[1] Quiazon, Mark Cristian D.

[2] Manlutac, Bernard D.

[3] Besario, Voltaire M.

[4] Centeno, Criselle J.

[5] Casiw, Gaypelyn M.

Stream Shield: An Anti-Piracy Movie Streaming Android Application with Screen Recording Detection and Integrated Media Content Protection using Advance Encryption Standard (AES) Algorithm

Abstract: - In the context of movie streaming, unauthorized screen recording during playback poses a significant threat to the integrity of copyrighted content, leading to illicit distribution and negatively impacting both content creators and legitimate viewers. To combat these issues, "StreamShield," an anti-piracy movie streaming Android application, has been developed. This project focuses on integrating algorithms and technology to address screen recording detection and content protection while actively engaging users in the fight against piracy. The key features of the StreamShield application are designed to fortify content protection and enhance the user experience. The application itself incorporates an Anti-Screen Recording Mechanism, an Encrypted Media File system using the Advanced Encryption Standard (AES) algorithm, and a Picture Overlay Interference feature that adds an extra layer of complexity for illicit screen recording. By addressing these challenges, StreamShield not only redefines copyright enforcement but also empowers users to actively participate in safeguarding creative content. This project adheres to ISO-25010 guidelines, ensuring functionality, performance efficiency, reliability, and usability, thus contributing to a more secure and accountable digital entertainment ecosystem.

Keywords: Anti-piracy, Content Protection, Screen Recording Detection, Movie Streaming App

I. INTRODUCTION

In today's digital age, the entertainment industry has undergone a radical transformation, granting audiences unprecedented access to a vast array of content through online platforms. Yet, this convenience has also ushered in challenges related to intellectual property protection and copyright enforcement. A particularly pressing concern is the unauthorized reproduction, distribution, and dissemination of copyrighted movies via screen recording for which it can have negative effects on the movie industry itself. It is vital for industry management to comprehend the impact of digital platform availability on piracy demand since this knowledge will inform successful solutions. Comparably, information on how pirates react to legal availability helps policymakers create anti-piracy policies that are relevant and flexible enough to fight piracy in this changing environment. This understanding facilitates the creation of proactive strategies to counter new trends in piracy, guaranteeing the industry's continuous expansion and safeguarding intellectual property rights in the digital age [1].

The importance of *intellectual property (IP) rights* provides content creators with the legal framework to safeguard their innovative works from unauthorized use, give them incentives, provide legal exclusive rights and protecting their knowledge and technologies. Copyrighted content in the context of movies is subject to many forms of infringement, especially screen capturing during playing on various movie streaming services. It has become a growing concern in intellectual property rights, posing a significant global challenge for policymakers, businesses, and the global economy. Commonly cited reasons for its prevalence include the cost-effectiveness of pirated

[1,2,3,4] Pamantasan ng Lungsod ng Maynila

1quiazonmarkcristian@gmail.com, 2bernardmanlutac19@gmail.com, 3voltaire35b@gmail.com, 4centenocriselle21@gmail.com [5] Philippine College of Criminology, gaypelyn.casiw@pccr.edu.ph

material, minimal quality degradation, easy accessibility, and perceived inefficiencies in existing laws [2]. This conduct not only compromises the viewing experience of legal viewers, but it also encourages the spread of unauthorized copies via torrents and illicit streaming sites. As a result, methods must be established to preserve the value of intellectual work.

This study delves into these issues, proposing the creation of an encompassing system that not only detects and prevents these infringements but also actively involves users in the battle against piracy. This proposed system strives to redefine the landscape of copyright enforcement as it empowers users to play an active role in preserving the integrity of creative content, fostering a more secure and accountable digital entertainment ecosystem for present and future generations.

1.1 Objectives

The main objective of this study is to create a system application that addresses the issues arising from unauthorized reproduction and distribution of copyrighted movies. Specifically, the study aims to achieve the following objectives:

1. To develop an application with integrated *anti-screen recording mechanisms* that actively monitors video playback and swiftly identifying ongoing screen recording. Upon detection, it deploys strategic countermeasures to halt the recording process, preserving content exclusivity and integrity. This platform effectively shields against unauthorized screen capture, safeguarding sensitive data and proprietary information.

