

ATTENTION U-NET KẾT HỢP PHÂN TÍCH NHIỀU ĐỂ PHÂN ĐOẠN VÙNG GIẢ MẠO TRÊN ẢNH HÓA ĐƠN

GVHD: PGS. TS. Lê Đình Duy

Học viên: Huỳnh Thiên Phước - 250101052

Tóm tắt

- Lớp: CS2205.SEP2025
- Link YouTube:
<https://www.youtube.com/watch?v=STBvjNW0V0k>
- Họ và tên: Huỳnh Thiên Phước - 250101052
- Tổng số slides không vượt quá 10
- Slides có sử dụng 1 số hình ảnh được tạo từ NotebookLM và Gemini Nano Pro nhằm phát thảo ý tưởng.




Giới thiệu - Bối cảnh và vấn đề

Thanh toán số bùng nổ, hóa đơn ảnh/scan trở thành chứng từ pháp lý chính.

Công cụ chỉnh sửa (Photoshop, GenAI) ngày càng tinh vi, mắt thường không thể phát hiện.

Nguy cơ thất thoát tài chính lớn cho doanh nghiệp và bảo hiểm.

INVOICE #00123		Date: 20/10/2023
Item A		\$100.00
Item B		\$200.00
TOTAL		\$5,000.00
		 Fake Number!

"Con số có thể bị sửa đổi pixel hoàn hảo, nhưng cấu trúc ảnh thì không."

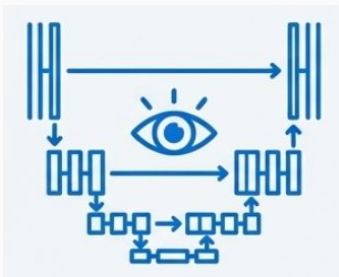
Mục tiêu



01

Xây dựng bộ dữ liệu

Thiết lập quy trình sinh dữ liệu giả lập (Synthetic Data Generation) tự động để tạo ra hàng nghìn mẫu hóa đơn bị chỉnh sửa (Splicing/Inpainting).



02

Phát triển Mô hình

Xây dựng kiến trúc **Attention U-Net** kết hợp bộ lọc nhiễu **SRM** để tối ưu hóa khả năng phát hiện chỉnh sửa trên ảnh tài liệu.



03

Đánh giá Hiệu năng

Đạt chỉ số F1-Score > 80% và chứng minh hiệu quả vượt trội so với các phương pháp truyền thống. Có khả năng ứng dụng thực tế.

