

Recuperación de Información y Recomendaciones en la Web (Webir) - Informe Final

Guillermo Maiese - guillermo.maiese@fing.edu.uy - 4.875.719-8

Guillermo Lara - guillermo.lara@fing.edu.uy - 4.861.715-0

Germán Cabarro - german.cabarro@fing.edu.uy - 5.101.325-0

Martin Corredera - martin.corredera@fing.edu.uy - 4.811.170-8

Grupo 08

25 de Noviembre de 2023

Resumen

El presente documento introduce la entrega final de la unidad curricular 'Recuperación de Información y Recomendaciones en la Web'. Este informe detalla el trabajo realizado del equipo, cuyo objetivo principal consistió en analizar herramientas disponibles para anonimizar y recuperar imágenes, centrándonos específicamente en rostros. La finalidad de este análisis fue proporcionar imágenes anonimizadas de manera automatizada a aquellos usuarios que lo soliciten y establecer un conjunto de estándares de calidad de anonimización para su evaluación. La intención subyacente en este trabajo es facilitar el uso de una herramienta de anonimización de imágenes, especialmente dirigida a personas del ámbito académico que no posean un conocimiento técnico avanzado.

Índice

1. Introducción	3
2. Problema	3
3. Enfoque de la Solución	4
4. Diseño	5
5. Implementación	6
5.1. Desarrollo de cada herramienta	6
5.2. Fortalezas y Debilidades de cada herramienta	9
6. Conclusiones	11
7. Trabajo a Futuro	14
Referencias	15

1. Introducción

En las páginas que siguen, exploraremos las herramientas y las estrategias que definen el procesamiento y recuperación de imágenes anonimizadas. Estas son esenciales en entornos donde la integridad de la información confidencial debe preservarse.

2. Problema

La anonimización de datos emerge como un tema de suma relevancia en el ámbito de investigaciones sociales y en diversas disciplinas que requieren el manejo de información de identificación personal. La necesidad de divulgar pruebas para respaldar conclusiones, sin comprometer la privacidad y la seguridad de los individuos, ha catalizado el desarrollo de técnicas avanzadas de anonimización. La anonimización de datos se ha convertido en una herramienta esencial para la investigación, pero su aplicación efectiva y segura, no siempre es sencilla. Por tanto, es crucial que los investigadores y otros usuarios no expertos tengan acceso a herramientas que les permitan comparar técnicas de anonimización, evaluar el riesgo de reidentificación y medir la calidad de la anonimización. Esto les brinda la capacidad de utilizar y compartir datos que, de lo contrario, serían inaccesibles debido a la complejidad del proceso y la falta de conocimientos especializados.

Aspectos clave del problema:

- Privacidad y Seguridad: La información visual, especialmente rostros, contiene datos personales sensibles. La falta de anonimización puede dar lugar a la identificación no deseada, comprometiendo la privacidad y seguridad de los individuos en las imágenes.
- Utilización por Investigadores: Los investigadores sociales dependen de la recopilación de datos visuales para enriquecer sus estudios y respaldar las conclusiones. Sin embargo, la necesidad de compartir estas imágenes de manera ética y segura requiere la implementación de técnicas efectivas de anonimización.
- Mejores Técnicas y Análisis de Herramientas: La selección de técnicas eficientes de anonimización es crucial. Se necesita una evaluación de herramientas disponibles, considerando factores como la efectividad de la anonimización, la preservación de características relevantes y la facilidad de uso.
- Reducir la Complejidad: La complejidad asociada con la anonimización de rostros a menudo desalienta su implementación efectiva. Se requiere una simplificación de procesos y la adopción de enfoques que no solo aseguren la protección de la privacidad, sino que también faciliten la aplicación práctica por parte de investigadores.

