SwiftBot: a Q/A Chatbot using LangChain

Soha Hussain | Github Repo

Introduction

Problem Statement

The given task is to create a question-answering chatbot on a given specific document using the LangChain framework.

Specifications of the chatbot:

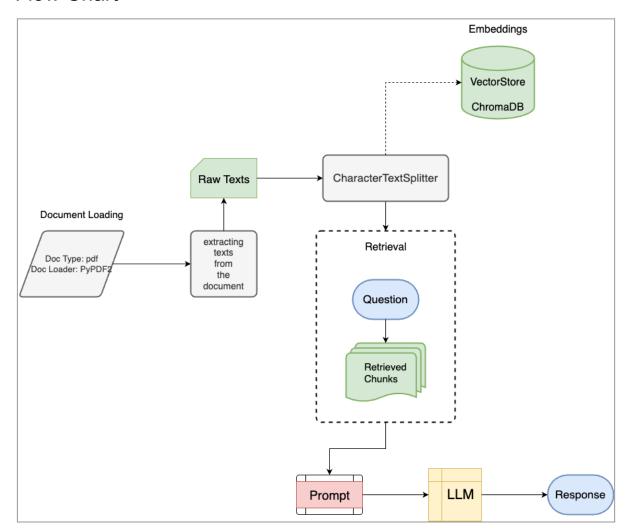
- 1. The document to be used for context is : <u>Celebrity, Music and Public Persona:</u>
 <u>A Case Study of Taylor Swift</u>
- 2. The chatbot should only respond with answers generated from the given document.
- 3. The chatbot should return the source text along with the response for each question.

LangChain

LangChain is an open-source developer framework for building LLM applications. Large Language Models (LLMs) are a type of artificial intelligence model designed to understand and generate human-like text. These models are part of a broader category of natural language processing (NLP) models.

Methodology

Flow Chart



Document Loading

The provided PDF document is loaded using the **PdfReader** method of **PyPDF2** library. The PDF is then traversed and the text is extracted from it.

Document Splitting

The extracted text is then passed through a **CharacterTextSplitter** which splits the text into small chunks of size 750, with a chunk overlap of 50.

Previously, the chunk size of 800 and chunk overlap of 100 was used, but it generated random answers with only a small part dealing with the actual questions.

Vector Stores and Embeddings

The open-source embedding database, **ChromaDB**, is used as the vector database to store the embeddings of the generated chunks. To generate the embeddings, **OpenAlEmbeddings** are used. The vector database is then saved on the local machine using the **persist**() method.

Retrieval

For retrieving the most similar chunk of text which can be used to answer a given query, a **similarity search** is performed on the vector database with a **threshold of 0.6**, meaning only the texts which have a similarity score of 0.6 or above will be utilised to generate an answer.

Earlier, the threshold of 0.5 was used, but it made the chatbot answer queries which were out of scope of the given document. Therefore the threshold was increased to 0.6.

Prompting

In order to generate concise and accurate answers and to ensure that the chatbot only responds to the questions with answers found in the provided document, a **custom prompt template** is created which provides the AI agent with specific instructions to be taken care of while generating a response. The instructions provided in the template is as follows:

As an AI assistant you provide answers based on the given context, ensuring accuracy and briefness.

You always follow these guidelines:

- -Only answer from the source documents
- -If the answer isn't available within the context, respond that it is not available
- -Otherwise, answer to your best capability, referring to source documents provided
- -Only use examples if explicitly requested
- -Do not introduce examples outside of the context
- -Do not answer if context is absent
- -Limit responses to three or four sentences for clarity and conciseness

The above prompt has a limitation. It does not provide the security aspect. In case the chatbot is asked to forget every prompt passed earlier, it may not work accordingly.

QA Chain

A RetrieverQA chain is initiated and the following parameters are passed to it:

- LLM : **OpenAI**, with the **temperature** argument set as **0**, to generate concise and factual answers
- Retriever: the retrieved vector containing the similar text chunks are passed using the as_retriever method
- The **return_source_documents** parameter is set as **True** to return the source text used to generate the answer
- The custom prompt template is also passed using the chain_type_kwargs parameter

Streamlit UI

A simple chat UI is built using the various **Chat Elements** provided by the **Streamlit** library.

