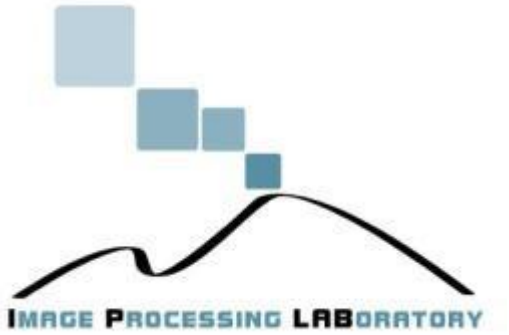
Università degli Studi di Catania

Facoltà di Scienze Matematiche, Fisiche e Naturali

Corso di Laurea in Informatica (a.a. 2012/13)



Plugin ImageJ
Steganografia Digitale

Massimiliano Portelli (matricola M01/000258)

Roberto Di Perna (matricola M01/000084)

INDICE

1. Introduzione

Il progetto realizzato consiste nell'implementazione di un plugin per il software forense ImageJ. Il plugin implementa una codifica ed una decodifica steganografica che ha come scopo quello di nascondere informazioni all'interno di un'immagine. Le informazioni possono essere semplici messaggi oppure interi file di dati.

2. Installazione ed utilizzo del plugin

Per utilizzare il plugin realizzato è necessario installarlo all'interno di ImageJ. Per farlo bisogna creare una cartella all'interno del seguente percorso: \ImageJ\plugins\.
Fatto ciò copiamo all'interno della directory appena creata i file .class, generati dalla compilazione di “Coder_.java” e “Decoder_.java”.
Fatto ciò è possibile utilizzare il plugin.

Avviamo ImageJ e apriamo un'immagine qualsiasi attraverso la voce File>Open. Una volta selezionata la nostra immagine cliccare la voce Plugins e dal sottomenù la voce “Coder”. (Figura 1)