Nội dung và Phương pháp - Tạo dữ liệu

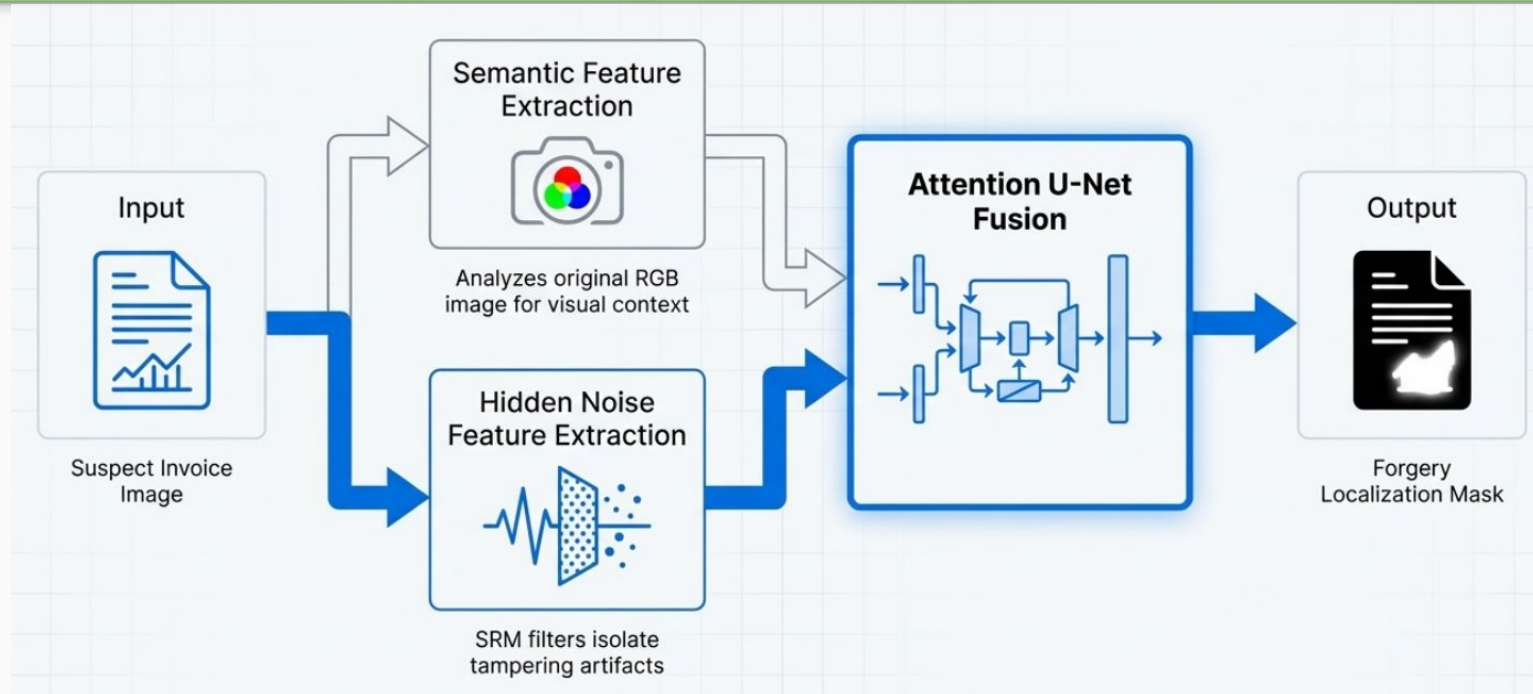


Vấn đề: Thiếu dữ liệu huấn luyện trong lĩnh vực pháp y tài liệu hoá đơn.

Hướng giải quyết: Dùng script để sinh dữ liệu đã bị chỉnh sửa dựa trên dữ liệu gốc thông qua phương pháp:

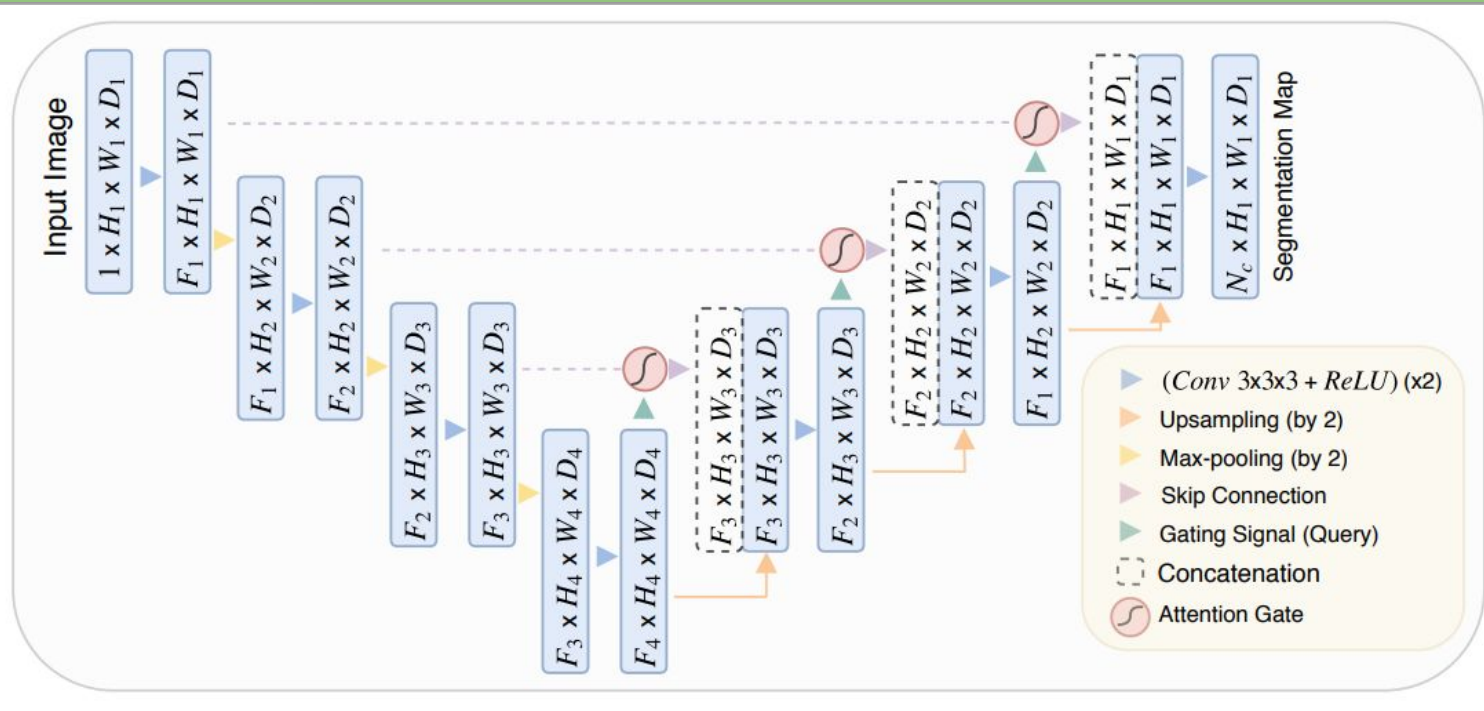
- **Splicing:** Cắt vùng văn bản từ hóa đơn này ghép sang hóa đơn khác.
- **Inpainting:** Xóa số liệu gốc và chèn số liệu mới với font chữ tương tự

