ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ
МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ КАЗАХСТАН
MINISTRY OF SCIENCE AND HIGHER EDUCATION OF THE REPUBLIC OF KAZAKHSTAN

ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ

МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

2024 (17) 1

Қаңтар – наурыз

ISSN 2708–2032 (print)
ISSN 2708–2040 (online)

Халықаралық ақпараттық және коммуникациялық технологиялар журналы
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Меншіктенуші: «Халықаралық ақпараттық технологиялар университеті» АҚ (Алматы қ.).
Қазақстан Республикасы Ақпарат және әлеуметтік даму министрлігінің Ақпарат комитетінде – **20.02.2020** жылы берілген.
№ KZ82VPY00020475 мерзімдік басылым тіркеуіне қойылу туралы куәлік.
Тақырыптық бағыты: ақпараттық технологиялар, әлеуметтік-экономикалық жүйелерді дамытудағы цифрлық технологиялар, ақпараттық қауіпсіздік және коммуникациялық технологияларға арналған.
Мерзімділігі: жылына 4 рет.
Тиражы: 100 дана
Редакцияның мекенжайы: 050040, Алматы қ-сы, Манас к-сі, 34/1, 709-кабинет, тел: +7 (727) 244-51-09.
E-mail: ijict@iitu.edu.kz Журнал сайты: https://journal.iitu.edu.kz

Международный журнал информационных и коммуникационных технологий
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Собственник: АО «Международный университет информационных технологий» (г. Алматы).
Свидетельство о постановке на учет периодического печатного издания в Министерство информации и общественного развития Республики Казахстан **№ KZ82VPY00020475,** выданное от **20.02.2020 г.**
Тематическая направленность: информационные технологии, информационная безопасность и коммуникационные технологии, цифровые технологии в развитии социо-экономических систем**.**
Периодичность: 4 раза в год.
Тираж: 100 экземпляров.
Адрес редакции: 050040 г. Алматы, ул. Манаса 34/1, каб. 709, тел: +7 (727) 244-51-09.
E-mail: ijict@iitu.edu.kz Сайт журнала: https://journal.iitu.edu.kz

---

«International Journal of Information and Communication Technologies»
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Owner: International Information Technology University JSC (Almaty).
The certificate of registration of a periodical printed publication in the Ministry of Information and Social Development of the Republic of Kazakhstan, Information Committee No. KZ82VPY00020475, issued on 20.02.2020.
Thematic focus: information technology, digital technologies in the development of socio-economic systems, information security and communication technologies
Periodicity: 4 times a year.
Circulation: 100 copies.
Editorial address: 050040. Manas st. 34/1, Almaty. +7 (727) 244-51-09. E-mail: ijict@iitu.edu.kz
Journal website: https://journal.iitu.edu.kz

МАЗМҰНЫ

ӘЛЕУМЕТТІК-ЭКОНОМИКАЛЫҚ ЖҮЙЕЛЕРДІ ДАМЫТУДАҒЫ ЦИФРЛЫҚ ТЕХНОЛОГИЯЛАР

АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАР

АҚПАРАТТЫҚ ҚАУІПСІЗДІК ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАРҒА АРНАЛҒАН

СОДЕРЖАНИЕ

ЦИФРОВЫЕ ТЕХНОЛОГИИ В РАЗВИТИИ СОЦИО-ЭКОНОМИЧЕСКИХ СИСТЕМ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

CONTENTS

DIGITAL TECHNOLOGIES IN THE DEVELOPMENT OF SOCIO-ECONOMIC SYSTEMS

INFORMATION TECHNOLOGY

INFORMATION SECURITY AND COMMUNICATION TECHNOLOGIES

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Vol. 5. Is. 1. Number 17 (2024). Pp. 122–134
Journal homepage: https://journal.iitu.edu.kz
https://doi.org/*10.54309/IJICT.2024.17.1.010*

ANALYSIS OF VOICE IMPERSONATION FRAUD: RISKS, CASES AND DEFENSE STRATEGIES

P.S. Pustovoitov[1*], N.A. Seilova[1], A.S. Gnatiuk[2]
International Information Technology University, Almaty, Kazakhstan.
E-mail: *36060@iitu.edu.kz*

Pustovoitov Pavel — master's student, Faculty of Computer Technologies and Cyber Security, International Information Technology University, Almaty, Kazakhstan
E-mail: *36060@iitu.edu.kz.* ORCID: 0009-0004-9188-2578;
Seilova Nurgul — candidate of Technical Sciences, associate professor, Department of Computer Engineering, International Information Technology University, Almaty, Kazakhstan
E-mail: nseilova@iitu.edu.kz. ORCID: 0000-0003-3827-179X
A.S. Gnatiuk — Doctor of Technical Sciences, Professor, National Aviation University, Kiev (Ukraine)

Abstract. The article provides analysis of the increasing menace posed by voice impersonation fraud in the era of digital technology. It emphasizes the progress achieved in DeepFake and Real-Time vocal Cloning (RVC) technologies, which made vocal impersonation not only feasible, but persuasive and easily accessible. The study examines some incidents in which modern technologies were employed for fraudulent purposes, emphasizing the gravity and potential ramifications of the offenses. The paper explores the difficulties encountered in identifying and thwarting voice impersonation fraud, analyzing the most recent advancements in cybersecurity and digital forensics designed to address this problem. The authors highlight the significance of creating strong defense plans and the necessity for continuous study in order to cope with quickly advancing technologies and discuss the ethical and legal consequences of voice impersonation, emphasizing the need for well-defined norms and ethical principles in the utilization of voice synthesis technologies.