3. Enfoque de la Solución

La solución propuesta fue un trabajo de investigación de las herramientas disponibles actualmente, estableciendo estándares comparativos, lo que nos permitió analizar las fortalezas y debilidades de cada una. Esto nos llevó a que, dadas las necesidades descritas anteriormente en el problema y la diversidad de herramientas disponibles, eligiéramos 4 herramientas que concluimos fueron las más apropiadas para este trabajo. Estas son:

- OpenCV: (Open Source Computer Vision Library) es una biblioteca de código abierto¹ [5] especializada en procesamiento de imágenes. Ofrece una amplia gama de funciones y algoritmos que permiten a los desarrolladores trabajar con imágenes y vídeos de manera eficiente. Desde la detección de rostros hasta la manipulación de imágenes, OpenCV es una herramienta versátil utilizada en aplicaciones de aprendizaje automático.
- Fiji ImageJ2: Fiji, basado en ImageJ2, es un software de procesamiento de imágenes que se centra en la visualización y análisis de datos de imágenes científicas. Diseñado para ser extensible y modular, Fiji simplifica tareas complejas en la investigación biológica y médica.
- Celantur: Es una herramienta especializada en la anonimización de datos, centrándose en la protección de la privacidad y confidencialidad de la información. Es utilizado para ocultar o enmascarar datos sensibles, especialmente en conjuntos de datos utilizados en investigación y análisis.
- Api4AI: Es una API diseñada para facilitar la integración de funciones de inteligencia artificial en aplicaciones y sistemas. Ofrece acceso a una variedad de algoritmos de aprendizaje automático y procesamiento de lenguaje natural, permitiendo a los desarrolladores aprovechar las capacidades avanzadas de la inteligencia artificial en sus propias aplicaciones sin la necesidad de desarrollar algoritmos desde cero.

¹Licencia Apache 2.0

4. Diseño

Para el diseño de la solución se enfocó en minimizar la cantidad de overhead de los componentes y la complejidad de los mismos. En esta sección mencionamos brevemente las tecnologías y protocolos utilizados en el desarrollo, así como un diagrama de componentes utilizado.

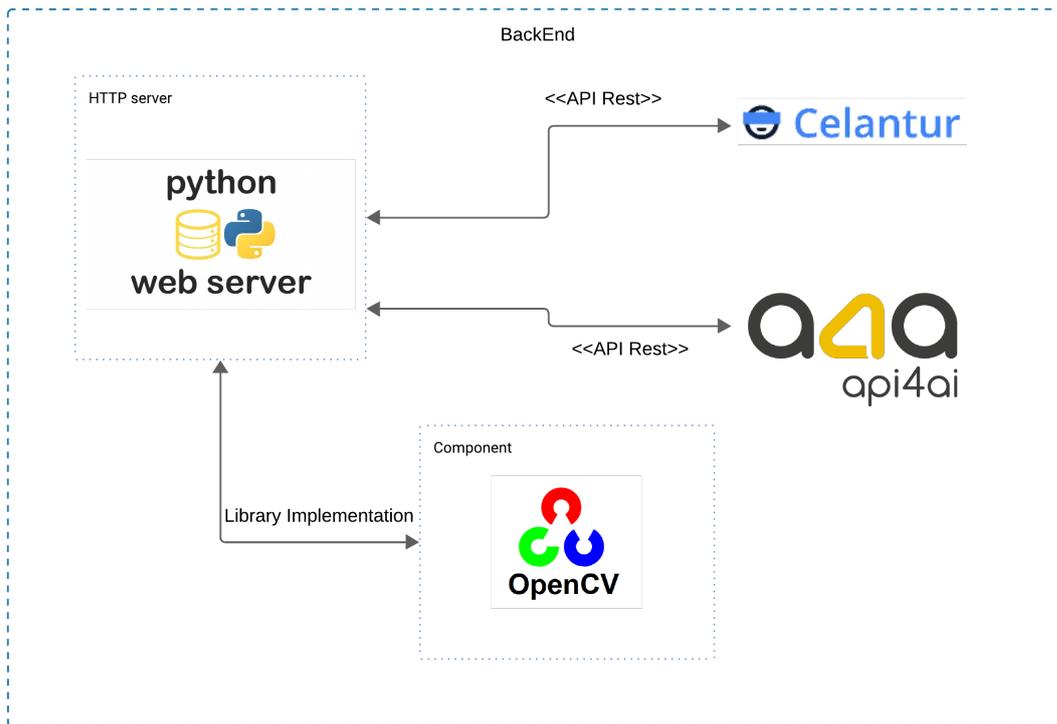


Figura 1: Diseño de la solución

Como podemos observar en la imagen en aquellos casos en los que era necesario realizar un desarrollo adicional para poder utilizar o consumir el servicio de ciertas herramientas, optamos por emplear Python para desarrollar los scripts necesarios. Cuando las herramientas proporcionaban un servicio de API REST, el script desempeñaba la función de generar la solicitud donde se incluía la imagen, y por otro lado manejaba la respuesta recibida. Por otro lado si la herramientas formaban parte de una librería, el script cumple la función de orquestar todo el proceso haciendo uso de las funciones que aportan la librería.