2. To implement a decryption logic using the *advanced encryption standard (AES) algorithm* within the streaming application that allows authorized users to watch the movie seamlessly while keeping the file encrypted on the user's device. The app will also have a feature that allows users to download specific movies for offline viewing. Once a movie is downloaded, users should be able to access and watch the movie even when they are not connected to the internet.

3. To integrate a *picture overlay interference* as an alternative for watermarking technology within the application. This approach involves superimposing visual elements onto movies through a randomized timing mechanism. This overlay introduces complexity that disrupts the screen recording process, presenting a formidable barrier to those seeking to illicitly capture the stream.

1.2 Motivation

In developing the StreamShield application, this study is driven by a clear motivation to address and resolve several critical challenges that the movie streaming industry is facing. The rampant infringement of copyright through screen recording poses a significant threat to the rights of content creators and distributors. The act of illicitly recording copyrighted movies during playback on various streaming platforms not only compromises the content's exclusivity but also affects the revenue established through legitimate channels. The proponents' motivation stems from the imperative need to devise effective mechanisms capable of detecting and preventing screen recording in real-time, assuring viewers a secure and exclusive watching experience.

1.3 Scope and Delimitations

The scope of this project, centered around the development of StreamShield, an Android application, aims to combat unauthorized distribution of copyrighted movies. The application will implement anti-screen recording mechanisms, deploy robust encryption using the Advanced Encryption Standard (AES) algorithm and incorporate a disruptive picture overlay feature during streaming. Additionally, the sample movies used in the application are retrieved from open source films available in the public domain for ethical and legal use.

This study also has certain delimitations. The application will be limited to the Android operating system, and development for other platforms, including iOS, is beyond the project's scope. While this project aims to detect and prevent screen recording, it may not be foolproof, and some screen recording methods may remain undetected. Lastly, this project assumes that users will have access to a stable internet connection for streaming and downloading content. Offline viewing will be supported for downloaded content.

1.4 Significance of the Study

This study aims to develop a system that prevents unauthorized distribution of copyrighted movies while engaging users in the ongoing effort to combat piracy.

This study is significant to the following:

1. *To content creators and distributors*, the system's foremost beneficiaries are movie creators and distributors who invest significant resources in producing and delivering high-quality cinematic content. By addressing the challenges of screen recording and unauthorized dissemination, the system enhances their ability to safeguard their intellectual property. This leads to increased confidence in the protection of their creative works, which in turn encourages continued innovation and investment in producing engaging movies.

2. *To the movie industry and revenue streams*, the proposed system mitigates the loss of revenue caused by unauthorized distribution and consumption of copyrighted movies. As the system actively prevents screen recording and unauthorized streaming, legitimate revenue channels are strengthened, fostering the growth and sustainability of the industry.

3. *To application users*, with piracy reduced, consumers can access high-quality content without concerns about compromised quality, potential security risks from pirated content, or encountering malicious websites during their search for entertainment. A piracy-free ecosystem enriches the user experience, ensuring the availability of diverse and engaging movies through legitimate channels.

4. *To future technology developers and researchers*, the study offers valuable insights for researchers and developers working on intellectual property protection mechanisms. The proposed anti-screen capture techniques, encryption mechanisms, and an alternative wise for watermarking contribute to the advancement of anti-piracy technologies, fostering a culture of continuous improvement in digital rights protection.

II. METHODOLOGY

2.1 Data Collection

The data collection process for this study employs a mixed methods approach, combining quantitative and qualitative techniques to gather comprehensive insights.

Quantitative Data Collection: Quantitative data will be collected through structured surveys. A survey questionnaire will be administered to a diverse sample of users who interact with the system, aiming to quantify user satisfaction, perceived effectiveness, and preferences.