Keywords: DeepFake technology, Real-Time Voice Cloning (RVC), biometric authentication, voice recognition technology, Artificial Intelligence (AI) in fraud, advanced voice synthesis techniques

For citation: P.S. Pustovoitov, N.A. Seilova, A.S. Gnatiuk. ANALYSIS OF VOICE IMPERSONATION FRAUD: RISKS, CASES AND DEFENSE STRATEGIES //INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES. 2024. Vol. 5. No. 17. Pp. 120–134 (In Eng.). https://doi.org/*10.54309/IJICT.2024.17.1.010*.

ДАУЫС ЖАЛҒАН ӘДІСТЕРІН ТАЛДАУ: ТӘУЕКЕЛДЕР, ЖАҒДАЙЛАР ЖӘНЕ ҚОРҒАУ СТРАТЕГИЯЛАРЫ

П.С. Пустовойтов[1*], Н.А. Сейлова[1], А.С. Гнатюк[2]
Халықаралық ақпараттық технологиялар университеті.
E-mail: *36060@iitu.edu.kz*

Пустовойтов Павел — Халықаралық ақпараттық технологиялар университетінің компьютерлік технологиялар және киберқауіпсіздік факультетінің магистрі, есептеу техника және бағдарламалық қамтамасыз ету білім бағдарламасы
E-mail: *36060@iitu.edu.kz.* ORCID: 0009-0004-9188-2578;
Сейлова Нургуль — техника ғылымдарының кандидаты, компьютерлік инженерия кафедрасының доценті, Халықаралық ақпараттық технологиялар университеті
E-mail: nseilova@iitu.edu.kz. ORCID: 0000-0003-3827-179X.
А.С. Гнатюк — техника ғылымдарының докторы, профессор Ұлттық авиация университеті, Киев (Украина

Аннотация. «Жалған дауыс әдістерін талдау: тәуекелдер, жағдайлар және қорғау стратегиялары» деп аталатын мақалада цифрлық технология дәуірінде дауысты еліктеу алаяқтықтан туындайтын қауіп-қатер жан-жақты талданады. Мәтін DeepFake және Real-Time вокалды клондау (RVC) сияқты технологияларда қол жеткізілген прогреске ерекше назар аударылады, бұл дауысты еліктеуді жүзеге асыруға ғана емес, сонымен бірге сенімдірек және оңай қол жеткізуге мүмкіндік берді. Зерттеу осы құқық бұзушылықтардың ауырлығы мен ықтимал салдарларына баса назар аудара отырып, алаяқтық мақсаттарда заманауи технологиялар қолданылған көптеген көрнекті оқиғаларды зерттейді. Бұл мақалада киберқауіпсіздік пен цифрлық криминалистикадағы ең соңғы жетістіктерді талдай отырып, осы мәселені шешуге арналған дауысты еліктеу алаяқтықты анықтау және алдын алуда кездесетін қиындықтар зерттеледі. Бұл күшті қорғау жоспарларын құрудың маңыздылығын және жылдам дамып келе жатқан технологиялардан хабардар болу үшін үздіксіз оқу қажеттілігін көрсетеді. Сонымен қатар, зерттеу дауыс синтезі технологияларын пайдалануда нақты анықталған нормалар мен этикалық принциптердің қажеттілігін атап көрсете отырып, дауыс имитациясының этикалық және құқықтық салдарын талқылайды. Аннотация мақаланың қауіп-қатерлерді түсінуге, жағдайларды анықтауға және дауыс еліктеу алаяқтықпен күресудің тиімді тактикасын қалыптастыруға арналған негізгі екпінін жинақтайды.

Түйін сөздер: DeepFake технологиясы, нақты уақыттағы дауысты клондау (RVC), биометриялық аутентификация, дауысты тану технологиясы, алаяқтықтағы жасанды интеллект (AI), дауысты синтездеудің кеңейтілген әдістері

Дәйексөздер үшін: П.С. Пустовойтов, Н.А. Сейлова, А.С. Гнатюк. ДАУЫС ЖАЛҒАН ӘДІСТЕРІН ТАЛДАУ: ТӘУЕКЕЛДЕР, ЖАҒДАЙЛАР ЖӘНЕ ҚОРҒАУ СТРА-ТЕ ГИЯЛАРЫ//ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОМ МУНИКАЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ. 2024. Т. 5. No. 17. 120–134 бет. (ағылшын тілінде). https://doi.org/*10.54309/IJICT.2024.17.1.010*.

