International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 9 Issue 3, May-Jun 2025 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Biometrics in Media and Entertainment

Matthew N. O. Sadiku[1], Paul A. Adekunte[2], Janet O. Sadiku[3]

[1]Roy G. Perry College of Engineering, Prairie View A&M University, Prairie View, TX, USA
[2]International Institute of Professional Security, Lagos, Nigeria
[3]Juliana King University, Houston, TX, USA

ABSTRACT

Biometrics, like fingerprints, facial recognition, and retinal scans, are increasingly used in the media and entertainment industry for a variety of purposes, including enhancing security, streamlining user experiences, and personalizing content. With biometric technologies, media organizations can enhance authentication, verification, and identification processes, thereby ensuring the integrity and reliability of information disseminated through digital platforms. This paper examines various uses of biometrics in media and entertainment.

KEYWORDS: *biometrics, media and entertainment (M&E), M&E industry*

How to cite this paper: Matthew N. O. Sadiku | Paul A. Adekunte | Janet O. Sadiku "Biometrics in Media and Entertainment" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-9 | Issue-3, June 2025, pp.885-892, URL: www.ijtsrd.com/papers/ijtsrd81167.pdf

IJTSRD81167

Copyright © 2025 by author (s) and International Journal of Trend in Scientific Research and Development Journal. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0) (http://creativecommons.org/licenses/by/4.0)

INTRODUCTION

Hollywood produces great entertainment. The United States media and entertainment (M&E) industry is a $703 billion market, comprised of businesses that produce and distribute motion pictures, television programs and commercials, streaming content, music and audio recordings, broadcast, radio, book publishing, video games and supplementary services and products. The M&E industry can be partitioned into four main verticals: film, music, book publishing and video games, as illustrated in Figure 1 [1]. The M&E industry is large and varied, constantly under pressure to innovate and explore emerging technologies for the potential impact on development.

Biometrics refer to the unique physical characteristics of a person, which could include fingerprints or facial recognition information. They offer solutions for identity verification, access control, and even personalization of content. For example, Apple's current range of devices use biometric authentication for easier device access.

Biometric technology involves the use of physiological or behavioral characteristics, such as fingerprints, facial recognition, iris scans, voice recognition, or DNA, to identify individuals. Biometrics are playing a growing role not only in the real-time policing and securing of increasingly crowded and varied venues worldwide, but also in ensuring a smooth, enjoyable experience for the citizens who visit them.

WHAT IS BIOMETRICS?

Any banking customer has used a password or a PIN code at least once. However, these traditional methods of verification are steadily giving way to the next generation of authorization tools. Passwords, codes, PINs, and safety questions have shown to be less dependable when used against modern cybersecurity threats. The financial sector is shifting towards safer, more customer-friendly verification. Biometric authentication has arisen as an answer to the outdated and more easily compromised traditional techniques.

Biometrics is the utilization of unique biological traits for identification. It is a technology powered method of personal identification that leverages unique biological patterns on and in human body. It is based on one-of-a-kind biological characteristics of a client,

which include fingerprints, facial traits, and more. It is a fast-developing field that utilizes users' unique biological characteristics, like fingerprints, facial features, iris patterns, or even voice, to identify and verify the users. This technology is poised to become just as common in the world of financial transactions, where convenience is key and security is paramount. It offers a significant leap forward compared to traditional passwords and PINs. It promises a future of banking that is not only exceptionally secure but also remarkably convenient and personalized. Figure 2 shows a representation of biometrics [2].

Biometric payments date to ancient civilizations, in which physical traits such as handprints and facial features were used for identification. Modern biometrics emerged in the 1800s and biometric payment systems began to gain traction in the early 2000s, when Pay By Touch introduced one of the first fingerprint-based payment systems. By the 2020s, biometric technology has become widespread and is integrated into smartphones for a variety of applications including payment authentication. Today, biometric payments are more popular and widely adopted than ever.

Biometric authentication employs cutting-edge technology to capture and analyze various biological attributes. Two main hardware setups allow biometric payments to work. The first uses the built-in hardware on a customer's smartphone or smart device, such as a fingerprint scanner or facial recognition, to authenticate their identity. The second scenario uses dedicated payment system hardware to verify a person using biometrics. When a user attempts to access a financial service, such as logging into an online banking account or making a transaction, the system prompts them to provide a biometric sample. This sample is compared against the stored biometric template for that individual. Access is granted if there is a match; if not, the system denies access.