Qualitative Data Collection: Qualitative data will be acquired through semi-structured interviews and open-ended survey questions. Open-ended survey questions will allow users to provide qualitative feedback on their experience, suggestions, potential improvements, and any issues they encountered while using the system.

2.2 Sampling Techniques

The sampling technique chosen for this study is convenience sampling, which involves selecting participants based on their easy accessibility and willingness to participate. In this approach, the study aims to gather data from a range of participants, focusing on those who have direct experience with movie streaming platforms and are willing to provide insights on the proposed anti-piracy application. A total of 30 respondents will be targeted for data collection.

2.3 Development

The methodology employed for the development of the Streamshield application is rooted in the Agile methodology. The adoption of agile project management is intricately tied to optimizing the development process, yielding benefits such as reduced errors, quicker delivery, enriched communication, elevated quality, enhanced risk assessment, and lowered expenses [3]. The methodology will be structured around six distinct phases: Plan, Design, Develop, Test, Release, and Feedback.

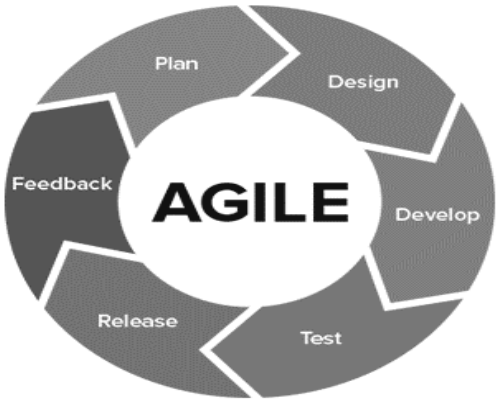

Fig. 1 Agile Methodology in System Development (Simsek, 2020)

2.3.1Plan

The planning phase for StreamShield's development establishes a solid foundation for the project. Through a collaborative project alignment meeting, the team ensures a shared vision and objectives. The core purpose of the application is clearly defined, focusing on preventing screen recording, securing media content, and adding barrier to the playback itself from any external method used for illicit capture. User requirements will be gathered through surveys and interviews, informing the creation of a detailed list of features and functionalities.

2.3.2Design

In this phase, the foundational elements of the StreamShield application are shaped, from its architecture, user interface, to its security measures. This also includes the technologies and algorithms to be used for the development such as in choosing programming languages, frameworks, and libraries. The overall system architecture, including components, databases, and APIs, is defined to establish a structured framework. Additionally, wireframes and prototypes are created to visualize and refine the application's interface. This phase serves as the blueprint for the development of the application, embodying critical choices in technology, user experience, and security measures such as AES encryption and screen recording prevention.

2.3.3Develop

In this phase, the application is constructed. encompassing both front-end and back-end components. This includes working of the Android application interface in alignment with the established UI/UX design. The phase also entails the integration of anti-screen recording mechanisms and the implementation of the overlay interference feature to enhance anti-piracy capabilities. Additionally, server-side components are built to facilitate user authentication, content management, and the encryption/decryption processes, ensuring a comprehensive and functional system.

2.3.3.1 System Architecture

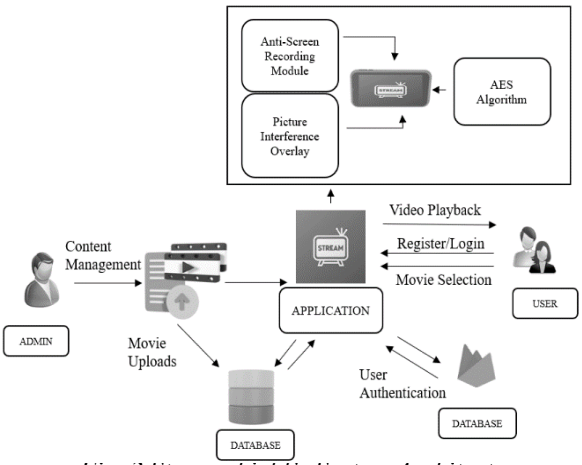

Fig. 2 Streamshield's System Architecture

Fig. 2 shows the system architecture of StreamShield showcasing the flow of data and processes within the application. The system starts with the Admin, who manages content within StreamShield. The Admin is responsible for uploading movies and related information, including metadata such as titles, synopsis, and cover art. This data is then transmitted to the StreamShield database for storage and retrieval. For users to access the StreamShield platform, they are required to register.

