IOSR Journal of Business and Management (IOSR-JBM)
e-ISSN:2278-487X, p-ISSN: 2319-7668. Volume 26, Issue 7. Ser. 6 (July. 2024), PP 63-66
www.iosrjournals.org

The Potential Use Of Gan In Electronic Payment: Based On Face Recognition

Junli Zhang
Department Of E-Commerce, Shenzhen Campus, Jinan University, China

Abstract:
A more significant issue with identity security is facing electronic payments, a relatively new industry in the Internet era, as a result of the rapid growth of artificial intelligence technologies. GAN, a type of deep learning model, has strong generative and discriminative capabilities that may be useful in finding a solution to the security issue with electronic payments. Since there isn't much research on GAN in the field of e-payments right now, this paper analyzes GAN qualitatively, conceptualizes application scenarios, and makes the proposal that GAN can simulate realistic images and data, improve recognition accuracy, detect forged information, and increase e-payment security while also analyzing its limitations and offering recommendations for future research in the field.

***Key Word**: Generative Adversarial Networks; Electronic Payment; Face Recognition; Application Scenarios*

Date of Submission: 08-07-2024 Date of Acceptance: 18-07-2024

I. Introduction

The swift advancement of artificial intelligence technology is significantly altering our lives in this age of constantly evolving technology. The quick growth of AI technologies, like ChatGPT4.0, in many spheres of our society has demonstrated once more the incredible potential of AI. With its distinct generation and discriminating methods, GAN (Generative Adversarial Network), an AI technology founded on the premise of the "two-player zero-sum game," has revolutionized numerous fields in recent years. Due to its many advantages—such as being quick and easy, overcoming space and time constraints, and more—electronic payment, a relatively new product of the Internet era, has significantly increased transaction efficiency and provided consumers with tremendous convenience. As a result, it has gained popularity as a means of making payments. It is important to remember, meanwhile, that security concerns are also becoming more widespread. An pressing issue is how to maintain the security of the payment process—particularly the veracity of identification—while still taking advantage of the conveniences of electronic payment.

In this regard, the development of GAN technology creates new opportunities for e-payment. GAN has enormous potential in the realm of identity identification because of its potent generating capabilities, which allows it to generate incredibly realistic images or data. For instance, GAN can assist in increasing the number of training samples and enhancing the precision and universality of face recognition algorithms. Additionally, the discriminative power of GAN can be applied to identify false identification data, so enhancing the security of electronic payments even more. "GAN Open Set Recognition" is a novel face recognition system that was introduced at the 2021 International Conference on Computer Vision (ICCV 2021). "GAN Open Set Recognition" is a new face recognition system that was officially introduced in 2021 at the most recent International Conference on Computer Vision (ICCV 2021)(Kong and Ramanan 2022). These data all indicate that GAN is progressively moving toward this new course.

There is currently very little study on GAN in the subject of e-payments, despite the fact that it has a wide range of potential applications. Consequently, this study uses facial recognition as an example to thoroughly analyze the use of GAN in e-payment and its impact on e-payment security, taking into account the current identity security risk in e-payment. We will examine the possible benefits and difficulties of GAN in e-payments using qualitative analytical techniques along with examples from the literature already in existence. Our goal is to offer helpful resources and insights for the advancement of the e-payment industry.

II. Fundamental Idea And Advantages Of Gan

Fundamental Idea Of Generating Adversarial Networks

In 2014, Ian J. Goodfellow introduced a deep learning model called Generative Adversarial Networks(Goodfellow et al. 2014). Under GAN, unsupervised learning is carried out by two opposing neural networks (the discriminator and the generator), each of which is made up of two opposing neural networks. The generator's job is to learn the distribution of real data and produce new, supposedly real data samples. It accomplishes this by taking in low-dimensional random noise and producing high-dimensional data samples (such as pictures). In contrast, the discriminator is a binary classifier that outputs a probability value based on whether the input data is generated by the generator or comes from a genuine dataset.

