Methods of improving security and resilience of VR systems' architecture

Artem Kachur[1*,†], Sergii Lysenko[1*,†], Oleh Bodnaruk[1,†], and Piotr Gaj[2,†]

[1] *Khmelnitsky National University, Khmelnitsky, Instytutska street 11, 29016, Ukraine*
[2] *Silesian University of Technology, ul. Akademicka 2A, 44-100 Gliwice, Poland*

Abstract

The article provides a thorough exploration of strategies to enhance the security and robustness of Virtual Reality (VR) systems. It starts by dissecting the current hardware architecture, pinpointing potential vulnerabilities, and suggesting improvements. The discussion extends to the use of cutting-edge encryption techniques, emphasizing their role in securing data transfer within VR systems and preventing unauthorized access.

Furthermore, the article delves into the development of sturdy firmware and operating systems, underscoring their significance in maintaining the system's resilience against cyber threats and operational disruptions. It also describes the importance of conducting comprehensive stress testing and vulnerability assessments, enabling developers to identify and rectify security loopholes and enhance system robustness.

The narrative progresses to the implementation of hardware redundancy and fault tolerance, illustrating how these practices can ensure uninterrupted system operation, even when certain components fail. Lastly, the piece tackles the critical aspect of user privacy within VR/XR environments, offering insights into the unique challenges and proposing strategies to protect users' personal data.

Overall, the article presents a holistic approach to fortifying VR systems, integrating various security measures to safeguard against threats, ensuring the reliability of the system, and enhancing the user experience in virtual realms.

Keywords 1

Virtual Reality, Security Enhancement, Advanced Encryption, Firmware Development, User Privacy Protection.

1. Introduction

Virtual Reality (VR) systems have rapidly emerged as transformative technologies with applications spanning diverse domains, including but not limited to gaming, healthcare, education, and industry. The immersive and interactive nature of VR experiences has captivated users and innovators alike, resulting in their pervasive integration into critical applications and environments. However, this proliferation has engendered an imperative concern: the security and resilience of VR system architecture. Ensuring the integrity, confidentiality, and reliability of VR systems has become an exigent scientific challenge, given the potential consequences of system vulnerabilities, data breaches, and operational failures. In response to these concerns, this article embarks on a systematic

IntelITSIS'2024: 5th International Workshop on Intelligent Information Technologies and Systems of Information Security, March 28, 2024, Khmelnytskyi, Ukraine

* Corresponding author.
† These authors contributed equally.
kachurav@khmnu.edu.ua (A. Kachur); sprlysenko@gmail.com (S. Lysenko); piotr.gaj@polsl.pl (P. Gaj); oleg6467@ukr.net (O. Bodnaruk)
0000-0002-4658-2056 (A. Kachur); 0000-0001-7243-8747 (S. Lysenko); 0000-0001-5647-9979 (P. Gaj); 0009-0000-8663-4124 (O. Bodnaruk)

exploration of methodologies aimed at enhancing the security and resilience of VR system architecture. Through a scientific lens, we delve into an array of critical components and methodologies, encompassing hardware analysis, advanced data encryption techniques, firmware and operating system development, systematic stress testing and vulnerability assessments, hardware redundancy, and user privacy protection within VR and Extended Reality (XR) environments. This scientific endeavor seeks to illuminate the multifaceted strategies and innovative solutions required to fortify VR systems, ensuring their reliability and security within an increasingly immersive digital landscape.

Malware detection is also of big importance in terms of VR security. The integration of new tools for malware detection in corporate networks, employing decentralized subsystems with characteristic indicators and analytical expressions for component states assessment, presents a crucial advancement in ensuring cybersecurity within virtual reality environments [1]. Metamorphic virus detection based on obfuscation features analysis has potential significance in virtual reality environments, where ensuring security against malicious software is critical for maintaining user safety and data integrity [2].

The development of a technique for IoT malware detection based on control flow graph analysis is crucial for ensuring the security and integrity of IoT devices interconnected with virtual reality (VR) systems, safeguarding against potential malware threats that could compromise VR experiences and user data [3]. The development of a novel DDoS botnet detection technique utilizing semi-supervised fuzzy c-means clustering, with a demonstrated detection rate of approximately 95%, may hold significant importance in enhancing the security infrastructure of virtual reality environments against potential cyber threats [4]. Techniques of botnet detection using polymorphic code analysis within a multi-agent system, augmented with a novel sensor, may hold significant promise for enhancing security protocols in virtual reality environments [5].