TYPES OF BIOMETRICS

Biometrics in financial digital services concerns the protection of users' financial and personal data and the conduct of financial transactions. The different types of biometric payments include [3]:

- *Fingerprint Recognition:* A fingerprint biometric is a representation of multiple points on the fingerprint, and the relative positions of those points. Fingerprint recognition is the most common form of biometric payment. It involves scanning and matching the unique patterns on a person's fingertip or fingertips to authenticate their identity and authorize a transaction. Fingerprint biometrics in finance offer several benefits to financial institutions and their customers. Figure 3 shows fingerprint biometrics [4].
- *Facial Recognition:* This technology works similarly to how our eyes and brains identify people. First popularized by Apple's Face ID, this method is quickly catching up to fingerprint recognition in popularity. It works by using infrared light to scan a person's face and pinpoint thousands of dots that make up their unique facial structure. The traits are transformed into a template for subsequent authorization. If the features are nearly identical, the admission is authorized. With face recognition technology, computer vision is used to create a biometric template of a user's face, measuring unvarying characteristics such as the distance between the eyes and the length of the nose. Figure 4 shows facial recognition [5].
- *Retina Recognition:* This is also known as eye scanning. Its essence is to check people based on the unique patterns found on their irises. By capturing the intricate patterns within the iris or retina, this method offers a high level of accuracy in authenticating users, and has long been trusted in high-security environments. A special camera captures the iris in high definition, and the resulting image is matched up with the pre-existing framework. If they are mostly identical, the client is allowed onto the application. Airports originally used iris scanning for security screening. However, it has now become part of banking security.
- *Voice Recognition:* This method is based on the vocal traits of users. The pitch of voice modulation, as well as speaking habits, help create a voiceprint for further verification. The method analyzes the nuances in speech patterns and voice characteristics, then compares this voiceprint to registered samples to certify a match.
- *Behavioral Recognition:* A client's behavior patterns have unique dynamics online, including typing rhythm, mouse/touchscreen use, speech, or walking. Unlike the other biometric authentication examples, this one takes into consideration the interaction with versatile systems and devices. A behavioral profile is established and then utilized for authorization. Behavioral recognition is non-disruptive and highly secure because of its resistance to forgery.
- *Vein Patterns:* Using near-infrared light and often centering on the palm or finger, this technology analyzes the pattern of visible blood vessels unique to each person.

- *Signature Recognition:* This somewhat less common process scans and digitizes a person's signature, then puts it through a shape-identifying algorithm to verify their identity.
- *Palm Recognition*: Similar to fingerprint scanning, this verification type relies on capturing the individual traits of the client's palm. It embraces patterns, ridges, loops, and other modalities. They are very precise and difficult to reproduce. Rich in detail and complex, these contribute to the successful identification.

Figure 5 shows some of these types of biometric authentication [6].

BIOMETRICS IN MEDIA AND ENTERTAINMENT

Biometrics encompass a variety of different technologies that use probabilistic matching to recognize a person based on their biometric characteristics. Biometric characteristics can be physiological features (for example, a person's fingerprint, iris, face or hand geometry), or behavioral attributes (such as a person's gait, signature, or keystroke pattern). The use of biometric technologies and systems is expanding significantly within the public and private sectors. Biometric technologies, such as facial recognition, voice, fingerprint or iris scanning technologies, are becoming cheaper, more advanced, and more accurate. As a result, they are becoming more integrated into people's daily lives, and in their interactions with government. Behavioral biometrics are increasingly being used for passive authentication, often as an additional layer of security.

APPLICATIONS OF BIOMETRICS IN MEDIA AND ENTERTAINMENT

Biometric technology has numerous applications in the entertainment industry, ranging from enhancing audience engagement to improving security and personalization. Common applications of biometric technology in media and entertainment include the following:

- *Live Events:* Biometrics are increasingly being adopted for use at sports and other live events. The technology is being used to enhance ticketing, credentialing, and sales of concessions, merchandise, and alcohol. Go-Ahead Entry, which links facial recognition with ticket accounts to make the process touchless, quick and secure, is just one example of how digital identity verification and blockchain-based ticketing are helping stadium operators enhance the fan experience. An example of a live event is shown in Figure 6 [7].
- *Personalization*: Biometric data can be used to tailor content recommendations, adjust settings, and even personalize the user experience in virtual environments. Biometric facial recognition technology is being used in the entertainment industry to personalize the user experience. For example, facial recognition technology can be used to identify a person and provide personalized recommendations for movies or music based on their interests and preferences. Personalizing the user experience using biometric technology involves using an individual's unique biometric data to tailor the content, services, or products they receive. As for personalized advertising, biometric data can also be used to personalize advertising based on an individual's interests and preferences. Figure 7 shows an example of personalization [7].
- *Biometric Authentication*: Social media apps may contain a lot of personal and sensitive data, which, if compromised, can have many negative impacts on a user. Securing this information is as important as securing an email account or an ecommerce account. Before the rise of biometric authentication, social media apps used password/PIN based authentication. Entering passwords on touch screen devices is hardly a user friendly experience, if users can recollect today's complex passwords at all. Biometric authentication on mobile devices has solved this problem and has improved the authentication process dramatically.