In a GAN, the discriminator and the generator engage in a dynamic game that is zero-sum, meaning that neither side can win or lose; this means that cooperation between the two sides is impossible and can be compared to "mutual combat" between the left and right hands. The generator strives to produce increasingly plausible scenarios. In an attempt to fool the discriminator, the generator attempts to produce ever-more-realistic data, but the discriminator's capacity to discern between created and genuine data keeps becoming better. Throughout the training process, this antagonism causes the two to change until they eventually achieve a saturated state.

The gradient descent method and the backpropagation algorithm are typically used to realize its training process. The discriminator receives inputs in the form of created and actual data in each iteration before producing an output that is either generated or real. Next, the discriminator's loss is computed, and backpropagation is used to adjust its parameters (weights, biases, etc.). The generator then creates new data and engages in combat with the discriminator once more, refining its parameters and calculating the loss to maximize output. Until the generator can provide data that is realistic enough to prevent the discriminator from telling genuine data from generated data, this procedure is repeated.

Advantages Of GAN And Current Status Of Applications

GAN has a number of advantages over variational autoencoders and autoencoders, primarily related to their capacity to produce realistic new samples and their special adversarial training method. In particular, GAN enables the generator to use another network that has been asynchronously trained to distinguish between "generated" and "real" data, and to progressively learn how to generate more realistic, high-quality fake data without requiring a significant amount of labeled data through the adversarial training of generators and discriminators. GANs are more adept at handling complex data, capturing underlying distributions and patterns, and producing data that adheres to particular distributions than autoencoders and variational autoencoders, which concentrate on learning and reconstructing data representations and might not produce as realistic and diverse data.

Holding such more desirable performance, GANs have made good progress in many fields(Cheng et al. 2020). For example, GAN can be used in text processing or natural language processing for dialog generation. In addition, it has contributed in the fields of audio processing, computer vision, and biology(Liu et al. 2022; Cao et al. 2019; Zhao et al. 2021). This paper focuses on the application of GAN in e-payment.

III. Principles Of Secure Identification For Electronic Payments

Advantages And Applications Of Face Recognition Technology

An essential component of many security technologies is authentication technology, commonly referred to as identity security recognition technology. These methods for identification and authentication also include Hong Membrane, fingerprint, and facial recognition. One of the most widely used technologies in recent years is face recognition, which uses data from a person's facial features to verify an identity.(Happy and Routray 2015; Corneanu et al. 2016). Face recognition technology is used in the medical profession to help with identity verification and electronic medical record administration, which enhances patient safety and efficiency. Furthermore, facial recognition holds significant value in the domains of justice and public safety, including the detection and apprehending of runaways and prison administration. To improve the client experience, it also offers quick check-in and check-out services to the tourism and hospitality sectors. Overall, the non-contact, quick, and accurate properties of face recognition technology are making it increasingly popular.

The use of facial recognition in electronic payments is primarily seen in "face swipe payment." The electronic gadget uses a camera to take a picture of the user's face, which it then compares to the pre-registered facial data in the system to confirm the user's identity and finish the payment process. China has a lot of big-box stores and restaurants that accept this form of payment, which is an excellent illustration of how well face recognition technology works with electronic payments.

Security Risks Of Face Recognition Technology

Like all things, facial recognition technology has two sides. People will find it convenient, but there are security dangers involved as well, like identity theft and counterfeiting, loss of confidential data, and so forth.

One of the most frequent risks associated with e-payments is the possibility of face theft and impersonation. This means that an attacker could use a face recognition system to trick the system by dressing in disguise, such as masks, hats, or glasses, or by breaking into the system or equipment and substituting a digital sample for the real face image. This would allow the attacker to pose as someone else for illicit purposes. In addition to posing a risk for identity theft, this one might have major repercussions like financial loss and privacy breaches. On the other hand, the danger of sensitive information leakage refers to the possibility that private information, including the user's identity and facial features, may be incorrectly gathered, stored, communicated, and used during the face recognition process. This danger could result from human error, inadequate data protection procedures, and system security flaws. In any event, once private data is exposed, criminals may utilize it to carry out illegal activities such as fraud, identity theft, hostile attacks, and other crimes that could seriously hurt users.