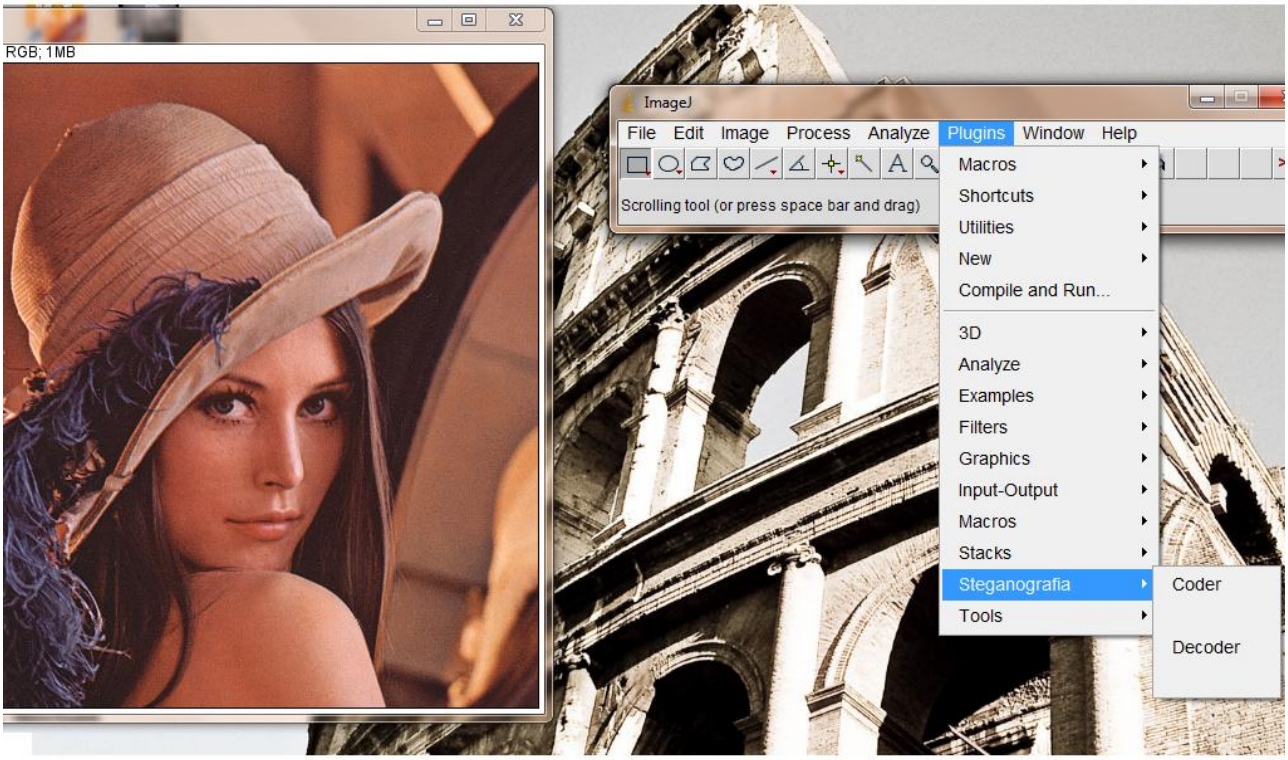


Figura 1

A questo punto si aprirà un'interfaccia (Figura 2) con diverse opzioni da selezionare.

- Inserire File o un semplice testo;
- Crittare il file/testo da inserire tramite una chiava generata con l'ausilio di una password inserita dall'utente;
- Selezionare i canali di colore da utilizzare;
- Selezionare il numero di bit da utilizzare per la codifica (massimo 2 per ogni canale);
- Selezionare la posizione iniziale del pixel su cui iniziare la codifica;
- Possibilità di inserire nell'immagine la chiave di decodifica;
- Opzione “Salto” (con un range ben preciso) che ci permette di “saltare” un determinato numero di pixel selezionato.

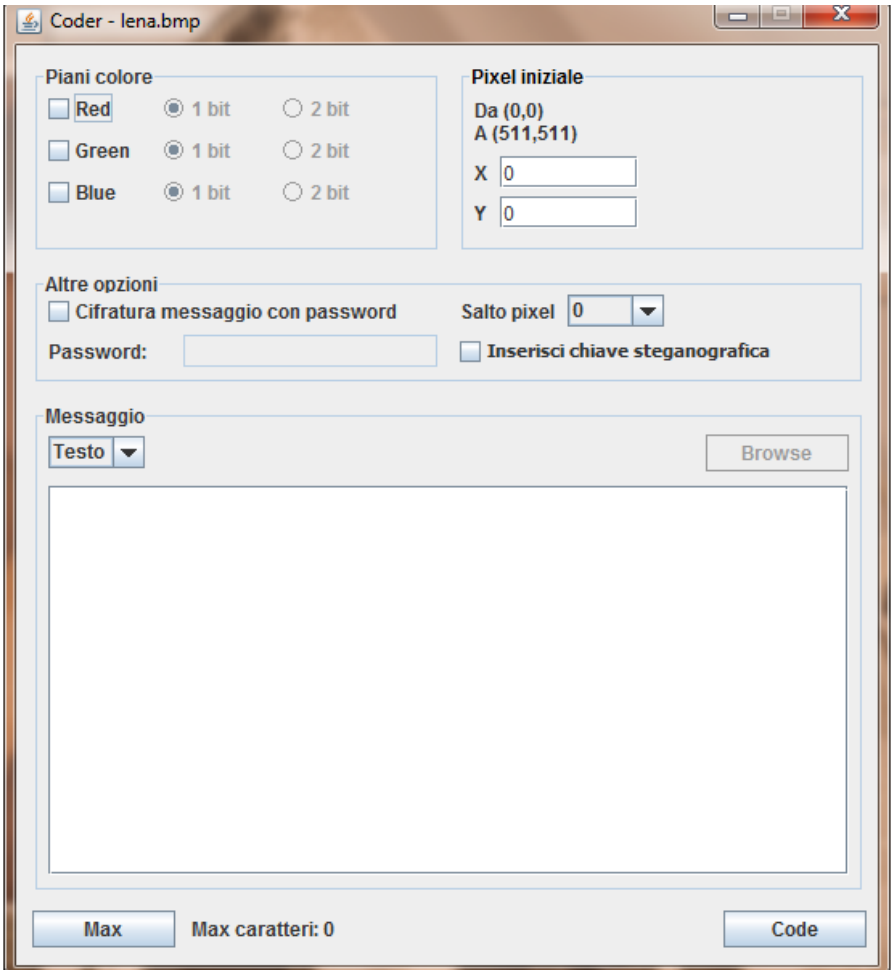


Figura 2

In base alla combinazione di opzioni che verrà stabilita dall'utente, cambierà anche la dimensione del file/testo da poter inserire. Inoltre, importante è la possibilità di selezionare l'inserimento della chiave steganografica, in quanto se questa viene inserita, in fase di decodifica il file verrà estratto in automatico; se invece la chiave non è selezionata, l'utente dovrà ricordare le opzioni date in fase di codifica per poter estrarre il file inserito in output.