BENEFITS

Countries around the world are using biometrics to streamline entertainment. For example, London is using biometrics to streamline ticketing during sporting events. Many biometric parameters of a person may be used by modern technology for identifying people, but they vary in cost, speed, and accuracy of usage. Another benefit is that biometric characteristics cannot be as easily shared, lost, or duplicated as passwords or tokens. Other benefits of biometrics in media and entertainment include the following [8,9]:

- *Easy to Use:* Biometric technology is straightforward to use. While they are primarily found in high-security spots, like airports, hospitals, and similar, everyday items like smartphones, tablets, and laptops utilize biometrics. Both Android and iOS devices use different forms of biometric technology, such as fingerprint and facial scanning, which means users no longer have to type out a passcode to access their phones. Some financial and

messaging apps, too, use biometric technology to allow users to gain access instead of typing out their passwords. This makes the user experience surrounding biometric technology so much more appealing.

- *Easy to Integrate:* Many software applications use biometrics, and because it is available for use across multiple platforms, it is relatively easy to secure your accounts in just one tap. Those with smart homes will also appreciate how easy it is to integrate biometrics into several IoT devices at home.
- *Difficult to Fake:* Biometric technology is relatively hard to fake and spoof. While not impossible, facial patterns, irises, and fingerprints are difficult to replicate and could take more effort than necessary. While some phones can be unlocked with photos, consumer technology companies can prevent this by improving their technology in general. For example, most smartphones use 2D facial recognition scanning technology. Still, in the future, more smartphones might adopt 3D facial recognition instead to make it even harder for hackers to spoof things.
- *High-security Assurance*: Because biometrics rely on fingerprints, irises, and other unique human features; they can be a better option than passwords for protecting accounts. When paired with other forms of multi-factor authentication (MFA), you can also add another layer of security that is more difficult for others to hack. Because biometric authentication generally requires a living, breathing human to be present, it can be pretty tricky for AI or other forms of technology to spoof.
- *Security:* Biometrics help verify user identities, mitigating risks like impersonation and identity theft. This can be crucial for securing access to content, platforms, and events. Biometrics can also be used to enhance safety measures, such as monitoring crowd density or identifying individuals on watchlists.
- *Behavior:* Emotions drive behavior, despite what we think. Appetite for good content is fierce. Viewer attention spans are short and getting shorter. Audiences are consuming media across multiple channels. As media consumption increases, the brands that survive will be the ones that are able to forge stronger emotional connections.
- *Personalized Experiences:* One of the most powerful applications of facial recognition in media is its ability to deliver personalized experiences and targeted marketing campaigns. This allows content distributors to create more engaging and relevant experiences for their audiences.

CHALLENGES

Facial recognition is surrounded by tons of baggage. The use of facial recognition in the real world is fraught with concerns about misuse, particularly when in the hands of law enforcement. The use of biometric technology raises several legal issues that need to be carefully considered and addressed to ensure that individuals' rights are protected. The potential negative impacts of biometrics include privacy, security, as well as ethical norms. Cultural or religious factors may also limit a group or individual's ability to participate or enroll in a biometric system. Another limitation of biometric systems is that unlike passwords or ID tokens, biometric characteristics cannot be reissued or cancelled. Other challenges faced by biometrics in media and entertainment include the following [10,11]:

- *Costs:* To maintain and sustain a strong security profile, companies will have to spend significant money to ensure software and hardware are up to date. Beyond companies, biometric security can also be expensive for personal use. Prices for biometric access control systems like electronic doors and installation could cost upwards of 2,500 US dollars.
- *Ethical Concern:* Ensuring ethical use and fairness of biometrics necessitates mandatory periodic assessments of biometric algorithms for bias and discrimination, particularly in high-stake scenarios such as law enforcement and employment.
- *Governance:* This is another important element to consider when adopting and using biometrics; the oversight and accountability of systems is critical to ensuring they are used appropriately. Organizations using biometric systems should have transparent complaints and enquiry systems in place, and identify the appropriate internal and external avenues for redress, in case of misuse of biometric information or faults in the biometric system.
- *Legal Challenges:* As biometric technology is increasingly being used in various industries, including healthcare, banking, security, and law enforcement, there are several legal issues that arise in the collection, storage, and use of biometric data. With this expanding market for biometrics has come an abundance of legal

questions, as state laws are in flux. Some states have laws in place, while others are in the process of implementing laws. The lack of strict legislation and prominent use of biometrics in popular interfaces has led to several lawsuits involving user privacy. Statutes tend to prevent use of personal biometric data without consent.