5. Implementación

Construcción del Set de Datos: Se seleccionó un set de datos de 50 rostros humanos de dominio público [1]. Con este set de datos, será realizada la obtención de métricas acerca de la calidad de anonimización de las distintas herramientas investigadas.

Tipo de datos: Debido a su sensibilidad, nos centraremos en imágenes de rostros obtenidos de fuentes públicas en internet.

5.1. Desarrollo de cada herramienta

A continuación se muestra la implementación de la solución para cada herramienta, utilizando el Set de datos descrito anteriormente

Celantur

Esta herramienta de software es especializada en la anonimización de datos. Para su efectiva implementación fue necesario registrarse en el sitio y obtener las credenciales necesarias para acceder a la API, de esta manera nos podemos autenticar utilizando email, contraseña e incluir la clave única para el consumo de los servicios. A continuación, fue necesario configurar el entorno de desarrollo, en este caso nuestro servidor en Python. La herramienta cuenta con una extensa API por lo que resulta indispensable consultar la documentación oficial de Celantur [9] para entender los métodos, los endpoints disponibles y los distintos parámetros requeridos para la anonimización de imágenes.

Con el objetivo de evaluar la eficacia de la herramienta, se realizaron pruebas utilizando diferentes rangos de parámetros. Este enfoque de modificación de parámetros nos sirvió para poder obtener y comparar los resultados obtenidos. Un aspecto relevante es que la herramienta además permite la obtención de Metadata adicional para cada imagen, lo que resulta de importancia para estas comparaciones. Finalmente, se destaca que Celantur nos permite descargar las imágenes anonimizadas a través de un enlace temporal, esto implica que no guardan ninguna información de usuarios o imágenes después de la descarga. Este último detalle fortalece la confianza en la protección de la privacidad de los datos en el sistema.



(a) Input file.



(b) Result.

Figura 2: Demo.

Fiji ImageJ2

Fiji ImageJ2 [10] es un software que permite aplicar distintos filtros a una imagen, como por ejemplo Blur Gaussiano, Mask o Noise, entre otros. Para realizar esto, se selecciona una imagen desde el sistema de archivos y se aplica un bounding box definidos por el usuario, seguido del filtro deseado, resultando en la imagen anonimizada.