АНАЛИЗ МЕТОДОВ ПОДДЕЛКИ ГОЛОСА: РИСКИ, СЛУЧАИ И СТРАТЕГИИ ЗАЩИТЫ

П.С. Пустовойтов[1*], Н.А. Сейлова[1], А.С. Гнатюк[2]
Международный университет информационных технологий, Алматы, Казахстан.
E-mail: *36060@iitu.edu.kz*

Пустовойтов Павел — магистрант, Международный университет информационных технологий, Алматы, Казахстан
E-mail: *36060@iitu.edu.kz.* ORCID: 0009-0004-9188-2578;
Сейлова Нургуль Абадулаевна — к.т.н., ассоциированный профессор кафедры компьютерная инженерия, Международный университет информационных технологий, Алматы, Казахстан
E-mail: nseilova@iitu.edu.kz. ORCID: 0000-0003-3827-179X.
А.С. Гнатюк — доктор технических наук, профессор Национальный авиационный университет, Киев (Украина)

Аннотация. В работе представлен анализ растущей угрозы мошенничества с выдачей себя за другое лицо в эпоху цифровых технологий. Прогресс, достигнутый в таких технологиях, как DeepFake и клонирование голоса в реальном времени (RVC) сделал голосовое олицетворение не только возможным, но и более убедительным и легко доступным. В исследовании рассматриваются известные инциденты, в которых современные технологии использовались в мошеннических целях и подчеркивается серьезность и потенциальные последствия этих преступлений. В работе исследуются трудности, возникающие при выявлении и пресечении мошенничества с использованием имитации голоса, анализируются последние достижения в области кибербезопасности и цифровой криминалистики, предназначенные для решения этой проблемы. Авторы подчеркивают важность создания надежных оборонных планов и необходимость постоянных исследований, чтобы идти в ногу с быстро развивающимися технологиями. В исследовании также обсуждаются этические и правовые последствия подражания голосу, подчеркивается необходимость определения четких норм и этических принципов при использовании технологий синтеза голоса.

Ключевые слова: технология DeepFake, клонирование голоса в реальном времени (RVC), биометрическая аутентификация, технология распознавания голо са, искусственный интеллект (ИИ) в мошенничестве, передовые методы синтеза голоса

Для цитирования: П.С. Пустовойтов, Н.А. Сейлова, А.С. Гнатюк. АНАЛИЗ МЕТО-ДОВ ПОДДЕЛКИ ГОЛОСА: РИСКИ, СЛУЧАИ И СТРАТЕГИИ ЗАЩИТЫ//МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУ НИКА-ЦИОННЫХ ТЕХНОЛОГИЙ. 2024. Т. 5. No. 17. Стр. 120–134. (На анг.). https://doi. org/*10.54309/IJICT.2024.17.1.010*.

Introduction

The swift advancement of speech synthesis technologies, such as DeepFake and real-time voice cloning (RVC), has introduced a new era of digital communication

capabilities. Nevertheless, technology has also spawned a significant and escalating menace: identity fraud. The emergence of this phenomena, wherein advanced artificial intelligence algorithms can accurately replicate individuals' voices, presents significant concerns for personal safety, privacy, and overall cybersecurity protocols.

In this article, we delve into the world of impersonation fraud. We will examine technologies capable of replicating certain human voices with remarkable precision. Furthermore, it examines the ramifications of these technologies in both favorable and unfavorable circumstances. Although they provide creative solutions in fields like entertainment and accessibility for individuals with speech problems, their abuse for fraudulent intentions is a significant peril. This article analyzes multiple documented instances of voice impersonation fraud, emphasizing the simplicity with which perpetrators can exploit these technologies to engage in activities such as identity theft, financial fraud, and the dissemination of false information.

This article is to present a thorough examination of voice impersonation fraud, encompassing extensive research on dangers, real-life instances, and emerging defense techniques. Its objective is to offer a comprehensive picture of the landscape of this fraudulent activity, its societal repercussions, and the ongoing endeavors to counteract this intricate form of fraud. Cybercrime.

Risks of Biometric Data Leakage: Dangers and Implications

In the contemporary day, when technology assumes a progressively significant role in our everyday existence, the widespread adoption of collecting, storing, and utilizing biometric data has been prevalent. Biometric data include data pertaining to an individual's physiological and biological characteristics, such as fingerprints, facial traits, iris patterns, and vocal characteristics. These data serve as crucial tools in the field of security and convenience, as they are utilized for biometric authentication and identification. Nevertheless, the utilization of these capabilities also entails significant hazards linked to the disclosure of biometric data.