Thus, applying generative adversarial network technology and its derivatives can, in part, reduce the likelihood of such dangers arising in electronic payment scenarios based on such a status quo.

IV. Scenario Conceptualization And Security Analysis Of Gan Application In Electronic Payment

Improvement Of Data And Adversarial Training

Although there aren't many real-world examples of GAN applications on e-payments to increase face recognition security, we can conceptualize some possible or understudied application scenarios based on a qualitative analysis of the principles and benefits of GAN.

In the first case, GAN serves as a generative model to support other methods rather than being used directly for identification. With data augmentation and adversarial training, it can be utilized to strengthen the face swipe payment system's identity security.

Here is an example of how to follow its application directions: The dataset used to train the recognition model in e-payment facial recognition systems determines the level of identification accuracy. In actuality, though, it could be somewhat tricky to gather enough complex and diverse data to train the model. To broaden and diversify the dataset, synthetic face images can be produced with GAN. In other words, a GAN model is constantly trained to produce a large number of synthetic images that are identical to real-world face images and mimic face images in a variety of settings, including altered lighting, angles, occlusions, and facial expressions. To give an example, when a person wears a mask, cap, or other occluding item, parts of their facial features may be partially obscured. By enhancing the original dataset and strengthening the recognition model's resilience to handle a range of complicated scenarios, these artificial images can help to increase security.

Furthermore, adversarial examples—that is, samples that have been subtly altered but yet contain enough information to trick the recognition model—can be produced using GAN. These hostile samples can be added to the training set to help the recognition model become more adept at fending off possible attacks and enhancing identification security.

Generating Virtual Face Models To Aid Fraud Detection

Due to the growing acceptance of "face-to-face payments," scammers are constantly searching for new methods to get around these supposedly unbreakable identification procedures. They could try to fool the identification system by using a range of high-tech techniques, such pictures, HD movies, or even complex 3D masks that imitate a real user's face.

To combat this kind of fraud, in the second scenario GAN can be used to create virtual face models. These models can mimic a range of fraudulent behavior may produce images, such as the use of photos, video screenshots, or manipulated face images. These artificial images not only resemble the real thing in appearance but also include a variety of fraudulent methods that fraudsters may attempt. These artificial images can then be added to the training set, acting as a fraud detection model of the "textbook," helping the system to detect fraud more precisely and enhancing its capacity to detect fraudulent activity, ensuring that fraudulent behavior has nothing to hide. Should the complete electronic payment recognition system for fraud detection be likened to the "police to catch thieves," then the introduction of GAN may be compared to the police offering a police car to aid in the more effective and successful pursuit of criminals. In these kinds of application settings, GAN helps to enhance the security of e-payment identification.

V. Analysis Of Limitations

In the area of electronic payments, GAN can potentially be limited by the following factors. The first is that the generated samples are restricted in scope. Through data augmentation and adversarial training, GAN can produce virtual face models, but the number of generated samples is still restricted. This implies that GAN might not be able to cover every potential fraud pattern in the face of increasingly complex fraud strategies, which could result in undiscovered hazards to identity security. Second, the model's complexity: the GAN model must simultaneously train the discriminator and generator networks, which results in an excessive number of model parameters and a significant amount of processing. This may have an impact on fraud detection accuracy and real-time in addition to raising the computational cost. The issue of data imbalance is the final one. Data imbalance is a common issue that arises throughout the GAN training process and can result in the model performing poorly in certain scenarios. This could have an impact on fraud detection accuracy, particularly in complex case situations.

VI. Summary

With its distinct adversarial structure and unsupervised learning capabilities, GAN, an artificial intelligence tool, lets us understand the potential it has opened up for the electronic payment industry in recent years. We can infer from the realistic background that facial recognition is the more widely used form of identifying technology in the electronic payment space. This study uses facial recognition as an example, and we evaluate how to improve the security of GAN in the field of electronic payment through the conceptualization of the application scenario based on the fundamental idea of GAN and the different hazards of present identification.

Despite possible limitations, overall, GAN will continue to unlock its potential to have a more positive and constructive effect on the electronic payments space in the future.