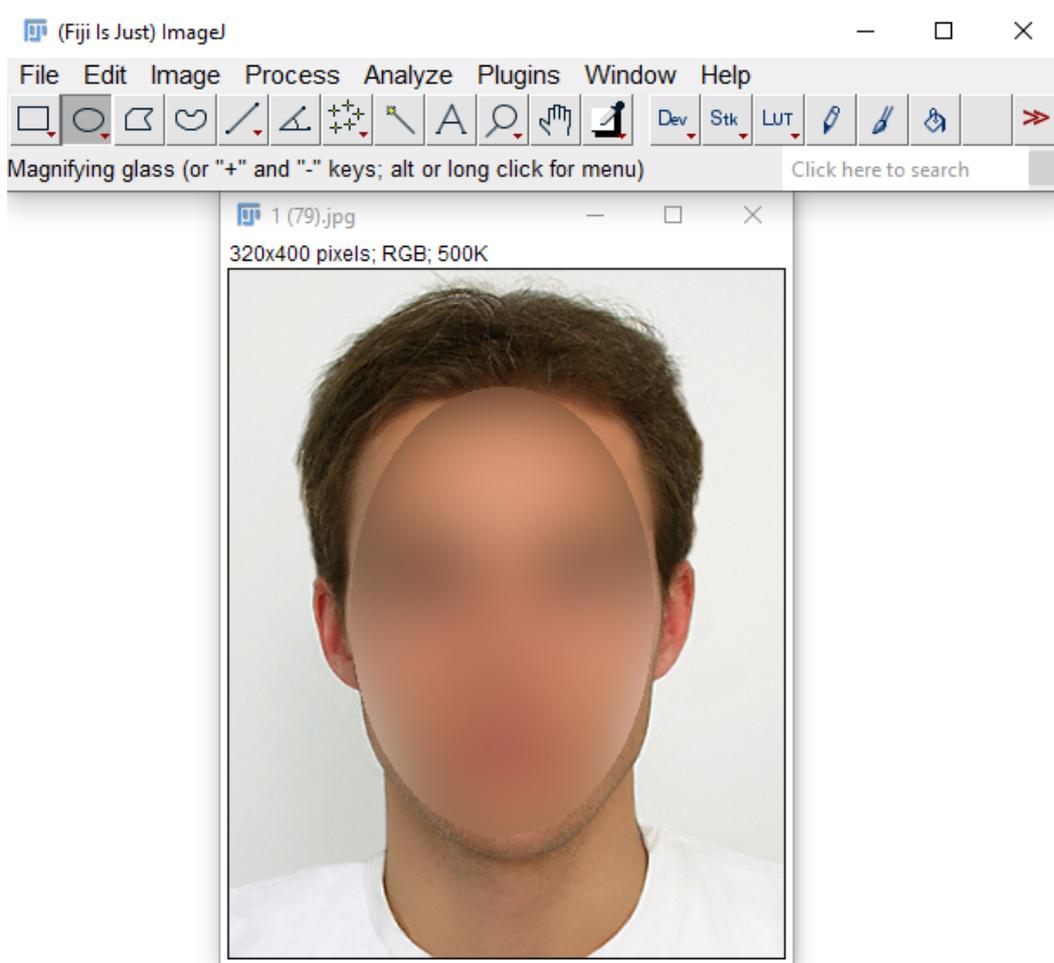


Figura 3: Blur Gaussiano utilizando Fiji ImageJ2

En este ejemplo se utilizó un blur Gaussiano. Esta opción permite definir un parámetro 'Sigma', el cual define la profundidad del blur. A mayor Sigma, mayor será la difuminación aplicada.

OpenCV

Para aplicar una posible solución con OpenCV [4] dónde fué implementado fue a través de un JupyterNotebook que es una herramienta que permite la creación de scripts en python para ejecutar de forma sencilla.

A través de esa herramienta para facilitar el desarrollo fue que se implementaron distintos módulos para la anonimización de las imágenes.

Estos módulos se utilizaron de forma secuencial o iterativa dependiendo de los parámetros ingresados en el módulo, construyendo así algo que se conoce como un pipeline de procesamiento de imágenes.