Una volta selezionato tutto basta cliccare sul pulsate code per inserire i dati nell'immagine, generando così una nuova immagine in output apparentemente identica all'originale (Figura 3).

Figura 3

Per quanto riguarda l'estrazione del nostro file da un'immagine andremo a selezionare la voce “Decoder” dal sottomenù Plugins. In tal modo ci ritroveremo la seguente schermata (Figura 4):

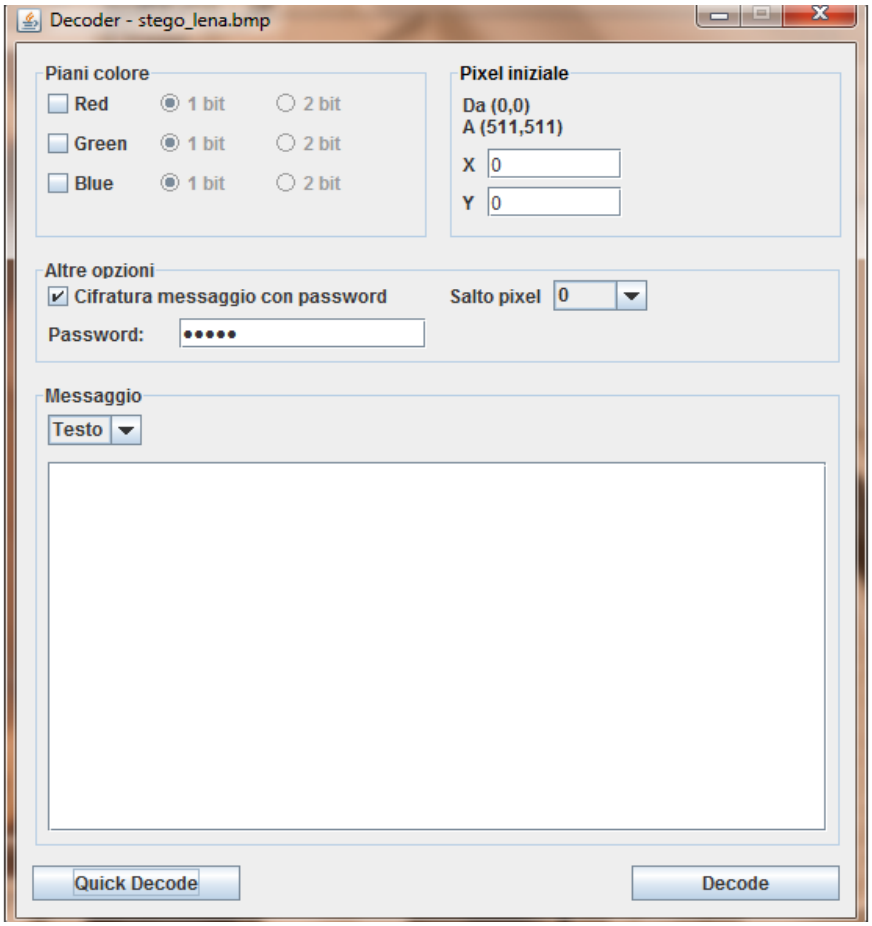


Figura 4

Nel caso in cui la chiave steganografica fosse stata inserita in fase di codifica, basterà cliccare il pulsante “Quick Decode” per analizzare l'immagine e ottenere il file nascosto all'interno; mentre, se all'interno dell'immagine da decodificare non vi fosse la chiave steganografica è necessario immettere tutte le opzioni selezionate in fase di codifica e cliccare sul pulsante “Decode”.