The User Registration process begins with users providing their account details, such as username, email, and password. These registration details are securely transmitted to Firebase. Firebase takes the lead in the user authentication process as it validates the user's registration information, ensuring the security and integrity of user accounts. After successfully logging in, users can interact with the StreamShield app. They are free to browse, select, and enjoy the movie content available in the app's library. During movie playback, StreamShield implements a range of features to protect the content and enhance the viewing experience: 1. While users engage with the movie content, StreamShield's Anti-Screen Recording Module is continuously active. If screen recording is detected, the system initiates countermeasures to prevent unauthorized copying of the content, ensuring the security and exclusivity of the viewing experience; 2. The Picture Interference Module introduces random visual overlays during movie playback. These overlays disrupt the screen recording process, making it challenging for individuals to capture content cleanly; 3. StreamShield utilizes the Advanced Encryption Standard (AES) algorithm to encrypt downloaded movie files. Users can download specific movies for offline viewing, with the files remaining encrypted until accessed through the app, safeguarding against unauthorized distribution.

2.3.3.2 Implementation of AES

The decision to employ AES (Advanced Encryption Standard) with a 128-bit key as the cornerstone of our security strategy stems from a meticulous evaluation of encryption standards. AES emerged as the natural choice due to its unparalleled cryptographic capabilities, effectively ensuring the impregnability of media files stored within the downloads section, accessible to users even in offline modes. This encryption protocol, specifically AES 128, has garnered widespread acclaim and adoption owing to its proven track record in fortifying diverse content types, ranging from plain text to multimedia, and audio against unauthorized access and tampering.

The shortcomings of its predecessor, DES (Data Encryption Standard), are the main cause of AES's rise to popularity. Though long regarded as very secure, DES eventually gave way to advances in computer power, leaving its 56-bit key susceptible to sophisticated assaults. As a result of these flaws and the growing demand for more robust encryption techniques, AES replaced DES in the field. The U.S. chose it as the industry-standard encryption algorithm. The National Institute of Standards and Technology (NIST) proved to be a reliable substitute, outperforming DES in terms of power and adaptability [4].

Our system's security goals are completely consistent with the robustness and dependability of AES-128 media files are guaranteed to remain intact even in cases of offline access. The solution strengthens data security and greatly reduces risks associated with illegal sharing and access across several devices by selecting AES 128-bit encryption. The deliberation approach is based on the purposeful use of AES, which is supported by its proven advantages over DES and its resilience to modern threats. As the main method of protecting sensitive data in our framework, AES 128-bit encryption has proven to be reliable and effective due to its strong ability to maintain data integrity and resistance to contemporary infiltration attempts.

Therefore, the purposeful choice of AES 128-bit encryption, based on its capacities exceeding DES and its unparalleled robustness, reinforces the security of media files that are stored and the overall integrity of our system, guaranteeing robust defense against unauthorized access or dissemination.