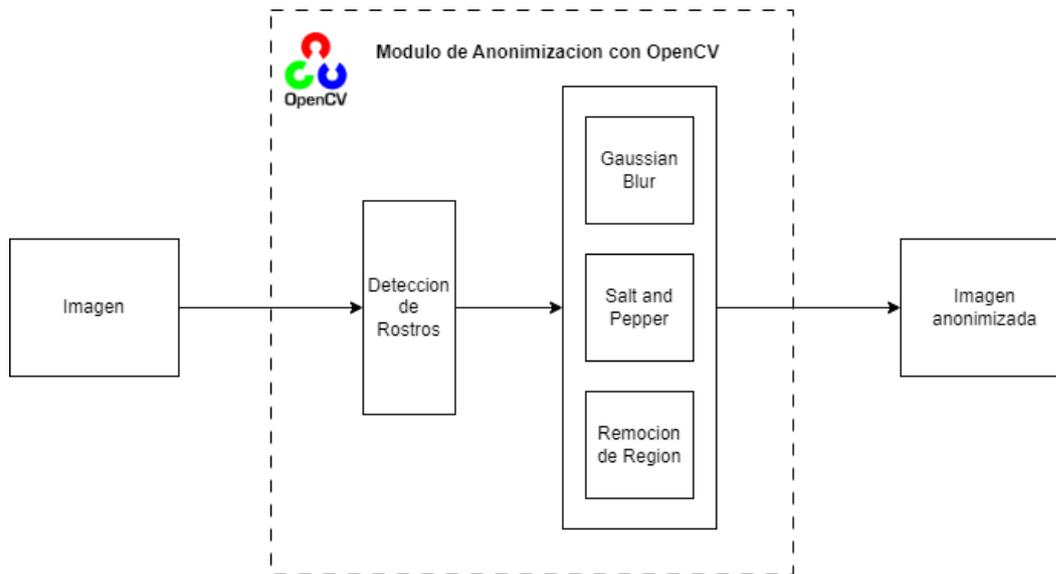


Figura 4: Pipeline de OpenCV para el tratamiento de imágenes

El módulo compuesto por los distintos métodos para agregar ruido o quitar una porción de las imágenes, permite que se indique cómo se desea realizar este proceso, permitiendo la completa modificación de este módulo en un trabajo a futuro.

Si bien esta librería permite una fácil y completa manipulación de imágenes, se requiere un desarrollo para poder acercar esta solución en algo que sea completamente funcional para cualquier usuario sin conocimientos técnicos.

Api4AI

La plataforma en la nube de Api4AI ofrece una amplia gama de herramientas, entre las cuales se encuentra la funcionalidad de Anonimización de Imágenes, como se describe en su sitio web [2] como una solución para la identificación de áreas sensibles en imágenes y la aplicación automática de blurring. Esta herramienta tiene la capacidad de identificar rostros en imágenes y aplica una máscara de blurring de forma automática, con el fin de volver este contenido sensible en las imágenes irreconocibles. Para lograr este cometido la herramienta utiliza algoritmos de aprendizaje automático para detectar las áreas donde se encuentran las caras dentro de una imagen, estas áreas se denominan bounding boxes y son utilizadas más tarde para determinar donde aplicar la máscara de blurring.

La herramienta cuenta con una Api [3] que ofrece un servicio en la cual se envía un imagen y se obtiene como resultado la imagen luego de haber sido procesada (aplicar blurring en caso

de detectar una cara) y metadata donde se agrega información sobre el procesamiento de dicha imagen.

5.2. Fortalezas y Debilidades de cada herramienta

Cuadro 1: Fiji ImageJ2

Fortalezas	Debilidades
<ul style="list-style-type: none"> ▪ Fácil utilización ▪ Interfaz de usuario amigable ▪ Permite definir bounding boxes personalizados ▪ Instalación rápida y sencilla ▪ Gran abanico de opciones de modificación de imágenes 	<ul style="list-style-type: none"> ▪ Difícil de integrar con otras herramientas ▪ No es posible utilizar de forma automatizada ▪ Poco eficiente a la hora de procesar un gran volumen de datos ▪ No ofrece métricas que midan el nivel de anonimización, ni el de re-identificación

Cuadro 2: OpenCV

Fortalezas	Debilidades
<ul style="list-style-type: none"> ▪ Ofrece varios modos de anonimización ▪ Permite una completa manipulación de imágenes ▪ Fácil de integrar con otras herramientas ▪ Extensa documentación que permite utilizar de forma precisa la herramienta ▪ Permite procesar un gran volumen de datos 	<ul style="list-style-type: none"> ▪ Requiere de desarrollo en python ▪ Requiere conocimiento de la librería ▪ Procesos complejos requieren soluciones a través de pasos intermedios ▪ La detección de rostros no es su principal funcionalidad

Cuadro 3: Api4AI

Fortalezas	Debilidades
<ul style="list-style-type: none"> ▪ Utiliza una Api web ▪ Fácil de integrar con otras herramientas debido a la documentación ▪ Permite procesar un gran volumen de datos ▪ Devuelve información relevante, como por ejemplo el porcentaje de detección de rostros 	<ul style="list-style-type: none"> ▪ Un solo método de anonimización ▪ Herramienta paga ▪ Requiere de desarrollo de código que consuma la Api de procesamiento de imágenes