Nelle figure qui di seguito riportiamo l'esempio di codifica e decodifica rispettivamente di un testo e di un qualsiasi tipo di file:

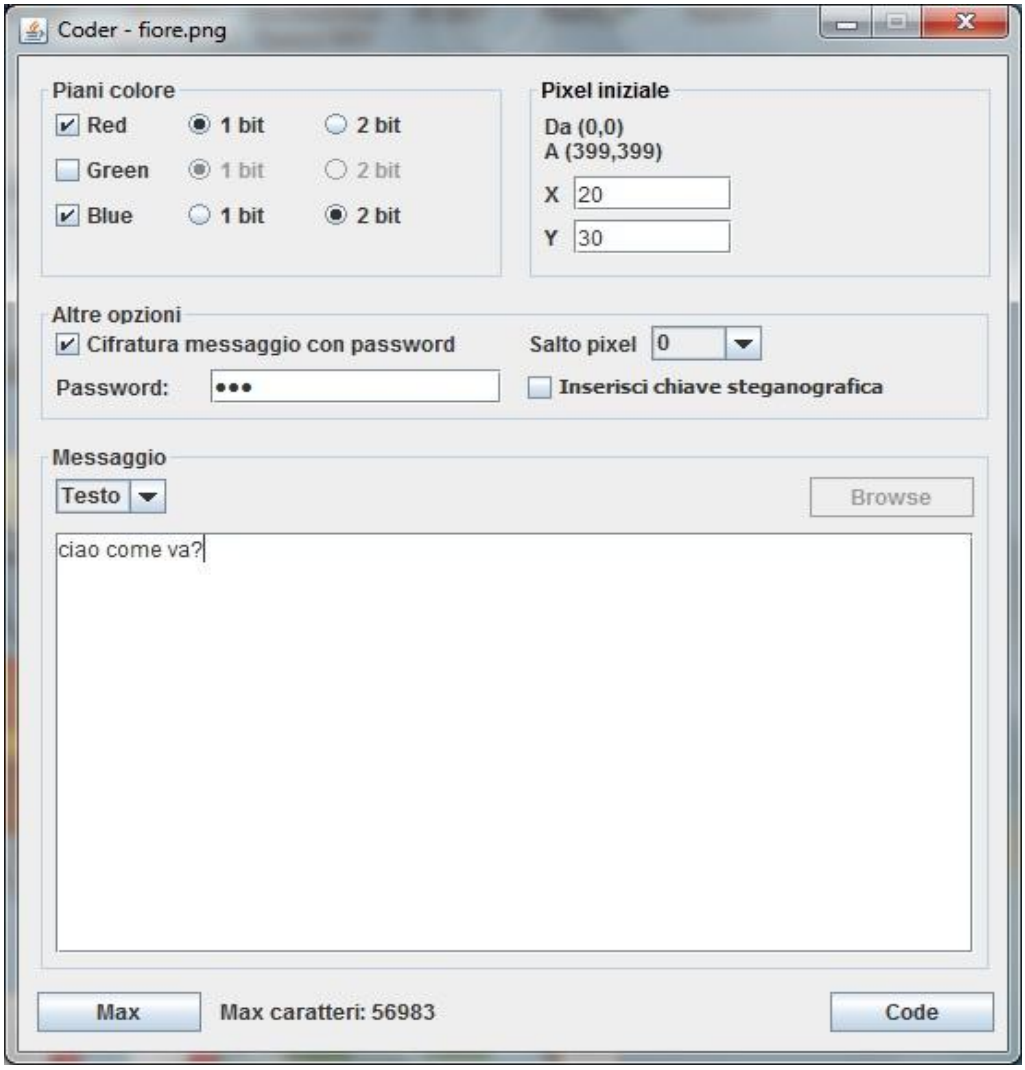


Figura 5.A

Il testo da “nascondere” all'interno dell'immagine è: “ciao come va?”. Abbiamo selezionato come si può ben vedere 3 bit di cui: 1 per il canale rosso e 2 per il canale blu (il canale verde resta invariato).

In fase di decodifica otterremo il seguente risultato:

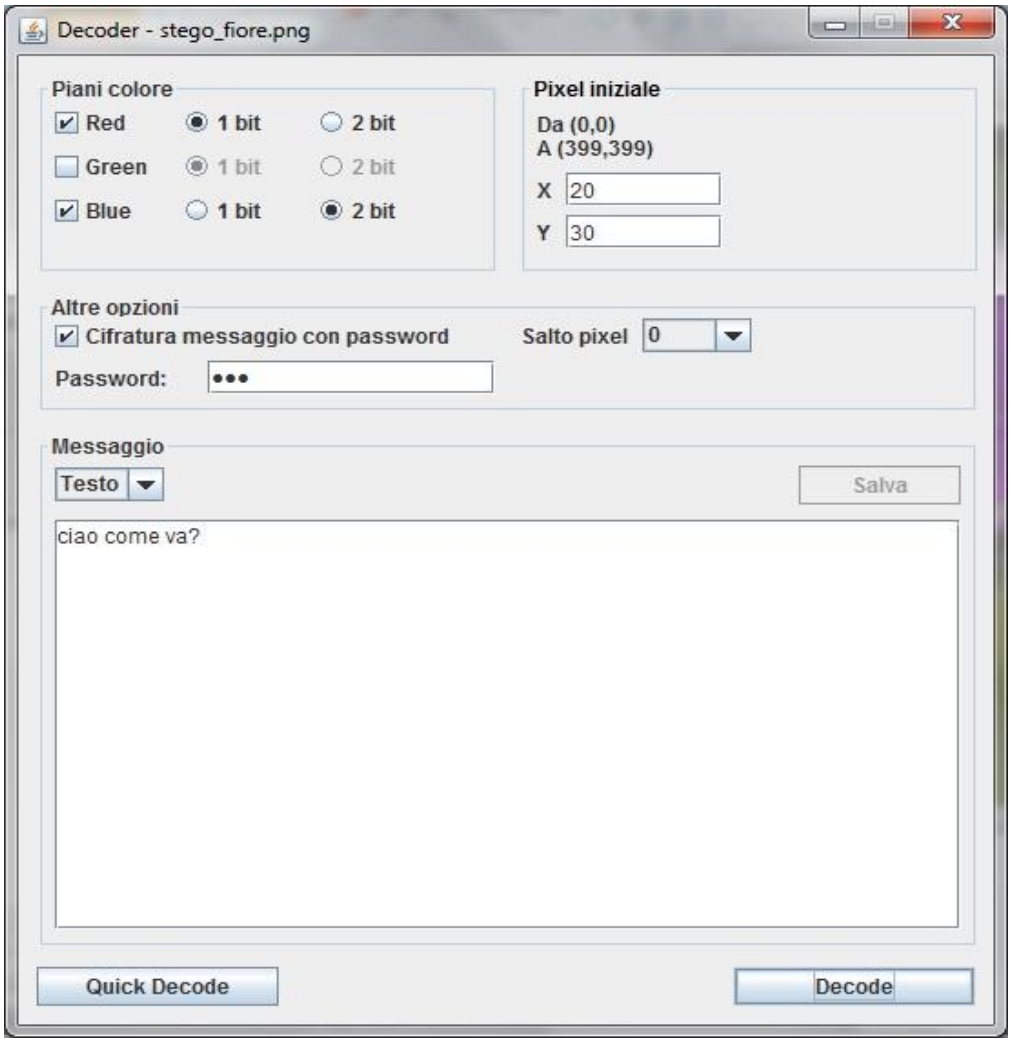


Figura 5.B

Non avendo inserito alcuna chiave steganografica all'interno dell'immagine, nella fase di decodifica è stato necessario selezionare le stesse opzioni date durante la codifica.

Vediamo adesso lo stesso procedimento prendendo in input un'immagine (un qualsiasi altro tipo di file avrebbe prodotto lo stesso risultato).

