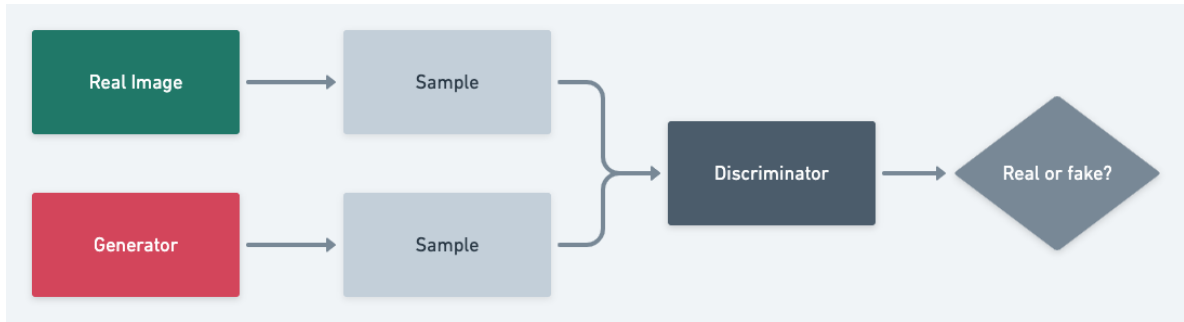


Họ và tên (IN HOA)	TRẦN ANH TUẤN
Ảnh	
Số buổi vắng	0
Bonus	16
Tên đề tài (VN)	PHÁT HIỆN TÀI LIỆU GIẢ DỰA VÀO PHƯƠNG PHÁP GAN
Tên đề tài (EN)	DETECT FAKE DOCUMENTS USING GENERATIVE ADVERSARIAL NETWORK
Giới thiệu	<p>Với sự phát triển của xã hội kéo theo các vấn đề về hành chính, giấy tờ pháp lý đối với mỗi người khi các cơ quan chức năng yêu cầu ngày càng gia tăng. Nhiều người không có các giấy tờ cần thiết mà các cơ quan chức năng yêu cầu nên tiến hành làm giả giấy tờ để qua mặt các cơ quan này. Ví dụ như tài liệu thế ước, chứng từ, hóa đơn, giấy tờ cá nhân, chứng minh thư ... dễ dàng bị làm giả bằng nhiều hình thức khác nhau. Nhiều người có thể lợi dụng</p>

để mạo danh những người khác để làm việc trái pháp luật. Các cơ quan chức năng rất khó để xác minh được những tài liệu này là giả hay thật. Hoặc việc sản xuất tiền giả rất dễ dàng lưu thông trong xã hội và qua mắt được mọi người vì độ tinh xảo và tỉ lệ giống thật rất cao, bằng những phương pháp thông thường rất khó có thể kiểm tra được. Chính vì vậy thông qua đề tài luận văn này, tôi đưa ra một phương pháp để xác định tài liệu có được làm giả hay không.

GAN (generative adversarial network) là một phương pháp dùng để sinh ra dữ liệu mới sau một quá trình học và tự kiểm tra dữ liệu có phải giả hay không. Nó có thể tự sinh ra một đối tượng mới, chữ viết mới, tài liệu mới, ... mà con người khó có thể nhận ra nó được tạo từ máy tính hay không. Trong GAN có quá trình sinh ra dữ liệu và tự kiểm tra dữ liệu có phải được tạo ra từ máy tính hay không. Ứng dụng việc tự kiểm tra dữ liệu sau mỗi lần học của GAN, máy tính có thể kiểm tra được các tài liệu đầu vào có bị làm giả hay không.

- Input: ảnh tài liệu cần kiểm tra việc làm giả.
- Output: đưa ra kết quả dự đoán cho tài liệu có phải là giả hay không.



Hình 1. Minh họa mô hình GAN

Mục tiêu	<ul style="list-style-type: none">- Tìm hiểu và xây dựng được mô hình GAN, nghiên cứu cơ chế, cách thức hoạt động của mô hình generator model và discriminator model.
----------	---

