerca di particolari valori possono aiutare la decifrazione del messaggio che risulta ogni volta diversamente codificato anche qualora fosse lo stesso identico.

Perciò un attaccante non riuscirebbe a decifrare il messaggio e nemmeno affermare che vi sia codificato persino nell'ipotesi limite che conosca già in modo esatto il messaggio.

Senza contare che la singola codifica di un numero primo è sufficiente per determinare una sequenza frattale univoca per mappare i bit signficativi da quelli inseriti con generazione pseudo casuale.

> *Ken Ono e il suo gruppo di ricerca, hanno infatti scoperto che le partizioni dei numeri primi si comportano in realtà come frattali. Le proprietà di divisibilità delle partizioni individuate, hanno permesso di vedere come la loro sovrastruttura si ripeta infinitamente.*

L'uso delle A.I. generative e di riconoscimento dei pattern/oggetti nelle immagini completa il quadro. Insomma le possibilità sono infinite.