In Kazakhstan, biometric data is legally defined as "information pertaining to the physiological and biological characteristics of an individual that enables their identification and is utilized by an operator for this specific purpose. This data encompasses fingerprints, facial attributes, iris patterns, and other biological parameters."

Biometrics serve two primary purposes: biometric authentication (verification) and biometric identification. Biometric authentication entails confirming an individual's identity by analyzing their biometric data. For instance, unlocking a smartphone using a fingerprint or scanning a person's face to access a bank account. Conversely, biometric identification involves recognizing individuals based on their biometric data. Examples include timekeeping systems that utilize fingerprints or facial recognition systems employed in public transport. Biometrics have become an essential aspect of contemporary existence, yet their extensive application gives rise to significant concerns regarding privacy and security.

Examples of the use of biometrics in various fields emphasize the relevance of this topic:

1. Using DNA to determine appearance: Police in Australia are planning to use

Massively Parallel Sequencing (MPS) technology to predict a person's gender, eye colour and ancestry based on DNA. This raises questions about the privacy of biological data and its use without consent.

2. Facial recognition from online photos: Professional criminals and law enforcement agencies are actively using photos posted on the Internet for facial recognition. This raises questions about the privacy and security of personal photographs.

The leakage of biometric data can have severe ramifications for individuals and society at large. An illustrative instance of such a breach is the Central Election Commission of Kazakhstan's loss of voter data in 2019. This incident impacted millions of Kazakhstani citizens, exposing their personal information, such as names, surnames, IINs, passport numbers, and addresses, to malicious entities. Consequently, this gave rise to potential risks concerning personal safety and potential fraudulent activities (Dana Buralkieva, 2022).

It is crucial to acknowledge that in such instances, the mere occurrence of a data leak, regardless of whether criminals utilized the data, may constitute a violation of human rights and necessitate legal recourse. Certain countries, such as those within the European Union, have established legislation and regulations to safeguard individuals' personal data and impose accountability for breaches of data security.

International evidence demonstrates that the unauthorized disclosure of biometric data constitutes a grave infringement upon both the fundamental rights of individuals and the security of citizens. A notable instance of this occurred in the United Kingdom, where a significant breach of Suprema data occurred, resulting in the exposure of the biometric information of over one million users. Consequently, those accountable, both individuals and organizations, faced severe consequences such as terminations and financial penalties.

Kazakhstan ought to draw lessons from the errors made by other nations and implement measures to avert the unauthorized disclosure of biometric data. This entails formulating stringent legal standards and regulations that oversee the acquisition, retention, and utilization of said data, as well as mandating training and awareness programs for the populace.

Material and Methods

Analysis of voice impersonation cases

In the modern era of digitalization, where information holds significant importance, voice has emerged as a crucial component of communication and identification. However, technological advancements have given rise to novel risks associated with voice spoofing. "Deepfake" technology enables the fabrication of remarkably authentic video and audio counterfeits, including voice spoofing, wherein the visages of public figures and renowned individuals can be employed to create implausible situations and utterances. This technology gives rise to grave concerns regarding the dissemination of misinformation and the misuse of information. Presented below are notable instances of voice spoofing that have impacted well-known personalities.

Fake Mark Zuckerberg video:

In 2019, a video surfaced depicting Facebook CEO, Mark Zuckerberg, endorsing

the regulation of user data and asserting his influence over the future. This video was generated using Deepfake technology and was so convincing that numerous social media users mistook it for genuine (Queenie Wong, 2019).

Barack Obama's Fake Speech:

Another notable instance of a Deepfake video involved the manipulated speech of former US President Barack Obama. This video, which was shared on social media, depicted Obama uttering inappropriate and scandalous remarks. The video was produced with the intention of spreading false information and generated significant fervor and discourse in both the media and society (Vincent, 2018).

An artificially manipulated audio tape featuring the voice of Vladimir Putin:

In 2020, a highly authentic audio tape started spreading on social media, allegedly featuring Russian President Vladimir Putin confessing to Russian involvement in the 2016 US election. The recording exhibited remarkable realism and said that Putin was affirming Russian influence in the election (Hao, 2020).

The audio recording immediately aroused skepticism, prompting extensive scrutiny from experts and journalists to ascertain its veracity. Evaluations of the vocal characteristics and linguistic style of the statement led to the determination that the recording was likely counterfeit. Subsequently, it was officially confirmed that the audio recording featuring Vladimir Putin was indeed a forgery. Credible sources, including Kremlin representatives, refuted its authenticity, and a subsequent investigation uncovered that it was a product of Deepfake technology.

Advertisement featuring Scarlett Johansson:

Scarlett Johansson, an actress, has filed a lawsuit against the producers of Lisa AI: 90's Yearbook & Avatar, an app that utilizes artificial intelligence. As reported by Variety, Johansson alleges that the developers unlawfully employed her name and likeness in the product's web advertisements without obtaining her consent.