Cuadro 4: Celantur

Fortalezas	Debilidades
<ul style="list-style-type: none"> ▪ Ofrece varios métodos para la anonimización ▪ Devuelve información relevante, como por ejemplo porcentaje de detección de rostros, nivel de re-identificación, y el bounding box aplicado ▪ Mantiene altos niveles de confidencialidad a la hora de anonimizar ▪ Fácil de integrar ▪ Permite procesar un gran volumen de datos ▪ Buena documentación 	<ul style="list-style-type: none"> ▪ Tiene una prueba gratis por tiempo limitado ▪ Herramienta paga

6. Conclusiones

A continuación, presentaremos las conclusiones individuales obtenidas para cada herramienta evaluada en el presente análisis. Posteriormente, consolidaremos estas observaciones para derivar en una conclusión general que abarque los aspectos más relevantes de todo el proceso de evaluación.

Celantur:

Con respecto a la herramienta, la documentación oficial de la API de Celantur se destaca por su exhaustividad, proporcionando a los usuarios información detallada sobre métodos, endpoints y parámetros. Esto contribuye significativamente a una implementación eficiente. En cuanto a la eficacia de la herramienta, se obtuvieron resultados positivos, en todos los casos del dataset de pruebas fue posible obtener la anonimización deseada. Fue posible aplicar satisfactoriamente todos los filtros (blur, mask, pixelate) y además se logró atenuar o acentuar estas modificaciones con el rango de parámetros modificables. La posibilidad de ajustar y probar diferentes configuraciones y rangos de parámetros brinda a los usuarios la flexibilidad necesaria para adaptar la anonimización a sus necesidades específicas. La herramienta ofrece un proceso de implementación intuitivo y accesible, desde el registro inicial hasta la obtención de credenciales y posterior consumo de servicios, simplificando así la integración en entornos de desarrollo.

Fiji ImageJ2:

En cuanto a la aplicación de filtros a las imágenes, esta herramienta es capaz de aplicar dichos filtros siempre y cuando haya un bounding box definido. Esto quiere decir que no hay riesgo de no poder identificar rostros debido a que es el usuario quien define dicho bounding box. Si bien esta herramienta es intuitiva y fácil de usar, debido a su naturaleza de ser un programa ejecutable operado por un usuario final, carece de la habilidad de procesar imágenes en grandes cantidades en tiempos acotados, por lo que su uso a nivel comercial se ve reducido drásticamente haciendo que otras herramientas sean más atractivas a la hora de desarrollar aplicaciones que requieran de anonimizar imágenes. Además, una fuerte desventaja de esta herramienta es que no se pueden anonimizar varios rostros que estén en una misma imagen debido a que la herramienta no permite definir múltiples cuadros delimitadores, incurriendo en la imposibilidad de procesar dichas imágenes.

OpenCV:

Para el caso de OpenCV lo principal que permite la herramienta es una completa manipulación de imágenes, y a pesar de brindar algunos modelos para detección de rostros, estos no son los más óptimos, ya que, en general, no detectan rostros que se encuentran en ángulo, sino que se detectan mejor si se encuentran de frente.

Esto nos lleva a concluir que por lo menos para poder detectar las regiones importantes a anonimizar, como lo pueden ser rostros, se necesitaría una herramienta especializada para detectar esas regiones, hoy en día es posible utilizar modelos de Computer Vision para esto, sin embargo, el entrenar un modelo excedía el alcance.

En cuanto al tratamiento de imágenes y su manipulación, es ideal, es una herramienta la cual su desarrollo continúa ² y es mantenida por la comunidad además de tener equipos dedicados en empresas multinacionales para que la librería no quede obsoleta.

Junto con esto, como permite el tratamiento de imágenes aplicando Gaussian Blur [6] en una región, aplicar Salt and Pepper o recortarla [7], es importante destacar que teniendo la región con bastante precisión utilizando un modelo, la efectividad de esta herramienta incrementa drásticamente.

Basándonos en estas condiciones, y sabiendo de sus limitaciones, la librería obtuvo resultados positivos, logró aplicar los métodos a 43 de 50 imágenes.

Para validar posteriormente la calidad y fuerza con las cuales fueron aplicados los efectos, se realizó una comparación manual entre las imágenes originales y las producidas por la herramienta.