2. Aspects and methods of resilience and security improvement.

In the realm of Virtual Reality (VR) and Extended Reality (XR), the resilience and security of hardware systems are of paramount importance. As these technologies continue to evolve and integrate more deeply into various aspects of daily life, from entertainment to education and beyond, ensuring their robustness and safeguarding user data becomes crucial. This text delves into several key aspects that are integral to strengthening the hardware resilience and security of VR/XR systems. Each aspect addresses a specific component of the VR/XR hardware ecosystem, ranging from the architecture of the hardware itself to the methods employed to protect user privacy. By exploring these aspects and their associated methods, we gain insights into the multifaceted approach required to enhance the security and durability of VR/XR technologies, thereby ensuring a secure and immersive experience for users (Fig.1).

In-Depth Analysis of Current Hardware Architecture. This aspect involves a comprehensive examination of the hardware components used in VR/XR systems. Component Analysis delves into the specifics of each hardware part, assessing their capabilities and limitations. It is crucial for understanding how individual components contribute to the overall system's performance and security. Benchmarking compares different VR/XR systems to identify performance standards and areas needing improvement. This method aids in establishing performance baselines and helps in identifying superior hardware configurations. Reverse Engineering is applied to deconstruct and analyze existing VR/XR devices. This method is invaluable for uncovering hidden vulnerabilities and understanding the underlying architecture of successful systems, providing insights for potential enhancements.

Advanced Encryption Methods for Data Security. Securing the data in VR/XR systems is paramount. Algorithm Evaluation involves scrutinizing current encryption algorithms to determine their effectiveness in the unique context of VR/XR environments. This method ensures that the encryption

does not impede real-time data processing while maintaining robust security. Custom Algorithm Design tailors encryption algorithms specifically for VR/XR systems, optimizing them for the high throughput and real-time requirements of these technologies. Hybrid Encryption Models combine the strengths of different encryption techniques, providing a balanced approach to security and performance, crucial for maintaining seamless VR/XR experiences without compromising data security.

Development of Resilient Firmware and Operating Systems. The resilience of firmware and operating systems in VR/XR hardware is critical for ensuring reliable and secure experiences. Modular Design allows for the easy updating and patching of systems, which is essential for responding to new threats and technological advancements. Intrusion Detection Systems embedded in the firmware enhance security by actively detecting and mitigating threats in real-time. Redundancy and Fail-safes ensure that the system remains operational even in the event of component failure or security breaches, making the VR/XR systems more robust and reliable.

Stress Testing and Vulnerability Assessment. This aspect focuses on proactively identifying and addressing potential weaknesses in VR/XR hardware. Penetration Testing simulates cyber-attacks to uncover vulnerabilities before they can be exploited maliciously. Environmental Stress Testing subjects the hardware to extreme physical conditions to ensure durability and continued functionality under various environmental stresses. Automated Vulnerability Scanning continuously scans the hardware and firmware for vulnerabilities, allowing for immediate detection and rectification of security issues.

Hardware Redundancy and Fault Tolerance. Ensuring that VR/XR systems remain operational and safe under failure conditions is vital. Dual-System Design implements backup components for critical hardware, ensuring system continuity in case of failures. Error Detection and Correction Techniques identify and correct errors in real-time, maintaining the integrity of the system's operations. Load Balancing distributes the processing load across multiple hardware components, preventing system overloads and ensuring smooth operation under varying load conditions.

User Privacy Protection in VR/XR Environments. Protecting user privacy in VR/XR environments is increasingly important. Anonymization Techniques help in making user data anonymous, ensuring personal information cannot be traced back to individuals, thus safeguarding privacy. Consent and Transparency Protocols establish clear guidelines for user consent, ensuring users are fully informed about what data is collected and how it is used. Data Minimization Strategies focus on collecting only the essential data needed for system functionality, reducing the amount of sensitive information that could potentially be compromised.

Each of these aspects and their methods contribute significantly to enhancing the hardware resilience and security of VR/XR systems, ensuring a safer and more reliable user experience (Fig. 1).

3. In-Depth Analysis of Current Hardware Architecture.

Component analysis is a crucial method for evaluating the current hardware architecture of XR devices. This assessment includes addressing challenges like capturing all five human senses, optimizing wearability and functionality, minimizing information mismatches, reducing wires, and addressing ethical concerns, all of which are vital for advancing immersive XR experiences [6].

Some implementations, such as [7], offer a structured approach to selecting suitable VR hardware. It acknowledges the complexity and diversity of VR hardware and addresses the challenge of relating technical specifications to their real-world effects.