- *Trust:* The issue of trust in media has generated a substantial body of research that has investigated the causes and effects of trust in media. The contemporary media landscape is grappling with a severe crisis characterized by the proliferation of misinformation, a decline in public trust, and the rampant spread of fake news, largely fueled by social media platforms. Biometric technology offers unique advantages in restoring trust in media. Biometrics, with its capabilities in identity verification, content authentication, mitigation of bots and Sybil attacks, and creation of personalized user experiences, offers unique advantages to restore trust, combat misinformation, and establish a secure online media ecosystem. The film industry in general is not recognized for its commitment to truth, and Hollywood's depiction of biometric technology is no exception.
- *Privacy:* The main concern of biometric information dissemination focuses on the protection of personal data. The abuse, tampering and leakage of personal and corporate data have triggered public concern about technical risks. Biometric data is highly personal and sensitive information, and therefore, the collection, storage, and use of such data may violate an individual's right to privacy. Many countries have enacted laws that regulate the use of biometric data and require companies to obtain individuals' consent before collecting their biometric information.
- *Data Security:* Protecting the security of biometric information is essential given its inherent and delicate nature. Biometric systems remain vulnerable at the perception, network, and application layers, posing a significant threat to the security of the Internet of things (IoT) and social networks. Biometric data can be hacked or stolen, just like any other personal data. Therefore, companies that collect and store biometric data need to take appropriate measures to secure such data from unauthorized access, disclosure, or misuse.
- *Data Quality:* This ensures that the personal information organizations hold is accurate, complete, and up to date. Data quality is particularly important at the enrolment stage, as the quality of a biometric sample will impact on the accuracy and effectiveness of the biometric system. For example, a low-quality biometric sample at the time of enrolment can increase the risk of false acceptance and false rejection in future presentations for authentication or identification. There are some factors that may affect the quality of a biometric sample, including low quality sensors or environmental conditions.
- *Perceived Risks*: Biometric technology pose risks as well as opportunities. Although biometrics offers some advantages for identity management, it is not a bullet-proof solution for fraud or identity theft. In the field of communication, perceived risks are included in our framework as an individual's subjective evaluation of potential negative outcomes or uncertainties associated with biometric technology services. Another privacy risk is the covert or passive collection of individuals' biometric information without their consent, participation, or knowledge.

CONCLUSION

Biometric identification is a signal for advancements we have yet to reach, and rather than think about the issues they could bring when deployed, we only focus on the optimistic possibilities. While biometric systems are becoming more effective as technology advances, they are not a foolproof method of authentication or identification.

Advancements in biometrics will likely open up even more opportunities for innovation in the entertainment industry. User adoption of biometrics is an increasing trend. More information on biometrics in media and entertainment can be found in the books in [12-15].

REFERENCES

[1] "Media and entertainment industry overview," https://investmentbank.com/media-and-entertainment-industry-overview/

[2] D. Orme, "The death of the PIN," https://internationaldirector.com/technology/the-death-of-the-pin/

[3] "Biometric payments: What are they and how are they shaping the future of commerce?" March 2024, https://www.payset.io/post/biometric-payments-how-are-they-shaping-the-future-of-commerce

[4] "Fingerprint biometrics in finance: Balancing security and convenience in a digital world," https://theenterpriseworld.com/how-fingerprint-biometrics-in-finance-work/

[5] "Face recognition," https://www.nec.com/en/global/solutions/biometrics/face/index.html

[6] "How biometrics in banking is redefining security and user experience?" April 2025 https://www.appventurez.com/biometrics-in-banking

[7] "Global live events industry focuses on biometrics in 2025," January 2025, https://www.pymnts.com/news/biometrics/2025/global-live-events-industry-focuses-biometrics/

[8] "The pros and cons of biometrics," June 2025, https://ceoworld.biz/2022/05/09/the-pros-and-cons-of-biometrics/

[9] S. Shilina, "Biometrics: A beacon of trust in the digital media crisis," April 2024, https://medium.com/@sshshln/biometrics-a-beacon-of-trust-in-the-digital-media-crisis-10f13ebe81d5

[10] F. Permata, "Biometric technology in the entertainment industry," March 2023, https://medium.com/@fapermata/biometric-technology-in-the-entertainment-industry-345b2777dd68

[11] "Biometrics and privacy – Issues and challenges," https://ovic.vic.gov.au/privacy/resources-for-organisations/biometrics-and-privacy-issues-and-challenges/

[12] W. Rodgers, *Biometric and Auditing Issues Addressed in a Throughput Model*. Information Age Publishing, 2011.