A promotional video lasting 22 seconds was shared on the social media page of the application. The film utilized authentic footage of Johansson taken during the production of Marvel's Black Widow, which was repurposed by a neural network. Johansson explicitly said that she was not involved in the creation of the video and did not provide approval for the utilization of her photos or voice.

According to Johansson's attorney, Kevin Yorn, they will take all necessary measures to defend her legally. The promotional post was pulled down once the complaint was initiated, while the app remains accessible on both the App Store and Google Play.

Tom Hanks likewise encountered a comparable issue when his likeness was utilized for promotional purposes without his authorization, mirroring a previous incident (Roth, 2023).

Unauthorized disclosure and improper handling of Alyona Andronova's records:

Voice actress Alyona Andronova has filed a lawsuit against Tinkoff Bank, alleging that her recorded voice, originally intended for training the bank's voice assistant, was utilized without her consent for other projects. The incident dates to 2019, when Andronova initially agreed to record text for the purpose of developing a neural network specifically for the bank's internal operations.

During the initial recording session, the actress was informed that her voice would be solely utilized within the bank for the purpose of training a voice assistant for the call center. However, after a few years, she became aware that her voice was being employed in advertisements and other questionable endeavors without her consent.

The actress explicitly stated that her contract with the bank did not include any references to fusion or neural networks. She also expressed that her attempts to communicate with the bank's legal representatives were unsuccessful, and that the compensation offered by the bank did not meet her expectations.

Tinkoff Bank refutes the accusations and asserts that they possess complete legal authority to utilize the actress's voice in accordance with the contractual agreement. Furthermore, they emphasize that the synthesized voices are employed for the purpose of automating call centers and other corporate operations.

The issue has sparked significant public outrage, leading to the creation of a petition on Change.org in support of Andronova. The petition calls for the legal acknowledgment of the human voice as an intangible commodity, safeguarded against unauthorized use without explicit authorization.

This text examines multiple instances of voice spoofing and highlights the significance of public vigilance and awareness regarding emerging technological risks. It also addresses ethical and security concerns in the era of digital advancements. Enhancing techniques for identifying and protecting against voice spoofing is an urgent task to establish robust safeguards against potential abuse and uphold confidence in voice identification.

Analysing voice impersonation tools

The world has recently experienced a wave of fraud using an innovative technology called Voice DeepFake. This technology involves manipulating audio recordings to create fake speeches. By using specialized software, it is possible to generate a speech using the recorded voice of a specific individual. The software can accurately replicate the tone and quality of the victim's voice by analyzing the speech into phonemes or short sounds, which are then combined to form new sentences. Any errors or inaccuracies in the playback are typically attributed to external noise or low communication quality.

The utilization of this technology is currently prevalent among criminals worldwide, and the identification of such fraudulent activities is becoming equally as difficult as uncovering a deceitful plot within a financial institution. As an illustration, you might receive a phone call from an individual claiming to be a "family member" with a familiar voice, persuading you to transfer money to assist them.

The researchers from the Security Algorithms, Networks and Data (SAND) Lab at the University of Chicago conducted a test on Voice DeepFake programs found on the open-source developer platform GitHub. Their objective was to determine whether these programs could bypass the voice recognition systems employed by Amazon Alexa, WeChat, and Microsoft Azure. Among these programs was SV2TTS (Figure 1), which, as claimed by its creators, can generate an accurate voice simulation with only five seconds of audio sampling (Wenger et al., 2021).

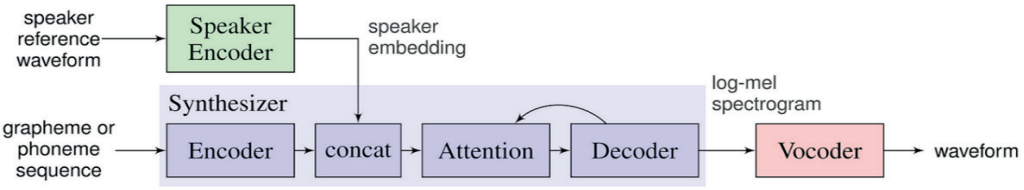

Figure 1 - The general SV2TTS architecture

SV2TTS, a voice cloning toolkit, has been found to successfully deceive Microsoft Azure systems approximately 30 % of the time. It is even more effective in bypassing WeChat and Amazon Alexa systems, with a success rate of 63%. The program has also proven to mislead individuals, as two hundred volunteers who were asked to differentiate between a real voice and an SV2TTS fake were fooled half of the time. Experts have discovered that DeepFake algorithms are particularly adept at imitating female voices and speech in all languages except English. The reasons behind this phenomenon remain unclear to researchers. These findings indicate that both humans and machines can be deceived by synthetic speech, and current defenses are inadequate. Consequently, criminals could potentially exploit modern voice clones to conduct various attacks on both individuals and software systems (Wenger et al., 2021).