	<ul style="list-style-type: none"> - Xây dựng hệ thống phát hiện tài liệu giả mạo dựa vào mô hình discriminator model trong mô hình GAN. - Liên kết với cơ quan chức năng (công an, sở ban ngành khác) để sử dụng các tài liệu đã được cơ quan chức năng đã đánh giá. Thực hiện dự đoán với các tài liệu đó trên hệ thống xây dựng. Đánh giá, so sánh với các hệ thống đã công bố.
Nội dung và phương pháp thực hiện	<p><i>Nội dung 1: Tìm hiểu mô hình GAN</i></p> <ul style="list-style-type: none"> - <i>Mục tiêu:</i> <p>Hiểu được mô hình GAN là gì, các thành phần có trong mô hình. Hai mô hình chính của GAN là generator và discriminator model. Hiểu được và cách thức hoạt động của hai mô hình chính này trong quá trình tự học.</p> <p>Phân tích các mô hình GAN đã công bố. Đánh giá điểm mạnh, yếu của các mô hình.</p> <p>Thực hiện cài đặt, chạy thử các mô hình GAN đã tìm hiểu.</p> - <i>Phương pháp:</i> <p>Tìm các bài báo khoa học liên quan tới GAN đã được công bố và nghiên cứu nội dung chi tiết.</p> <p>Dựa vào những gì mà các tác giả chia sẻ trong bài báo, tiến hành cài đặt, chạy thử các thử nghiệm trên các mô hình đó.</p> <p><i>Nội dung 2: Xây dựng mô hình phát hiện tài liệu giả mạo</i></p> <ul style="list-style-type: none"> - <i>Mục tiêu:</i> <p>Xây dựng hệ thống phát hiện tài liệu giả dựa trên các mô hình đã nghiên cứu ở nội dung 1. Hệ thống phải đảm bảo được discriminator model nhận dữ liệu đầu vào từ bên ngoài để đánh giá được tài liệu có phải là giả mạo hay không. Sau mỗi lần đánh giá, xác nhận kết quả và ghi nhận lại kết quả để cải thiện cho lần đánh giá tiếp theo.</p>

	<ul style="list-style-type: none"> - Phương pháp: <p>Xây dựng hệ thống phát hiện tài liệu giả mạo. Hệ thống phải đảm bảo tính chất của mô hình GAN.</p> <p>Dựa vào đặc trưng của mô hình GAN, ngoài việc để generator tự tạo dữ liệu cho discriminator hoạt động và cải thiện chất lượng đánh giá như mô hình đã đề xuất. Cho phép discriminator đánh giá các kết quả đã được phân loại để cải thiện chất lượng.</p> <p>Nội dung 3: Đánh giá</p> <ul style="list-style-type: none"> - Mục tiêu: <p>Sau khi xây dựng được hệ thống, cần phải đánh giá mức độ chính xác và hiệu quả của hệ thống.</p> <p>Tiếp cận với các cơ quan chức năng thường xuyên gặp phải các vấn đề về làm giả như công an, các sở ban ngành để thu thập dữ liệu và đánh giá trên các bộ dữ liệu mà đã được các cơ quan phân loại.</p> - Phương pháp: <p>Dựa vào dữ liệu từ các cơ quan chức năng cung cấp đã được phân loại, đánh giá. Thực hiện lại việc đánh giá trên hệ thống xem mức độ chính xác của hệ thống đã cài đặt. Ngoài ra các dữ liệu chưa được phân loại của các cơ quan có thể thực hiện đánh giá trên hệ thống để tham khảo cho các cơ quan chức năng.</p>
Kết quả dự kiến	<ul style="list-style-type: none"> - Xây dựng được hệ thống phát hiện tài liệu giả và cài đặt hệ thống này cho các cơ quan chức năng như một kết quả tham khảo. - Hiểu và nắm được mô hình GAN và các thành phần bên trong. - Đánh giá hệ thống đã cài đặt so với các phương pháp GAN đã công bố. - Bộ dữ liệu thu thập được từ các cơ quan chức năng.

Tài liệu tham khảo	<p>[1] Woohyeon Shim, Minsu Cho. CircleGAN: Generative Adversarial Learning across Spherical Circles. In arXiv:2011.12486v2, 2021.</p> <p>[2] Phillip Isola Jun-Yan Zhu Tinghui Zhou Alexei A. Efros. Image-to-Image Translation with Conditional Adversarial Networks. In arXiv:1611.07004v3, 2018.</p> <p>[3] Gefei Wang, Yuling Jiao, Qian Xu, Yang Wang, Can Ya. Deep Generative Learning via Schrodinger Bridge. In arXiv:2106.10410v1, 2021.</p> <p>[4] T. Chen, M. Lucic, N. Houlsby, and S. Gelly. On self modulation for generative adversarial networks. In Proceedings of International Conference on Learning Representations (ICLR), 2019.</p> <p>[5] Xi Chen, Yan Duan, Rein Houthoofd, John Schulman, Ilya Sutskever, Pieter Abbeel. InfoGAN: Interpretable Representation Learning by Information Maximizing Generative Adversarial Nets. In arXiv:1606.03657v1, 2016.</p> <p>[6] Ian J. Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, Yoshua Bengio. Generative Adversarial Nets. In arXiv:1406.2661v1, 2014.</p> <p>[7] Zhirui Zhang, Shujie Liu, Mu Li, Ming Zhou, Enhong Chen. Bidirectional Generative Adversarial Networks for Neural Machine Translation. Proceedings of the 22nd Conference on Computational Natural Language Learning, 2018, pp. 190-199.</p> <p>[8] T. Karras, T. Aila, S. Laine, and J. Lehtinen. Progressive growing of gans for improved quality, stability, and variation. In arXiv:1701.10196, 2017.</p>
-----------------------------------	---