L’11 novembre 2022 il gruppo Catch Em All insieme al proponente Gregorio Piccoli, ha sostenuto un meeting costruttivo e migliorativo, della durata di un’ora, in cui le idee del team sono state esposte, evidenziando i pregi e le criticità di ognuna.

Il team dichiara di aver evidenziato un feedback molto positivo su l’utilità di meeting insieme al proponente poiché con essi vengono evidenziate idee implementative, criticità non pensate e soluzioni alternative, ottenute con un dialogo costruttivo insieme ad una persona di alta professionalità e con punti di vista logici, implementativi e professionali di un certo calibro.

Sono stati evidenziati diversi punti in questo incontro:

* Captcha formato da 9 immagini diverse scontornate, appartenenti a diversi gruppi di appartenenza. Per esempio di queste 9 immagini generate, 4 saranno mele, 2 saranno delle montagne e 3 delle ferrari. All’utente verrà richiesto, come task, di selezionare tutte le immagini riguardanti una determinata classe, per esempio verrà richiesto di selezionare tutte le mele presenti nel captcha.

Se la selezione sarà corretta, o almeno con un margine di errore basso, per esempio ha selezionato, riferendomi all’esempio citato prima, 3 mele e 1 montagna, allora il captcha sarà considerato risolto, altrimenti verrà generato un altro captcha da risolvere, diminuendo di 1 i possibili tentativi rimasti di verificarsi come “persona” e non bot.

* Implementazione di un database contenente l’id delle immagini del database unsplash, in particolare verrà inserito un insieme di classi delle immagini, per esempio 20, permettendo in un futuro di aumentare il numero di queste classi. Queste classi sono per esempio: “Ferrari, apple, mountain, ecc”,e per ognuna di queste classi il team si occuperà di classificare un numero di immagini prestabilito, per esempio 50 immagini per ogni classe all’interno di questo database. Queste immagini avranno la peculiarità di essere coerenti con il gruppo di appartenenza dato, poiché verranno verificate da un utente umano, portando l’errore di queste immagini sulla loro classificazione e disegno dei contorni a 0.
* Partendo da questa base di immagini già correttamente classificate, il nostro captcha sarà composto in parte da immagini gia classificate correttamente, e in parte da nuove immagini randomiche generate tramite lo script python.

Queste nuove immagini generate in maniera automatizzata hanno il rischio di non essere corrette, poiché il margine d’errore su ogni singola immagine è elevato.

In particolare il margine di errore è dovuto a due principali criticità:

1. Le immagini del database unsplash non sono sempre fedeli alla chiave di ricerca con cui sono collegate, ovvero per esempio se si ricerca tramite la chiave di ricerca “macchina”, vi è una percentuale di rischio che l’immagine non sia di una macchina, come sperato, ma sia un immagine relativa a un’altra classe assai diversa a quella richiesta;
2. Lo script di scontornamento, che da delle immagini genera delle nuove immagini in bianco nero contenenti solo i contorni del soggetto dell’immagine iniziale, non è efficace al 100%. In una buona percentuale dei casi, lo script genera una nuova immagine completamente diversa, spesso incomprensibile o evidenziando particolari non inerenti con la classe dell’immagine in questione;

Visto queste criticità, verrà implementato un sistema di classificazione, esso funzionerà in base ai feedback ricevuti dalle iterazioni degli utenti che hanno risolto i captcha.

Ma cosa intendiamo noi per feedback? Citiamo di nuovo l’esempio del captcha formato da 4 mele, 2 montagne e 3 ferrari e la task richiesta è di selezionare tutte le mele. Prendiamo sempre d’esempio che 2 di queste mele siano certificate dal nostro database come immagini inerenti a delle mele e 2 invece generate randomicamente dallo script . Come detto queste ultime 2 sono inattendibili, per cui non sappiamo ancora nulla sulla loro coerenza. Se l’utente selezionare queste due nuove immagini nella risoluzione del captcha, noi otterremo un feedback positivo sull’immagine, poiché l’utente è riuscito correttamente a classificarle, mentre invece se non le selezionerà otterremo un feedback negativo su queste, poiché non sono state riconosciute come “mele”. Creando un sistema di valutazione, basato quindi sull’iterazione dell’utente e un insieme diverso di feedback ricevuti per una particolare immagine, ad ogni iterazione avremo un idea sempre migliore se l’immagine in questione è coerente o meno.

Un vantaggio di questa idea è che al crescere di iterazioni, intese come risoluzioni di captcha, il numero di immagini nel nostro database classificate correttamente sarà sempre maggiore, avendo così un sistema scalabile che aumenta autonomamente il numero di immagini per i captcha.

Ovviamente per non avere influenze negative nella classificazione, verrà implementato un sistema che terrà conto solo dei feedback attendibili, scartando tutte le risoluzioni, e quindi feedback, che sono a priori sbagliate, evitando cosi attacchi brute force intenti a danneggiare la nostra classificazione delle immagini.

* Un altro punto introdotto, è l’implementazione di un sistema “proof of work” basato sulla richiesta da parte del dispositivo dell’utente di effettuare calcoli, principalmente funzioni hash, che mirano a disincentivare attacchi brute force da parte dei bot e bla bla bla

**LUCA CONTINUA TU QUESTO PUNTO CHE LO SPIEGHI DI SICURO MEGLIO DI ME, CITA CHE L’IDEA ESISTE GIA, COME FUNZIONA QUELLA GIA ESISTENTE E COME NOI AVEVAMO PENSATO DI IMPLEMENTARLA DIVERSAMENTE APPORTANDO IL MINING E DI COME GREG CI HA SPIEGATO LE CRITICITA DEL MINING, E DI COME ORA PENSEREMO DI RISOLVERE QUESTE CRITICITA E BLA BLA BLA.**

Inoltre è stata evidenziata la critica costruttiva da parte del proponente di non aver costruito una presentazione adeguata contenente un discorso a senso compiuto per arrivare alla conclusione delle idee esposte a lui. Il team riguardante questa criticità si impegna a migliorare il modo in cui esporrà le future idee e implementazioni decise.