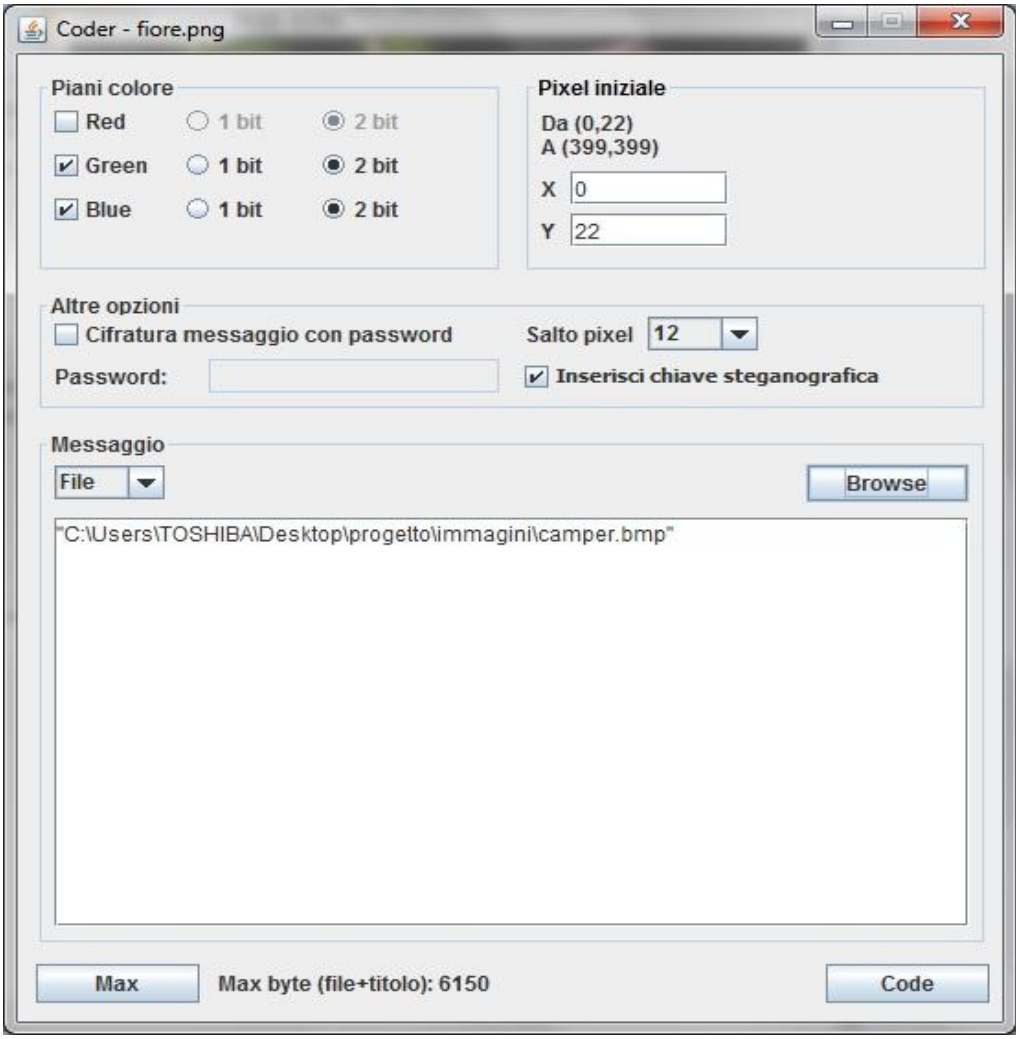


Figura 6.A

Come possiamo vedere abbiamo selezionato: 4 bit in totale, 2 per il canale Verde e 2 per il canale Blu. Inoltre, stavolta inseriremo nell'immagine in output anche la chiave steganografica, quindi in fase di decodifica non sarà necessario sapere quale opzioni abbiamo scelto in fase di codifica.

In fase di decodifica avremo quindi il seguente risultato:

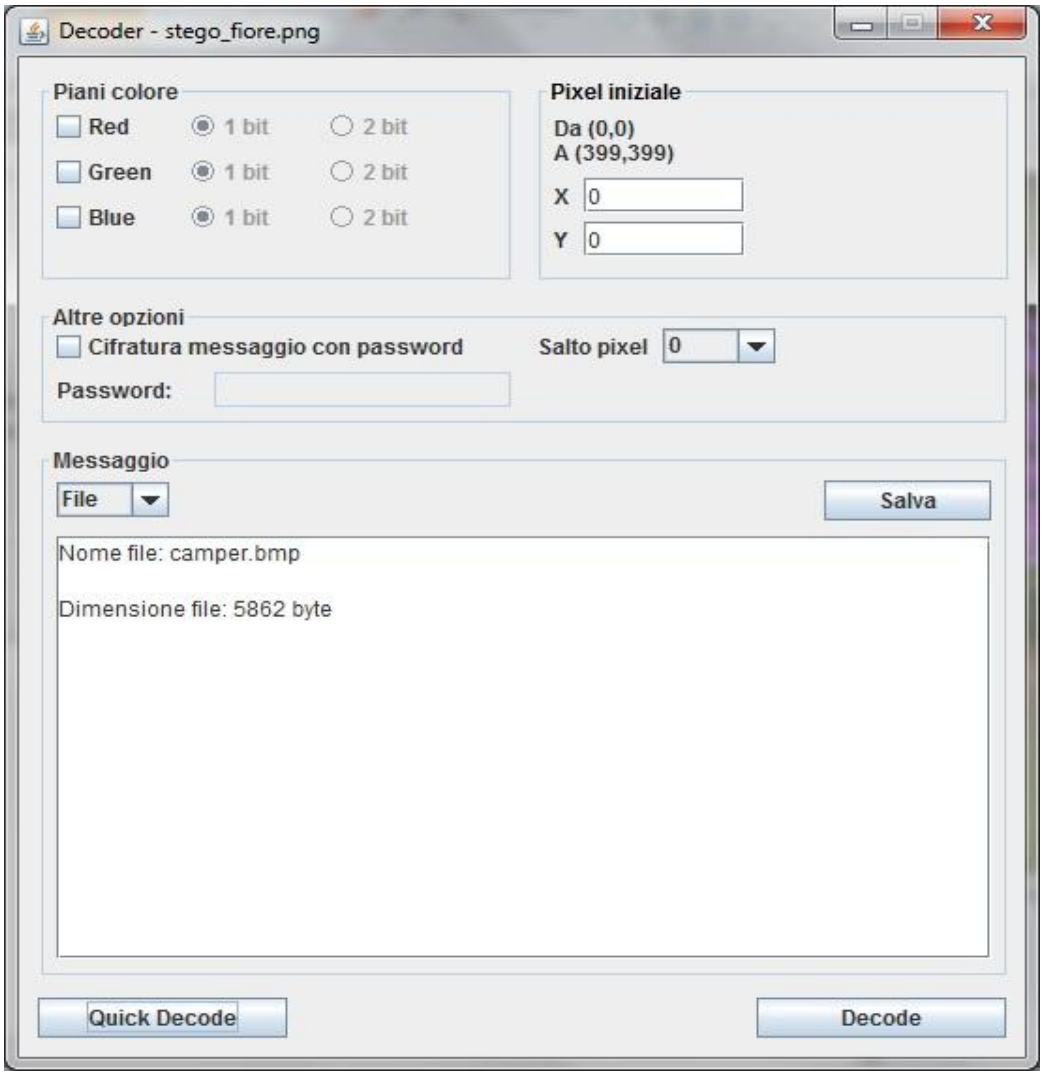


Figura 6.B

Basta cliccare sul pulsante “Quick Decode” per analizzare l'immagine ed ottenere il file nascosto all'interno.

3. Progettazione

Sono state realizzate due classi: Coder_, che si occuperà dell'inserimento dei dati all'interno di un'immagine; e Decoder_, la quale si occuperà dell'estrazione di questi ultimi.
La stenografica dei dati nel progetto avviene tramite la modifica dei bit LSB dei 3 livelli di colore R, G e B dell'immagine presa in input. I pixel dell'immagine saranno processati uno alla volta, scomposti nei tre livelli di colore e modificati i bit finali di ogni livello, per poi comporre un nuovo pixel che verrà sostituito a quello dell'immagine in input. È stata resa possibile, inoltre, la crittografia dei dati (File o semplice testo), attraverso l'algoritmo di crittografia DES e a una chiave di codifica generata mediante l'utilizzo di una password scelta dall'utente.

4. Glossario

Steganografia: è una tecnica che si prefigge di nascondere la comunicazione tra due interlocutori, infatti il termine è composto appunto dalle parole greche στεγανός (nascosto) e γραφία (scrittura). (Fonte: Wikipedia)

LSB (dall'inglese least significant bit, bit meno significativo): è la tipologia di steganografia più diffusa. Si basa sulla teoria secondo la quale l'aspetto di un'immagine digitale ad alta definizione non cambia se i colori vengono modificati in modo impercettibile.Ogni pixel è rappresentato da un colore differente, cambiando il bit meno significativo di ogni pixel, il singolo colore non risulterà variato in modo significativo e il contenuto dell'immagine sarà preservato nonostante questa manipolazione. (Fonte: Wikipedia)

Crittografia (dall'unione di due parole greche: κρυπτός (kryptós) che significa "nascosto", e γραφία (graphía) che significa "scrittura"): è la branca della crittologia che tratta delle "scritture nascoste", ovvero dei metodi per rendere un messaggio "offuscato" in modo da non essere comprensibile/intelligibile a persone non autorizzate a leggerlo. Un tale messaggio si chiama comunemente crittogramma e le tecniche usate tecniche di cifratura. (Fonte: Wikipedia)

DES: in crittografia il Data Encryption Standard (DES) è un algoritmo di cifratura scelto come standard dal Federal Information Processing Standard (FIPS) per il governo degli Stati Uniti d'America nel1976 e in seguito diventato di utilizzo internazionale. Si basa su un algoritmo a chiave simmetrica con chiave a 56 bit. (Fonte: Wikipedia)