En las primeras iteraciones de comparación, al aplicar los efectos de ruido en las imágenes no logramos una calidad deseable, llevando así que tengamos que modificar la intensidad con la cual se aplicaba el ruido o combinar distintos métodos de ruido para obtener resultados satisfactorios.

Una vez obtenidos los métodos finales con los cuales la anonimización se interpretaba como satisfactoria, procedimos a analizar más en detalle la comparación entre las imágenes obtenidas con sus originales.

En cuanto a la calidad de la información posterior a anonimizar, para los valores que aplicamos, entendemos que se sitúa en un término medio, principalmente por la agresividad de los métodos de ruido provocan que se pierdan algunos rasgos que podrían llegar a interesar mantener, por ejemplo color de ojos, color de cejas, entre otros.

Por este motivo es que también se considera que el riesgo de reidentificación es medio, ya que aplicar con poca agresividad los métodos de ruido nos permitieron al principio poder re-identificar las imágenes; sin embargo, en posteriores iteraciones, esto no fue posible.

Quedando así que, al ser dependiente de la agresividad a aplicar, se considera un riesgo medio, ya que aplicar mucha o poca, puede llegar a afectar este riesgo.

Finalmente, la reversibilidad del proceso es una tarea difícil de realizar, para los parámetros que elegimos en la última iteración, la existencia de métodos [8] no eximen la posibilidad, a pesar de esto, la detección y recuperación manual a través de métodos tradicionales no fue exitosa.

Con lo cual concluimos que la reversibilidad requiere experiencia en el área, llevando a que sea una tarea difícil de realizar debido a la agresividad aplicada en el método.

En conclusión, la librería es sencilla de utilizar, pero requiere desarrollo y dedicación a comprender las funcionalidades básicas para posteriormente aplicar algunas más complejas.

En cuanto a las características deseables, es una librería que permite la completa customización de las tareas a realizar, mientras se desarrollen correctamente. Igualmente, se podría decir que esta librería no tiene una forma de acercar fácilmente los métodos hacia el usuario final, pero un usuario técnico o especializado podría crear una herramienta amigable para

²Al día de hoy, el último release es la versión 4.8.1 con fecha 27 de Septiembre de 2023.

brindar este tipo de solución a usuarios no técnicos o sin tanto conocimiento.

En resumen, podemos concluir que se trata de una herramienta fácil de utilizar, pero que requiere arduo desarrollo. Se recomienda su empleo en procesos de anonimización que requieran un nivel de exigencia muy elevado debido a su posible customización y costo de implementación.

Api4AI:

En lo que respecta a la eficacia de la herramienta, los resultados fueron positivos, ya que logró aplicar el blurring en todas las imágenes, con la excepción de una única instancia en la que no se obtuvo el resultado deseado.

Por otro lado, para evaluar la calidad del proceso de anonimización aplicado por la herramienta, comparamos las 49 imágenes en las que se logró aplicar el desenfoque con sus respectivas imágenes originales. Este análisis se llevó a cabo con el objetivo de determinar el grado de anonimización, la calidad de la información después del proceso de anonimización, el riesgo de reidentificación y la reversibilidad del proceso.

El grado de anonimización fue significativamente elevado, ya que no fue posible identificar rostro si intentábamos buscar aquellas características que eran discernibles en la imagen original.

Respecto a la calidad de la información después de la anonimización, podemos concluir que se sitúa en un término medio. Esto se debe a que la máscara de blurring es bastante densa, lo que prácticamente la vuelve inutilizable para obtener información sobre el área donde se aplicó. Dado que podría ser de interés preservar cierta información de esas áreas para propósitos específicos de investigación, este aspecto debe ser considerado. Acompañando al comentario anterior, el riesgo de reidentificación es considerablemente bajo, dado que la herramienta exhibe una agresividad notable en cuanto al nivel de desenfoque aplicado. Esta característica dificulta significativamente el proceso de reidentificación.

Finalmente, la reversibilidad del proceso se presenta como una tarea difícil de llevar a cabo. Como se mencionó en los puntos anteriores, la imagen después del procesamiento exhibe una máscara de blurring densa y extensa, lo que complica significativamente el proceso de reversión.