Nội dung và Phương pháp - Pipeline



Ý tưởng chính: Hệ thống kết hợp cả thông tin thị giác (phân tích RGB) và thông tin nhiễu để đưa vào mạng Attention U-Net, giúp phát hiện các vết chỉnh sửa tinh vi.

Nội dung và Phương pháp - Attention U-Net



Tích hợp các module **Attention Gate** tại các kết nối nhảy (skip connections) giữa luồng Encoder và Decoder. Mục đích là lọc bỏ các tín hiệu từ vùng nền và tăng cường tín hiệu tại vùng biên của vết chỉnh sửa.

Kết quả dự kiến

Company Name

Ober Company
133 Company Street
Karian, NA 65126
E-mail: mvinn@gmail.com

COMMERCIAL INVOICE

Tonore: 0082366
Commercial AC30050
TN9/6/787/22

Vendor Information

Vendery Nom
12\$ Loney Street
Commerella, NX 25115
Phone: 335 6864

Vendor Information

Condary: Company
Besonarve: Matminsam
Cost: 00233

Item Description	Quantity	Unit Price	Total
One plated provates hroscnest	1	\$30.00	\$150.00
Subscribed fnovatore otk's mast	1	\$19.00	\$158.00
Resert the ment brshere mauertitibes	1	\$20.00	\$50.00
Resers snape of item	1	\$10.00	\$36.00
Subtotal			\$394.00
TOTAL AMOUNT DUE			\$2,135.00

Description:

A forgery designed to be undetectable by the human eye.

Source Sans Pro:

Source Sans Pro 412345

Model

Company Name

Ober Company
133 Company Street
Karian, NA 65126
E-mail: mvinn@gmail.com

COMMERCIAL INVOICE

Tonore: 0082366
Commercial AC30050
TN9/6/787/22

Vendor Information

Vendery Nom
12\$ Loney Street
Commerella, NX 25115
Phone: 335 6864

Vendor Information

Condary: Company
Besonarve: Matminsam
Cost: 00233

Item Description	Quantity	Unit Price	Total
One plated provates hroscnest	1	\$30.00	\$150.00
Subscribed fnovatore otk's mast	1	\$19.00	\$158.00
Resert the ment brshere mauertitibes	1	\$20.00	\$50.00
Resers snape of item	1	\$10.00	\$36.00
Subtotal			\$394.00
TOTAL AMOUNT DUE			\$2,135.00

Description:

A forgery designed to be undetectable by the human eye.

Source Sans Pro:

Source Sans Pro 412345

- Hệ thống có thể dự đoán được vị trí đã bị chỉnh sửa và highlight.
- Chỉ số F1-Score > 0.8.
- Thời gian xử lý ~1s cho mỗi hoá đơn.

Tài liệu tham khảo

- [1]. Ronneberger, O., Fischer, P., & Brox, T. (2015). "U-Net: Convolutional Networks for Biomedical Image Segmentation." MICCAI
- [2]. Oktay, O., et al. (2018). "Attention U-Net: Learning Where to Look for the Pancreas." Medical Imaging with Deep Learning
- [3] Zhou, P., et al. (2018). "Learning Rich Features for Image Manipulation Detection." CVPR.
- [4] Bi, X., et al. (2019). "RRU-Net: The Ringed Residual U-Net for Image Splicing Forgery Detection." CVPR Workshop.
- [5] Kwon, M. J., et al. (2021). "CAT-Net: Compression Artifact Tracing Network for Detection and Localization of Image Splicing." NeurIPS.