The method involves a three-step selection process. Firstly, it considers strategic and organizational factors, using an extended learning factory morphology to define objectives and criteria for hardware selection. The second step focuses on didactic requirements, determining the needed degrees of freedom for tracking and the number of devices based on the intended competencies and action tasks. Finally, in the third step, technical specifications like resolution and

field of view are evaluated. This systematic approach helps organizations and educators make informed decisions, ensuring that selected VR hardware aligns with the intended goals and enhances the overall user experience.

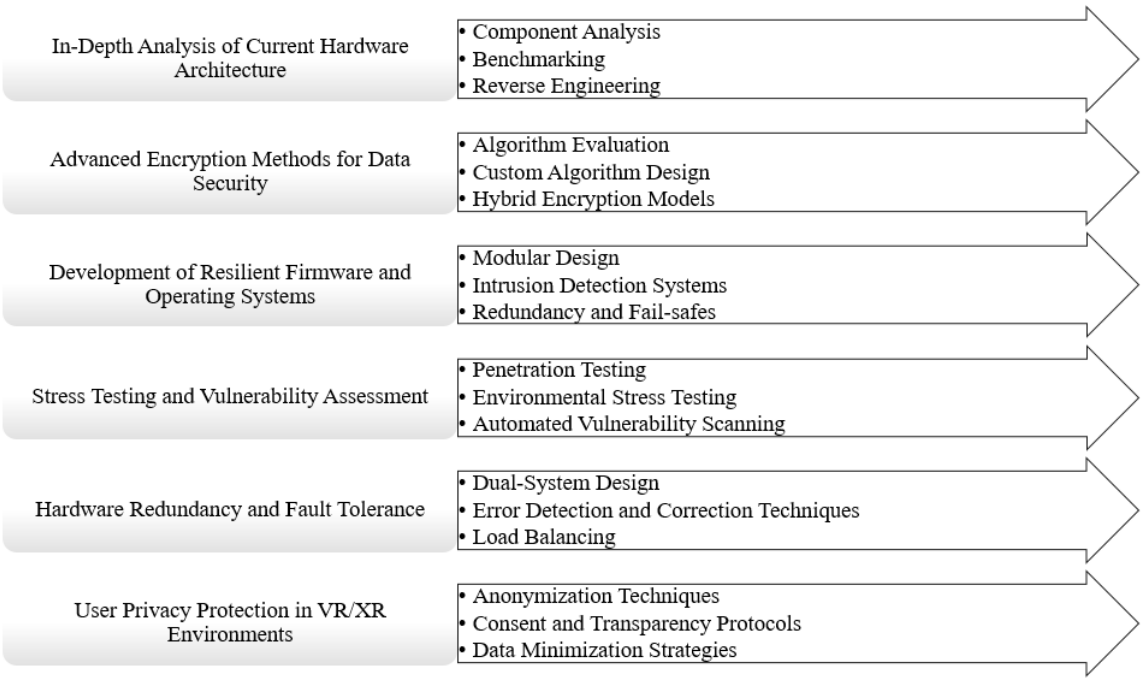

Figure 1: Aspects and methods overview.

Another approach to doing component analysis is to adjust the TAM (technology acceptance model). A proposed VR Hardware Acceptance Model (VR-HAM) is an extension of the established Technology Acceptance Model (TAM), tailored specifically for the virtual reality hardware context. VR-HAM introduces two key variables: curiosity and price willingness, while also incorporating purchase intention as a critical outcome associated with VR hardware acceptance [8].

Curiosity, in this context, refers to the innate desire to seek and acquire new information. This curiosity is primarily driven by interest rather than a sense of deprivation. We argue that individuals with a natural curiosity are more likely to perceive VR hardware as user-friendly because their inclination to explore motivates them to learn about the product.

Price willingness plays a pivotal role in consumer decision-making. Consumers evaluate the value of a product while considering its price. In the diverse VR hardware market, where prices range widely, price willingness serves as a crucial cue for assessing the perceived usefulness, ease of use, and enjoyment of VR hardware. Including this variable in the model is particularly relevant given the emerging nature of the VR hardware market.

The hypotheses derived from the VR-HAM encompass various relationships, such as the positive impact of perceived ease of use, perceived enjoyment, past use, and price willingness on perceived usefulness. Additionally, age is hypothesized to have a negative effect on perceived usefulness, while curiosity, past use, and price willingness are expected to positively influence perceived ease of use. Perceived ease of use and price willingness are also anticipated to positively affect perceived enjoyment.

Data collection for this study involved nonprobability snowball sampling on LinkedIn, targeting professionals with connections. Initially, 150 respondents were approached, and a survey link was provided. Participants were encouraged to share the survey link with three individuals in their network who met specific criteria. The response rate yielded 283 usable responses, representing a 74% response rate.