It is important to acknowledge that voice clones are not suitable for widespread use or large-scale attacks. This technology is primarily designed for targeted attacks on specific individuals. The likelihood of unintentionally becoming a victim of a DeepFake voice clone is currently exceptionally low, particularly for private individuals. However, for certain individuals, particularly those who are wealthy and subject to systematic surveillance, such an attack could potentially occur.

It is crucial to acknowledge that technology has advanced, and the occurrence of such attacks is no longer a fictional plot. Governments are now taking action to combat the creation of clones. The United States has already enacted legislation to safeguard its citizens from deceptive representations of their identity, which governs the use of manipulated videos. Similarly, California has implemented a law that makes it a crime to employ uncoordinated visual and audio clones for advertising and political purposes. The problem of manipulated videos has also spurred the emergence of a new field of study - the creation of digital forgery detection systems.

When discussing technologies associated with voice spoofing, there are three primary components: speech generation, speech synthesis, and voice cloning. We have previously examined speech generation and synthesis using SV2TTS (Speaker Verification to Text-to-Speech) technology. However, it is equally important to consider another technology called RVC (Real-Time Voice Cloning).

Let us go from SV2TTS to RVC:

SV2TTS has the capability to generate voice assistants, personal assistants, and audio content of superior quality. Nevertheless, like with any potent technology, it may be misused. The utilization of SV2TTS for voice spoofing can pose significant risks, including fraud, social engineering, and the dissemination of misinformation.

Real-Time Voice Cloning (RVC) is an advanced technology that utilizes neural networks and deep learning to accurately replicate a person's voice. By capturing a brief audio sample of the target individual's voice, RVC can generate text that will be spoken in a voice that closely resembles the original. RVC enables the creation of highly authentic voice replicas that are challenging to differentiate from the genuine voice.

Multiple methods and instruments exist for voice replication utilizing RVC:

1. Voice model training involves recording a substantial amount of audio data from the target subject. This data is then utilized to train a neural network that captures the distinctive characteristics of the voice.

2. Generating a vocal model: Following the training of the neural network, a vocal model is produced, which may be stored and utilized for the purpose of speech synthesis.

3. Voice synthesis and spoofing involve the creation of artificial voices that can be used to generate voice messages, audio files, and even mimic actual speech. This technology allows for the possibility of misuse, such as engaging in deceit and fraud.

It is crucial to acknowledge that RVC has diverse applications, including benign ones like generating synthetic voice actors or assistants. However, concerning dangers and voice spoofing, this technology represents significant risks of misuse and infringement on privacy.

To address the risks posed by voice cloning through RVCs, it is necessary to implement more stringent laws, advance voice authentication and verification systems, and enhance overall information literacy in society. It is crucial to acknowledge that the emergence of voice spoofing technologies necessitates measures to safeguard personal data and ensure online security.

The emergence of advanced technologies like SV2TTS (Speaker Verification to Text-to-Speech) and RVC (Real-Time Voice Cloning) has significantly elevated the complexity and risk associated with voice impersonation fraud. These tools empower criminals to generate highly authentic counterfeit voices, enabling them to execute criminal activities. Now, let us examine the various methods and instances of fraud that involve voice impersonation:

Fraudsters can employ voice cloning (RVC) to replicate the voices of acquaintances, such as family, friends, or coworkers. These counterfeit voices can then be utilized for the purpose of deceiving others and obtaining monetary advantages. Deceptive phone calls from financial institutions and establishments: Fraudsters may contact individuals, assuming the identity of bank personnel, government entities, or other esteemed organizations. Employing a fabricated tone, they may solicit personal information, passwords, or even execute financial transactions in the name of the victims.

Social Engineering: Scammers can employ counterfeit voices to execute social engineering schemes. They can persuade targets to conduct specific acts, such as money transfers or divulging confidential information, by placing trust in a fabricated voice.

Through the utilization of RVC (Real-Time Voice Cloning) and SV2TTS (Speaker Verification to Text-to-Speech) technologies, malicious individuals can generate extensive audio recordings and voice messages with the intention of disseminating misinformation and propagating falsehoods to vast audiences.

These cases of fraud, highlight the seriousness of the problem of vote fraud:

1. In 2019, individuals engaged in fraudulent activities employed voice deepfake technology to deceive a UK energy company into transferring a substantial amount of money to a non-existent corporate account. By artificially generating the voice of a senior staff member, they effectively executed the fraudulent scheme.

2. In 2020, perpetrators utilized speech deepfakes to illicitly appropriate millions of dollars from a Japanese corporation. Specifically, a counterfeit vocal representation was employed to perpetrate financial deception and facilitate the transfer of funds to the criminals' accounts.

The prevalence and complexity of voice impersonation fraud are on the rise. Experts and legislators are urging caution and implementing measures to counter this menace, such as enacting legal frameworks to regulate the use of technology and providing public education on safeguarding against voice impersonation fraud.