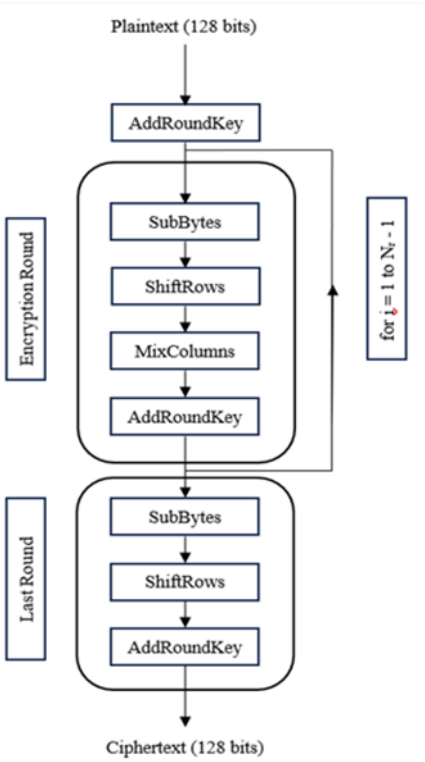

Fig. 3 General Process of AES 128-bit key

StreamShield offers a download section where users can view files that have been downloaded, encrypted using an AES 128-bit key. This algorithm comprises four transformation functions, Substitute Bytes, Shift Rows, Mix Columns, and Add Round Key. AES 128-bit key performs 10 rounds of encryption which in last round the Mix Columns transformation function is excluded. Our aim is to encrypt media files across StreamShield application users.

Each round comprises four transformation functions, except for the final round that excludes Mix Columns. Following Round 10, the output produced is ciphertext. This ciphertext is represented in hex format, enhancing security, and making it more challenging for intruders to decipher.

A. Substitute Bytes

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Fig. 4 Rijndael S-Box

Fig.4 shows that AES contains a grid of a 16x16 matrix of byte values. The Rijndael S-Box comprises all possible

values that can be substituted. This permutation is essential in determining the values of each block (8-bit) of the matrix.

29	9F	4C	2A
CE	A2	78	27
64	72	1E	8D
7C	9E	94	55

Fig. 5 Sample Index Values

The first value shown in *Fig.5* is X, and the second value is Y. These values are determined when X and Y intersect.

$S_{0,1} \rightarrow X, Y$

$S'_{0,0}$	$S'_{0,1}$	$S'_{0,2}$	$S'_{0,3}$
$S'_{1,0}$	$S'_{1,1}$	$S'_{1,2}$	$S'_{1,3}$
$S'_{2,0}$	$S'_{2,1}$	$S'_{2,2}$	$S'_{2,3}$
$S'_{3,0}$	$S'_{3,1}$	$S'_{3,2}$	$S'_{3,3}$

Fig. 6 Sample Mapping of S-Box

A5	DB	29	E5
8B	3A	BC	CC
43	40	72	5D
10	0B	22	FC

Fig. 7 Sample Values to Map in S-Box

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

Fig. 8 Values Based on S-Box

It starts from the top left, extending all the way to the right. Its direction is horizontal.

2.3.4Test

The testing phase is dedicated to validating the StreamShield application's functionality, performance, and user experience to meet established standards. It involves comprehensive unit testing for individual components to ensure their intended functionality. Additionally, the interactions between front-end and back-end components are thoroughly tested through integration testing, ensuring performance and functional efficiency.

2.3.5Release

The release phase involves the deployment of the StreamShield application, potentially initiating with the release of a beta version to a select group of users for further testing. During this stage, feedback, bug, and error reports are actively collected, allowing for continuous improvements and refinements based on user experiences.

2.3.6Feedback

In this phase, reviews and feedback are being collected from the users for continuously improving the features and over all functionality of the application.

2.4 Evaluation

The StreamShield application will be evaluated using ISO 25010 to assess its software quality attributes. The proponents employ a 5-point Likert Scale as the scaling technique to interpret the numerical values obtained from the gathered data. The results were interpreted using the numerical rating scale for interpreting the evaluation result:

Table I. Rating Scale for Interpreting the Evaluation Result

Numerical Rating	Range	Interpretation
5	4.21 – 5.00	Excellent
4	3.41 – 4.20	Very Satisfactory
3	2.61 – 3.40	Good
2	1.81 – 2.60	Fair
1	1.00 – 1.80	Poor

III. RESULTS AND DISCUSSIONS

The proponents delve into the outcomes of this study and the insights garnered from a comprehensive survey conducted among a diverse group of at least 20 respondents. This will present an in-depth analysis and discussion of the results obtained through the survey, shedding light into the habits, experiences, and perspectives of individuals regarding movie streaming, piracy, and the potential solutions offered by Streamshield applications

Listed below are some examples of questions that are used in the survey form.