In summary, the VR-HAM extends the TAM framework to capture the nuances of VR hardware acceptance, introducing curiosity and price willingness as essential factors. The study collected data through LinkedIn, offering insights into the acceptance of VR hardware in an evolving market.

In order to measure the model's validity, researches applied a structural equation modeling (SEM) analysis. To estimate results, they used the χ^2/df ratio, the comparative fit index (CFI), the Tucker–Lewis Index (TLI), the root mean square error of approximation (RMSEA), and the standardized root mean square residual (SRMR). CS is Completely standardized path coefficient. SRMR = 0.069; CFI = 0.954; χ^2 = 1106.495; χ^2/df = 1.682; RMSEA = 0.049; TLI = 0.950; df = 658 (Table 1).

Table 1
Summary of results from hypotheses testing.

Hypothesis	Relationship	CS	Assessment
H1	Perceived ease of use ⟶ Perceived usefulness	0.892	Supported (∗∗)
H2	Perceived enjoyment ⟶ Perceived usefulness	0.290	Supported (∗∗)
H3	Age ⟶ Perceived usefulness	-0.050	Not Supported (NS)
H4	Past use ⟶ Perceived usefulness	-0.084	Not Supported (NS)
H5	Price willing to pay ⟶ Perceived usefulness	0.062	Not Supported (NS)
H6	Curiosity ⟶ Perceived ease of use	0.318	Supported (∗∗)
H7	Age ⟶ Perceived ease of use	-0.086	Supported (∗)
H8	Past use ⟶ Perceived ease of use	0.131	Supported (∗∗)
H9	Price willing to pay ⟶ Perceived ease of use	0.129	Supported (∗∗)
H10	Perceived ease of use ⟶ Perceived enjoyment	0.631	Supported (∗∗)
H11	Price willing to pay ⟶ Perceived enjoyment	0.249	Supported (∗∗)
H12	Perceived ease of use ⟶ Attitude toward using VR hardware	0.257	Supported (∗∗)
H13	Perceived enjoyment ⟶ Attitude toward using VR hardware	0.543	Supported (∗∗)
H14	Perceived usefulness ⟶ Attitude toward using VR hardware	0.187	Supported (∗∗)
H15	Perceived ease of use ⟶ Attitude toward purchasing VR hardware	0.266	Supported (∗∗)
H16	Perceived enjoyment ⟶ Attitude toward purchasing VR hardware	0.348	Supported (∗∗)
H17	Perceived usefulness ⟶ Attitude toward purchasing VR hardware	0.261	Supported (∗∗)
H18	Attitude toward using VR hardware ⟶ Use Intention	0.716	Supported (∗∗)
H19	Past use ⟶ Use intention	0.066	Supported (∗∗)
H20	Attitude toward purchasing VR hardware ⟶ Purchase intention	0.505	Supported (∗∗)
H21	Perceived enjoyment ⟶ Purchase intention	0.160	Supported (∗∗)
H22	Perceived usefulness ⟶ Purchase intention	0.128	Supported (∗∗)

Resilience in VR hardware pertains to its ability to maintain functionality and performance under stressors such as hardware failures and environmental conditions. Meanwhile, security measures are essential to protect user data and system integrity from potential exploits.

By highlighting the importance of resilience and security in VR hardware, we aim to underscore the significance of developing robust and secure devices to foster trust and confidence among users and stakeholders.

An enhanced approach is proposed in [9]. This study's methodology involved undergraduate psychology students and graduate engineering students as participants, recruited voluntarily via social networks, classes, and cafeterias. Data collection was conducted through questionnaires, excluding responses with missing values or non-optimal experimental conditions, leaving 89 valid participants aged 18 to 29. They were divided into two groups to perform assembly tasks in a virtual environment using either a head-mounted display (HMD) or a cave automatic virtual environment (CAVE), with the setup supported by sophisticated hardware and software, including Unity3D and HTC Vive controllers. The study aimed to test an extended Technology Acceptance Model in VR, incorporating user experience variables, VR-specific variables, and user characteristics.

Approaches like Virtual Reality Assembly Assessment (VR2A) focus on the overall production engineer's assessment objective generating quantifiable metrics [10]. The Benchmarking Framework for Interactive 3D Applications in the Cloud, presented in [11], proposes a novel research infrastructure, Pictor, for cloud 3D applications and systems. MazeRunVR [12] investigates into the first steps towards development of a VR locomotion benchmark framework.