Result and Discussion

Defense Methods

Amidst the significance of information security, emerging fraudulent technologies can endanger personal data and financial resources. Nevertheless, countermeasures against these risks are advancing alongside the evolution of voice forgery technologies. The most recent advancement in this domain is the AntiFake algorithm, devised by American scientist Ning Zhang (Ogliore, 2023).

The AntiFake algorithm aims to increase the difficulty of producing persuasive deepfakes. It utilizes an adversarial artificial intelligence (AI) technique, previously employed by cybercriminals, to counteract their activities. The algorithm intentionally distorts the captured audio signal, rendering it understandable to humans while becoming incomprehensible to the AI. Consequently, the synthesized voice of the AI becomes distinct from the human voice in the original sample.

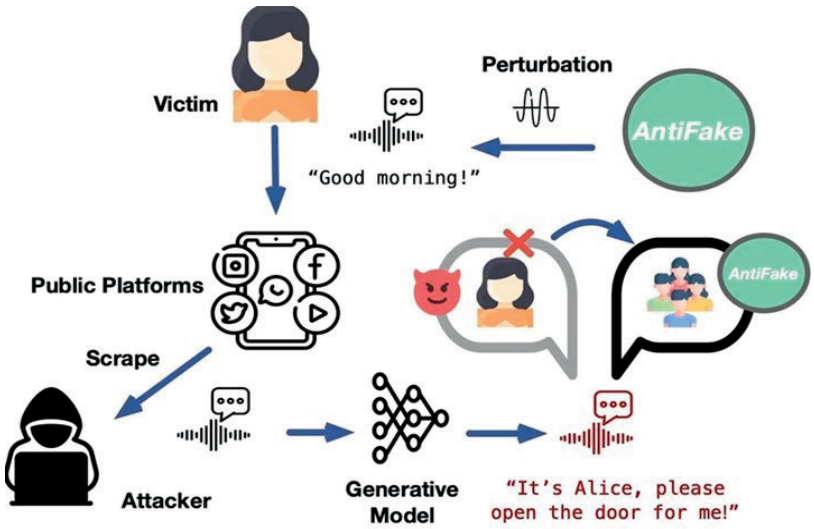

Figure 2 - Overview of how AntiFake works

Evaluations have demonstrated the considerable efficacy of the AntiFake algorithm. It successfully thwarts the production of persuasive deepfakes by an impressive 95%. Consequently, any attempts to fabricate a deepfake using an altered recording would result in an AI-generated voice that appears untrustworthy and unconvincing.

With the continuous advancement of voice authentication and voice spoofing technologies, there is a constant emergence of new tools and features. However, the effectiveness of countering fraudsters can still be achieved by employing strategies that are specifically designed for this purpose. AntiFake technology serves as evidence that modern developments can effectively safeguard against information security threats and mitigate fraud associated with voice spoofing.

In the dynamic realm of technology and information risks, ensuring security and safeguarding identities are crucial hurdles. Advanced solutions like AntiFake can enhance voice authentication and deter fraudulent activities. Furthermore, it is imperative to establish legislation and regulations to govern voice authentication and identification, thereby fostering a more secure and dependable digital environment.

In addition to utilizing algorithms such as AntiFake, there exist several techniques and strategies to enhance the security of voice authentication:

1. Multiparameter authentication refers to the process of assessing multiple biometric data, including voice, fingerprints, and retinal scans, to enhance security. By requiring attackers to mimic many biometrics, this method makes spoofing more challenging.

2. Implementing multi-factor authentication involves incorporating various authentication factors, including but not limited to biometrics, passwords, pin codes, or one-time codes.

3. Access Control: The integration of voice authentication systems with access control methods is necessary to limit access to sensitive data exclusively to authorized individuals.

4. Technological Advancement: Consistent updates to voice authentication algorithms and systems can enhance their resilience against emerging attack methods and fraudulent activities.

Conclusion

To summarize, voice impersonation fraud, as described in "Voice Impersonation Fraud: Risks, Cases, and Defense Strategies," is a major and constantly changing issue in the field of digital security and personal privacy. The progress made in DeepFake and Real-Time Voice Cloning (RVC) technologies, although providing exciting possibilities for innovation and imagination, also present a significant danger when exploited for malicious purposes.

The article highlights the importance of addressing voice impersonation fraud by examining several prominent cases. It is evident that conventional cybersecurity measures are inadequate in dealing with the complexity of voice synthesis technologies. Therefore, there is an immediate requirement for the creation of more advanced detection tools, stronger legal frameworks, and greater public awareness to effectively combat this type of fraud.

Furthermore, it is of utmost importance to emphasize the ethical and legal implications

associated with the utilization of voice impersonation technologies. The article underscores the need to establish explicit ethical principles and rigorous legislation to regulate the application of these technologies, guaranteeing their responsible use while respecting the privacy and consent of individuals.