A. General Questions and Results

Question 1. Do you frequently watch or stream movies on digital platforms?

In this inquiry, 18 out of 21 respondents (85.7%) frequently watch or streams movies on digital platforms and this indicates that there is a high demand for movie streaming apps. This is further supported by the fact that only 3 respondents (14.3%) said they occasionally watch or stream movies on digital platforms. This data also revealed a possibility that the StreamShield anti-piracy movie streaming application is very likely to be used.

Question 2. How often do you encounter spoilers or leaks about movies or TV shows you plan to watch?

The results of how the respondents frequently encounter movie spoilers or leaks is 61.9%. This suggests that there is a demand for an anti-piracy solution like StreamShield, especially among those who frequently experience spoilers, as it can help prevent unauthorized distribution and sharing of content. Additionally, 28.6% mentioned encountering spoilers or leaks occasionally while 9.5% said that they rarely come across spoilers or leaks.

Question 3. Are you aware of the issue of movie piracy and illegal streaming?

The result says that all 21 respondents confirmed that they are aware of the issue regarding movie piracy and illegal streaming. This emphasizes the need for effective anti-piracy measures and content protection mechanism of movies on digital platforms.

Question 4. Have you ever used a screen recording feature while streaming movies or TV shows?

The result reveals that a majority of 76.2%, reported that they have never used a screen recording feature while streaming. This represents users who have not engaged in unauthorized screen recording activities and underscores the importance of implementing screen recording detection features in StreamShield to maintain the integrity of the content. However, 19.0% admitted to having used a screen recording feature while streaming movies or TV shows and 4.8% respondent said *maybe* suggests that some people do use this feature. This minority highlights the existence of screen recording activities and underscores the necessity of StreamShield's screen recording detection capabilities.

Question 5. Would you be willing to use a streaming application like StreamShield that offers screen recording detection and media content protection which aims to combat piracy in the movie streaming industry?

The result says that there is a strong demand for an anti-piracy movie streaming app among people who are concerned about piracy and who want to support the film industry. 71.4% of the respondents expressed their willingness to use a streaming application StreamShield. Though 19% of the respondents said they were not sure whether they would use the application and the remaining 9.5% said they would not use it, is not necessarily a negative sign.

B. Evaluation Results

Using the 5-Likert scale (see Table I), the respondents were able to answer the following evaluation questions:

Functionality

Respondents were asked to assess the effectiveness of StreamShield's anti-screen recording mechanism in preventing unauthorized screen captures during video playback. The category delves into the perceived accuracy of StreamShield in identifying and preventing screen recording during movie playback, providing valuable insights into the application's functional prowess in addressing piracy-related concerns. The findings indicate a positive evaluation overall, with an impressive overall mean rating of 3.6, denoting a "very satisfactory" rating.

Performance Efficiency

StreamShield's performance efficiency, with a very satisfactory overall mean rating of 3.7, indicates that users find the application responsive and quick in streaming movies while implementing anti-piracy features. The positive response underscores StreamShield's ability to balance speed, responsiveness, and content protection effectively, ensuring a smooth and efficient streaming experience for users.

Reliability

The result interprets with the very satisfactory rating and an overall mean rating of 3.73 in the reliability category illustrating StreamShield's effectiveness in delivering a reliable and stable performance, assuring users that the application works consistently without crashes or freezing, thus ensuring an uninterrupted streaming experience.

Security

The survey results in the category, with a very satisfactory overall score of 3.53, indicate that users generally find the application to be effective in preventing unauthorized screen captures and enhancing content security. The very satisfactory rating suggests that most respondents are confident in StreamShield's ability to safeguard content by thwarting illicit screen capture, contributing to an overall secure streaming experience.