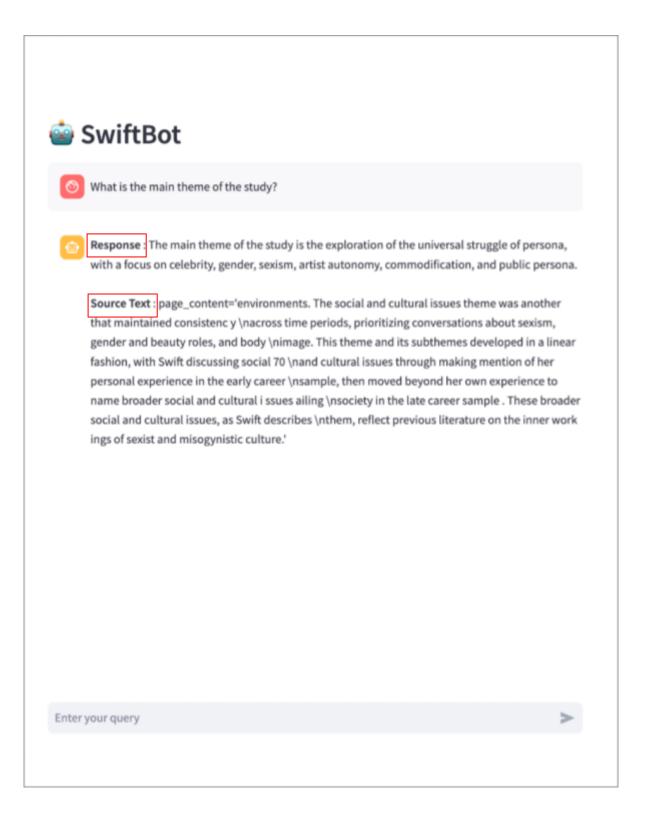
Some features of the UI are:

- The chats are stored and the chat history is displayed on app rerun using the Streamlit's **session state** feature
- **chat_input** is used to display an input window for the user to enter a query
- chat_message is used to display the user input and bot's response along with a avatar

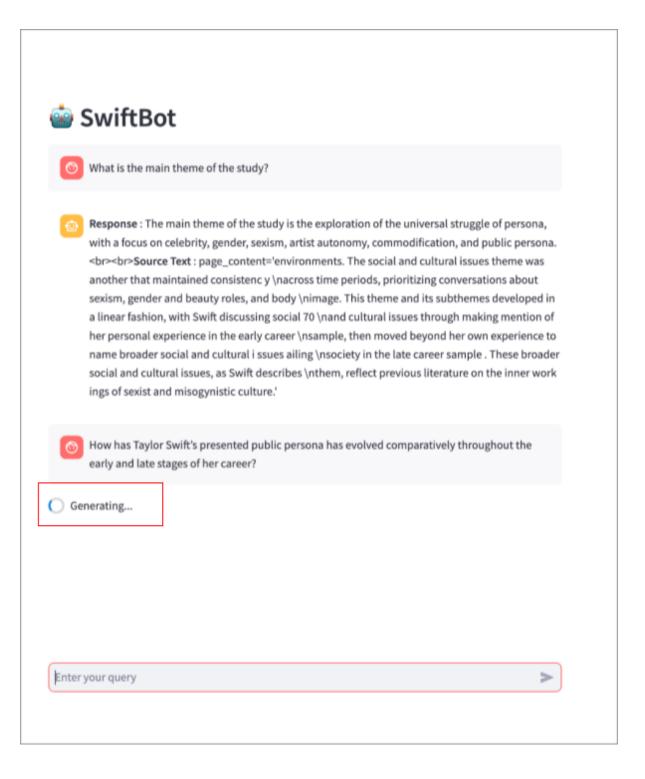
In order to ensure that the bot does not answer questions beyond the provided context, a check is applied. In case the number of source documents returned are 0, the bot will respond as "Sorry I can't answer the following question based on the context provided.", else the response will be the generated response of the bot from the extracted source documents.