[13] K. Gates, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*. NYU Press, 2011.

[14] Information Resources Management Association (ed.), *Biometrics: Concepts, Methodologies, Tools, and Applications*. IGI Global, 2016.

[15] M. Gofman and S. Mitra (eds.), *Biometrics in a Data Driven World: Trends, Technologies, and Challenges*. Boca Raton, FL: CRC Press, 2016.

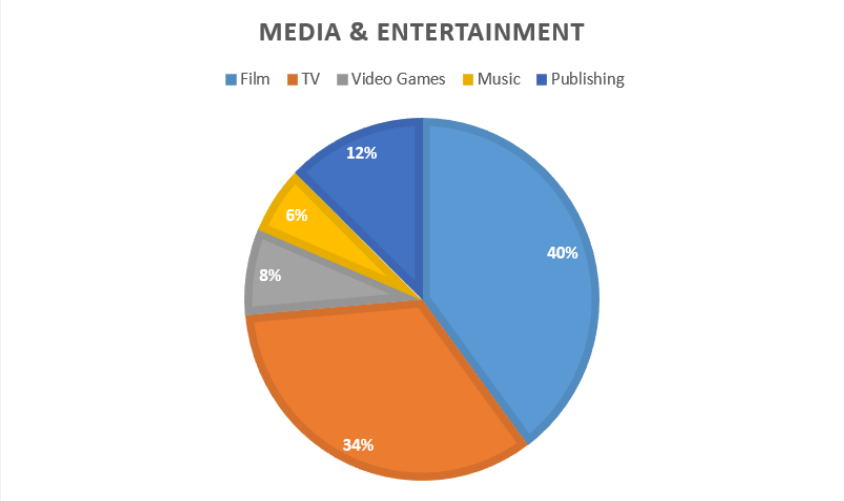

Figure 1 The media and entertainment industry [1].

Figure 2 A presentation of biometrics [2].

Figure 3 Fingerprint biometrics [4].

Figure 4 Facial recognition biometrics [5].

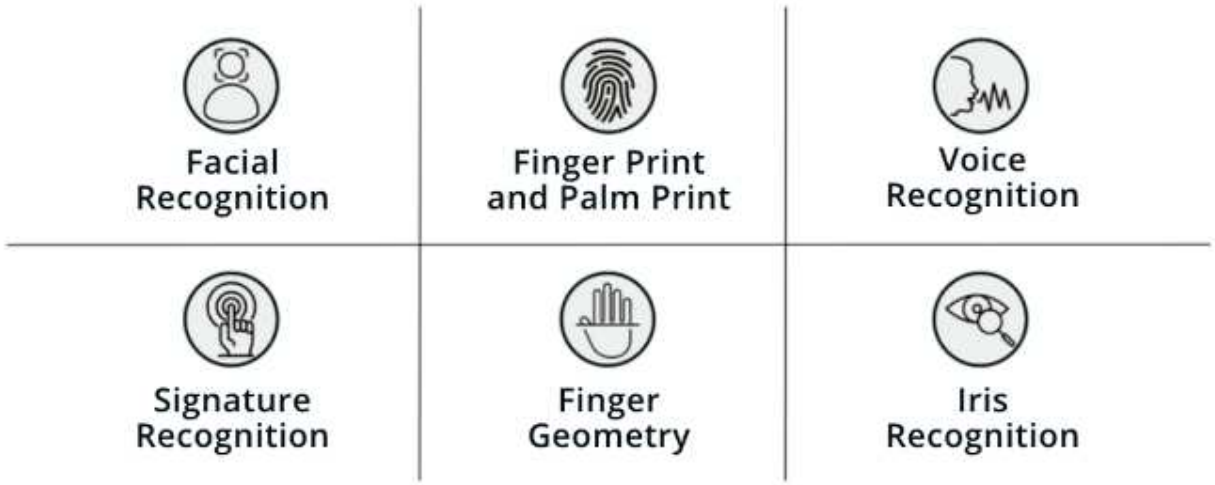

Figure 5 Types of biometric authentication [6].

Figure 6 A live event [7].

Figure 7 An example of personalization [7].