To effectively combat voice impersonation fraud, it is essential to establish a cooperative endeavor involving technology developers, legal specialists, cybersecurity experts, and the general population. By remaining well-informed, watchful, and initiative-taking in devising and executing comprehensive strategies, we can reduce the dangers associated with voice impersonation fraud and protect the authenticity of our digital communications in this constantly changing technological environment.

ЛИТЕРАТУРА

Венгер Э., Бронкерс М., Чианфарани К., Криан Дж., Ша А., Чжэн Х. и Чжао Б.Й. (2021, 12 ноября). "Hello, It's Me": Атаки на синтез речи на основе глубокого обучения в реальном мире. Материалы 2021 конференции ACM SIGSAC по компьютерной и коммуникационной безопасности. — *https://doi.org/10.1145/3460120.3484742*

Дана Б. (2022, December 8). Сбор биометрических данных: с какими рисками могут столкнуться казахстанцы? - CABAR.asia. CABAR.asia. — *https://cabar.asia/ru/sbor-biometricheskih-dannyh-s-kakimi-riskami-mogut-stolknutsya-kazahstantsy*

Roth E. (2023, 1 Ноября). Скарлетт Йоханссон подала в суд на приложение искусственного интеллекта за клонирование ее голоса в рекламе. The Verge. — *https://www.theverge.com/2023/11/1/23942557/scarlett-johansson-ai-app-developers-lawsuit*

Hao K. (2020, September 29). Deepfake Putin is here to warn Americans about their self-inflicted doom. MIT Technology Review. — *https://www.technologyreview.com/2020/09/29/1009098/ai-deepfake-putin-kim-jong-un-us-election/*

Queenie W. (2019, June 12) Deepfake video of Facebook CEO Mark Zuckerberg posted on Instagram. CNET. — *https://www.cnet.com/tech/tech-industry/deepfake-video-of-facebook-ceo-mark-zuckerberg-posted-on-instagram/*

Оглиоре Т. (2023, 27 Ноября). Защита вашего голоса от подделки - The Source - Washington University in St. Louis. The Source. — *https://source.wustl.edu/2023/11/defending-your-voice-against-deepfakes/*

Vincent J. (2018, April 17). Watch Jordan Peele use AI to make Barack Obama deliver a PSA about fake news. The Verge. — *https://www.theverge.com/tldr/2018/4/17/17247334/ai-fake-news-video-barack-obama-jordan-peele-buzzfeed*

REFERENCES

Dana B. (2022, December 8). Biometric data collection: what risks might Kazakhstanis face? - CABAR.asia. CABAR.asia. — *https://cabar.asia/en/biometric-data-collection-what-risks-might-kazakhstanis-face*

Roth E. (2023, November 1). Scarlett Johansson hits AI app with legal action for cloning her voice in an ad. The Verge. — https://www.theverge.com/2023/11/1/23942557/scarlett-johansson-ai-app-developers-lawsuit

Hao K. (2020, September 29). Deepfake Putin is here to warn Americans about their self-inflicted doom. MIT Technology Review. — https://www.technologyreview.com/2020/09/29/1009098/ai-deepfake-putin-kim-jong-un-us-election/

Queenie W. (2019, June 12) Deepfake video of Facebook CEO Mark Zuckerberg posted on Instagram. CNET. — https://www.cnet.com/tech/tech-industry/deepfake-video-of-facebook-ceo-mark-zuckerberg-posted-on-instagram/

Ogliore T. (2023, November 27). Defending your voice against deepfakes - The Source - Washington University in St. Louis. The Source. — https://source.wustl.edu/2023/11/defending-your-voice-against-deepfakes/

Vincent J. (2018, April 17). Watch Jordan Peele use AI to make Barack Obama deliver a PSA about fake news. The Verge. — *https://www.theverge.com/tldr/2018/4/17/17247334/ai-fake-news-video-barack-obama-jordan-peele-buzzfeed*

Wenger E., Bronckers M., Cianfarani C., Cryan J., Sha A., Zheng H. & Zhao B.Y. (2021, November 12). "Hello, It's Me": Deep Learning-based Speech Synthesis Attacks in the Real World. Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security. — https://doi.org/10.1145/3460120.3484742

ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ

МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

Правила оформления статьи для публикации в журнале на сайте:
https://journal.iitu.edu.kz
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Собственник: АО «Международный университет информационных технологий» (Казахстан, Алматы)

ОТВЕТСТВЕННЫЙ РЕДАКТОР
Раушан Жалиқызы

КОМПЬЮТЕРНАЯ ВЕРСТКА
Жадыранова Гульнур Даутбековна

Подписано в печать 15.03.2024.
Формат 60x881/8. Бумага офсетная. Печать - ризограф. 9,0 п.л. Тираж 100
050040 г. Алматы, ул. Манаса 34/1, каб. 709, тел: +7 (727) 244-51-09).

Издание Международного университета информационных технологий
Издательский центр КБТУ, Алматы, ул. Толе би, 59