Results

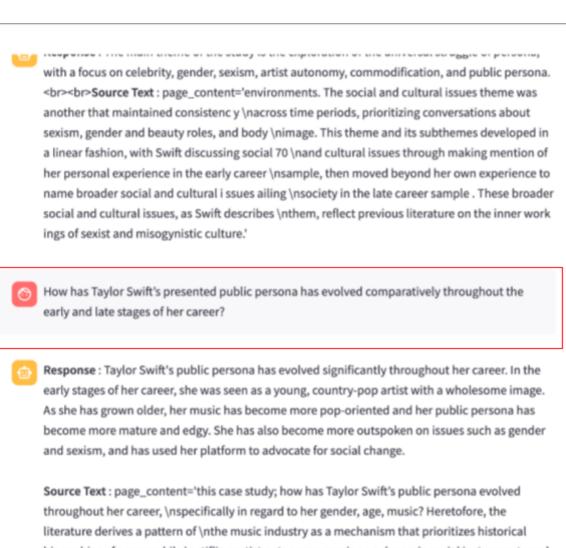
1. The image representing both the response and the source text generated by the chatbot.



2. The image representing a Generating spinner displayed while the bot is generating answers.



3. Bot's response on a few more questions



Enter your query

>

4. Image representing bot's respond when a query not related to the document provided is asked

her personal experience in the early career \nsample, then moved beyond her own experience to name broader social and cultural i ssues ailing \nsociety in the late career sample . These broader social and cultural issues, as Swift describes \nthem, reflect previous literature on the inner work ings of sexist and misogynistic culture.' How has Taylor Swift's presented public persona has evolved comparatively throughout the early and late stages of her career? Response: Taylor Swift's public persona has evolved significantly throughout her career. In the early stages of her career, she was seen as a young, country-pop artist with a wholesome image. As she has grown older, her music has become more pop-oriented and her public persona has become more mature and edgy. She has also become more outspoken on issues such as gender and sexism, and has used her platform to advocate for social change.

Sor>Source Text: page_content='this case study; how has Taylor Swift's public persona evolved throughout her career, \nspecifically in regard to her gender, age, music? Heretofore, the literature derives a pattern of \nthe music industry as a mechanism that prioritizes historical hierarchies of power while \nstifling artist autonomy, music as a dynamic social instrument used multifacetedly, musician \nand celebrity culture as dramaturgical performance that necessitate sophisticated and interactive \nidentity construction and maintenance, the deep -rooted nature of the entertainment industry to \ncommercialize and commodify individuals, and gender and sexism as evolving and aggregate \nsocial concepts of control. $\n \n \n \n \n \n \n \n \n \n \n$ THREE: METHODOLOGY' What is table salt? Sorry I can't answer the following question based on the context provided.

5. Bot's respond on a few more questions

Enter your query

- What is table salt?
- Sorry I can't answer the following question based on the context provided.
- Define music and its types.
- Response: Music is an art form that uses sound and silence to create a composition. It can be divided into different genres such as classical, jazz, rock, pop, and hip-hop. Music can also be used to evoke emotions and provide a sense of refuge from everyday life. Modern technology has made it possible to access music anywhere and anytime.

Source Text: page_content='(Lee 2012). \n Music is also used as a place of refuge in social life. Music offers many people space and \ntime to dissociate from the reality of their lives a nd situations, negative or otherwise. All types of \nmusic have the potential to transport listeners, even temporarily, outside of their subjective \nexperiences, into the worlds they create. Often, instruments, melodies, and sounds that music \ncontains suspend daily circumstances and parameters to offer asylum to those listening. Modern \ntechnological advancements have made this possible wherever one goes and whenever one \nwants, offering a place to escape for wellbeing purposes, even when immersed in daily routi nes \n(Roy and Dowd 2010).'

Enter your query

>