Usability

The survey results for the usability of the application are positive, with a very satisfactory overall score of 3.97. It highlights users who find StreamShield simple but user-friendly and intuitive. This rating indicates that StreamShield effectively combines anti-screen recording features with a seamless and easily navigable user interface, contributing to the application's usability and overall user satisfaction.

IV. CONCLUSION

The development and evaluation of StreamShield, with its primary goal of anti-screen recording detection, has yielded promising results. Guided by ISO 25010 standards, the application has effectively achieved its objective in various crucial dimensions. The application excels in terms of functionality, performance efficiency, reliability, security, and usability as it consistently shows a very satisfactory rating. StreamShield has effectively achieved its central objective of anti-screen recording detection while ensuring a user-friendly experience. Its success in balancing content protection and user satisfaction fights against piracy within the movie streaming industry. Ongoing development and optimization will be essential to maintain these high standards in the ever-evolving content piracy landscape.

REFERENCES

[1] Smith, M. D., Telang, R., & Zhang, Y. (2019). "I want you back: The interplay between legal availability and movie piracy." International Journal of the Economics of Business, 26(1), 199-216.

[2] B. R. Kumar, B. A. Vardhan, C. R. Gupta, and P. Surekha, "Reduction of movie piracy using an automated anti-piracy screen recording system: anti-piracy screen recording system," in 2019 4th International Conference on Information Systems and Computer Networks (ISCON), November 2019, pp. 301-304, IEEE.

[3] Rasnacis, A. and Berzisa, S., "Method for adaptation and implementation of agile project management methodology," Procedia Computer Science, vol. 104, pp. 43-50, 2017.

[4] A. M. Abdullah, "Advanced encryption standard (AES) algorithm to encrypt and decrypt data," Cryptography and Network Security, vol. 16, no. 1, p. 11, 2017.

[5] O. Tade and O. P. Mmahi, "Movie piracy networks at Alaba international market, Lagos, Nigeria," International Journal of Offender Therapy and Comparative Criminology, vol. 62, no. 1, pp. 274-285, 2018.

[6] Y. Yue, "The effects of movie piracy on box-office revenue: an empirical analysis of the Chinese movie market," Journal of Applied Economics, vol. 23, no. 1, pp. 618-655, 2020.

[7] N. K. Dubey and H. Modi, "Comparative study of various techniques against camcorder piracy in theater," in 2018 4th International Conference on Computing Communication and Automation (ICCCA), December 2018, pp. 1-4, IEEE.N. K. Dubey and H. Modi, "Comparative study of various techniques against camcorder piracy in theater," in 2018 4th International Conference on Computing Communication and Automation (ICCCA), December 2018, pp. 1-4, IEEE.

[8] W. Sun, Z. Gao, G. Zhai, J. Zhang, Z. Wang, and Y. Zhu, "An improved algorithm for real-time dual-view display," in 2020 IEEE International Symposium on Circuits and Systems (ISCAS), October 2020, pp. 1-5, IEEE.

[9] A. Edosomwan, "Protecting intellectual property rights in Nigeria: A review of the activities of the Nigerian Copyright Commission," World Patent Information, vol. 58, article 101908, 2019.

[10] L. Aguiar, J. Claussen, and C. Peukert, "Catch me if you can: Effectiveness and consequences of online copyright enforcement," Information Systems Research, vol. 29, no. 3, pp. 656-678, 2018.

[11] J. Gu, "From divergence to convergence: Institutionalization of copyright and the decline of online video piracy in China," International Communication Gazette, vol. 80, no. 1, pp. 60-86, 2018.

[12] G. C. Prasetyadi, A. B. Mutiara, and R. Refianti, "File encryption and hiding application based on advanced encryption standard (AES) and append insertion steganography method," in 2017 Second International Conference on Informatics and Computing (ICIC), November 2017, pp. 1-5, IEEE.

[13] N. A. A. Mohd and A. Y. A. Ashawesh, "Enhanced AES algorithm based on 14 rounds in securing data and minimizing processing time," in Journal of Physics: Conference Series, vol. 1793, no. 1, p. 012066, February 2021, IOP Publishing.