En conclusión, respecto a Image Anonymization de Api4AI, es una herramienta sumamente sencilla de utilizar, dado que dispone de un servicio en la nube que realiza todo el proceso automáticamente. Nuestra única tarea consiste en enviar la imagen que deseamos anonimizar, simplificando así el procedimiento de manera considerable.

Por otro lado, la herramienta presenta algunas deficiencias en relación con los resultados obtenidos. El blurring resulta ser excesivamente agresivo en ocasiones, lo que dificulta la visualización de la imagen. Además, la herramienta tiende a generar bounding boxes algo extensos en comparación con el área efectiva en la que debería aplicarse el blurring, provocando una pérdida de información significativa en general.

En cuanto a características deseables para una herramienta de este tipo, no se cuenta con la posibilidad de ajustar el tamaño del bounding box ni de elegir otro tipo de anonimización que no sea el blurring.

En resumen, podemos concluir que se trata de una herramienta fácil de utilizar. Se reco-

mienda su empleo en procesos de anonimización que no requieran un nivel de exigencia muy elevado.

Se logró el desarrollo de muchas de las características deseadas, a pesar de esto quedan funcionalidades que serían interesantes de agregar, tanto algunas que se encontraban previamente en los objetivos como otras nuevas que surgieron durante el desarrollo.

Algunas de estas es la posibilidad de editar en pasos intermedios las regiones de interés de los rostros, permitiendo al usuario final poder agrandar o reducir dichas regiones para conservar porciones de la imagen que le sean importante conservar.

Junto con esto, una de las características que también quedó pendiente fue la posibilidad de manipular la intensidad de la anonimización, permitiendo también poder conservar algunos rasgos de las imágenes que en otros ámbitos podrían ser interesante conservar.

Resultado final

Se logró el objetivo principal del proyecto que consistía en realizar una tarea de investigación sobre el abanico de tecnologías actuales y brindar comparaciones objetivas de las herramientas disponibles. Consideramos que este documento puede servir como base de análisis para futuras decisiones técnicas hacia usuarios finales académicos.

7. Trabajo a Futuro

Se logró el desarrollo de muchas de las características deseadas, pero sin dudas quedan funcionalidades que serían interesantes de agregar, tanto algunas que se encontraban previamente en los objetivos como otras nuevas que surgieron durante el desarrollo. Así mismo, se logró aplicar distintos métodos de anonimización al set de datos establecido a través de las distintas herramientas investigadas, y distinguir las distintas fortalezas y debilidades de cada herramienta, elaborando conclusiones clave sobre las mismas.

Algunos de los puntos a investigar y desarrollar en un futuro son:

- Realizar una interfaz gráfica web: Construir un componente FrontEnd que permita a un usuario final no técnico el uso y manejo visual de la herramienta.
- Generación de Reportes y Estadísticas: Generar reportes para cada herramienta.
- Usuarios que asignen puntajes a las herramientas: Permitir tener una calificación basándose en la facilidad o parámetros de usabilidad que los usuarios finales crean pertinentes
- Permitir editar a los usuarios las regiones a anonimizar: brindar un ambiente de ejecución más customizado.

Referencias

- [1] Kaggle - Dataset Human-Faces <https://www.kaggle.com/datasets/ashwingupta3012/human-faces/>
- [2] Api4Ai - Image Anonymization <https://api4.ai/apis/image-anonymization>
- [3] Api4Ai - Api Rest de Image Anonymization <https://demo.api4ai.cloud/img-anonymization/v1/results>
- [4] OpenCV - Documentation <https://docs.opencv.org/4.x/>
- [5] OpenCV - Github <https://github.com/opencv/opencv/tree/master>
- [6] OpenCV - Gaussian Blur https://docs.opencv.org/4.x/d4/d86/group__imgproc__filter.html#gaabe8c836e97159a9193fb0b11ac52cf1
- [7] OpenCV - Basic Operations https://docs.opencv.org/4.x/de/d06/tutorial_js_basic_ops.html
- [8] Correction by Projection: Denoising Images with Generative Adversarial Networks <https://arxiv.org/abs/1803.04477>
- [9] Celantur - API Documentation <https://doc.celantur.com/cloud-api/api-endpoints>
- [10] Fiji ImageJ2 - Documentation <https://imagej.net/software/imagej2/>