[14] N. Atikah, M. R. Ashila, E. H. Rachmawanto, and C. A. Sari, "AES-RC4 Encryption Technique to Improve File Security," in 2019 Fourth International Conference on Informatics and Computing (ICIC), October 2019, pp. 1-5, IEEE.

[15] O. C. Abikoye, A. D. Haruna, A. Abubakar, N. O. Akande, and E. O. Asani, "Modified advanced encryption standard algorithm for information security," Symmetry, vol. 11, no. 12, p. 1484, 2019.

[16] N. A. Fauziah, E. H. Rachmawanto, and C. A. Sari, "Design and implementation of AES and SHA-256 cryptography for securing multimedia file over Android chat application," in 2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), November 2018, pp. 146-151, IEEE.

[17] Y. Yusfrizal, A. Meizar, H. Kurniawan, and F. Agustin, "Key management using combination of Diffie–Hellman key exchange with AES encryption," in 2018 6th International Conference on Cyber and IT Service Management (CITSM), August 2018, pp. 1-6, IEEE.

[18] A. Singh, P. Agarwal, and M. Chand, "Image encryption and analysis using dynamic AES," in 2019 5th International Conference on Optimization and Applications (ICOA), April 2019, pp. 1-6, IEEE.

[19] G. Mujtaba, M. Tahir, and M. H. Soomro, "Energy efficient data encryption techniques in smartphones," Wireless Personal Communications, vol. 106, no. 4, pp. 2023-2035, 2019.

[20] O. C. Abikoye, A. D. Haruna, A. Abubakar, N. O. Akande, and E. O. Asani, "Modified advanced encryption standard algorithm for information security," Symmetry, vol. 11, no. 12, p. 1484, 2019.

[21] J. Zhang, Z. Gu, J. Jang, H. Wu, M. P. Stoecklin, H. Huang, and I. Molloy, "Protecting intellectual property of deep neural networks with watermarking," in Proceedings of the 2018 on Asia Conference on Computer and Communications Security, May 2018, pp. 159-172.

[22] A. K. Sahu, K. Umachandran, V. D. Biradar, O. Comfort, V. Sri Vigna Hema, F. Odimegwu, and M. A. Saifullah, "A Study on Content Tampering in Multimedia Watermarking," SN Computer Science, vol. 4, no. 3, p. 222, 2023.

[23] M. Asikuzzaman and M. R. Pickering, "An overview of digital video watermarking," IEEE Transactions on Circuits and Systems for Video Technology, vol. 28, no. 9, pp. 2131-2153, 2017.
[24] J. Zhang, Z. Gu, J. Jang, H. Wu, M. P. Stoecklin, H. Huang, and I. Molloy, "Protecting intellectual property of deep neural networks with watermarking," in Proceedings of the 2018 Asia Conference on Computer and Communications Security, May 2018, pp. 159-172.
[25] D. Ariatmanto and F. Ernawan, "An improved robust image watermarking by using different embedding strengths," Multimedia Tools and Applications, vol. 79, no. 17-18, pp. 12041-12067, 2020.
[26] X. Yu, C. Wang, and X. Zhou, "A survey on robust video watermarking algorithms for copyright protection," Applied Sciences, vol. 8, no. 10, p. 1891, 2018.
[27] M. Simsek, "Agile Trend Analysis-2020," Medium, June 4, 2020. https://muhammedsimsek.medium.com/agile-trend-analysis-2020-cf774571d5ed.
[28] Advanced encryption standard AES algorithm to Encrypt and decrypt data. (n.d.). https://www.researchgate.net/profile/Ako-Abdullah/publication/317615794_Advanced_Encryption_Standard_AES_Algorithm_to_Encrypt_and_Decrypt_Data/links/59437cd8a6fdccb93ab28a48/Advanced-Encryption-Standard-AES-Algorithm-to-Encrypt-and-Decrypt-Data.pdf