Let us consider the idea of Virtual Reality Assembly Assessment. The VR2A experiment design serves as an open, standardized method for evaluating a VR system's geometric limitations in assembly assessment scenarios. By varying two parameters - clearance and assembly part sizes - within an abstract assembly task, the VR2A benchmark provides users with quantified insights into the smallest sizes and clearances for reliable assembly assessments. This benchmark abstracts various influencing factors and error parameters, focusing solely on assessing clearances and part size limitations relevant to assembly tasks. In the VR2A scenario, inspired by a children's game, a virtual reality scene is established, featuring a static table and six discs with cavities of varying sizes. Six dynamic cubes, each representing different sizes, are interactively placed on the table. Participants are tasked with inserting the cubes into corresponding cavities on the discs, indicating whether each cube "Fits in", "Does not fit in", or if they are "Unsure". Task completion time is not measured, emphasizing assessment accuracy over speed.

The VR2A scores are calculated based on the relative frequency of each response, with penalties applied for "Unsure" feedback. This scoring system provides an overall measure of uncertainty for each variation of size and clearance, enabling exploration of VR system limitations. By setting individual thresholds based on VR2A scores, users can determine acceptable sizes and clearances for their specific assessment needs.

The results are calculated as follows: Each of the three answer possibilities are sorted into matrices containing the relative frequency for each condition. The relative frequencies of answers "Fit in" ($A_{Positive}$) "Does not fit in" ($A_{Negative}$) and "I'm unsure" ($A_{Neutral}$) are calculated. (1) calculates the relative homogeneity of answers between the assessments. If $S_{homogenity}$equals zero in the matrix, the value of 0% would indicate, that the same amount of people state "Fits in" and "Does not fit in". Therefore, the assembly assessment would not include any reliable results.

$$S_{homogenity} = abs(A_{Positive} - A_{Negative}) \quad (1)$$

The overall VR2A score S_{VR2A} additionally penalizes "I'm unsure" feedbacks by the participants (see (2)). Therefore, VR2A score can be interpreted as the overall uncertainty for each variation of size and clearance

$$S_{VR2A} = abs(A_{Positive} - A_{Negative}) - A_{Neutral} \quad (2)$$

Therefore, S_{VR2A} can theoretically range from -100% to 100%. Using these results, the overall VR system limitations can be explored using VR2A. Setting an individual threshold of for example 80% VR2A, gives a clear understanding, how small assembly parts and clearances may get in order to achieve the personal VR assessment purpose. Results are depicted in Fig. 4. Low scores indicate high uncertainty and inhomogeneity of answers. The lowest VR2A value can be found in scenario 6.25mm

sized cube with 103% clearance with the value of -31.2%. Highest values have been found for the biggest cube in 97% scenario: All participants recognized correctly, that the 200% cube does not fit in.

The results show that detecting collisions is easier than identifying small clearances. VR assembly scores were significantly higher for 97% overlap compared to 103% clearances, with minimal difference between 97% overlap and 110% clearances. Maximum uncertainty was expected at 100% clearance scenarios, while 103% clearances yielded the smallest VR2A values. Further research is needed to explore whether this trend holds across all assessments.

Participants tended to provide judgment answers rather than stating "I cannot assess it", even in scenarios with no clearance. Human tremble and VR headset resolution were identified as limiting factors, particularly for smaller cube sizes. While participants found it challenging to assess large cubes due to the need for significant head movement, VR2A still operates with collision avoidance disabled, suggesting potential for further research with collision detection enabled.

In summary, the VR2A benchmark offers a standardized method for evaluating VR assembly assessment performance and limitations. It can be applied universally across different environments, simulation software, and VR hardware. Future research will explore the impact of more complex assembly geometries and task-completion time, as well as evaluating VR2A across diverse populations and technologies. Third-party research will also be integrated to enhance the benchmark's robustness and applicability.

MazeRunVR [12] includes a game, developed using the Unreal Engine, which features a procedurally generated maze that changes layout each session, preventing memorization of paths and ensuring a unique experience under 5 minutes to encourage repeated playthroughs. This design choice aims to explore user movement in all directions, evaluating their adaptability to dead ends and different locomotion methods: arm swing, walk-in-place, and trackpad movement. At the game's conclusion, players rate their locomotion preference on a 3-level Likert Scale. Data from each session, including locomotion preference and gameplay duration, is collected for analysis. The game's availability is broadened through a dedicated website, promoting engagement through various social media platforms.

MazerunVR, available since August 25, 2019, had around 40 participants and 80 play sessions by September 20, 2019. Geographic data showed 30% of sessions were from New Zealand and 26.3% from Germany, with other notable contributions from Japan, the USA, Egypt, Mexico, China, Turkey, the Netherlands, and Korea. In testing locomotion methods, arm swing, walk-in-place, and trackpad movement were compared, revealing significant speed and preference differences. Arm swing (mean rank speed: 53.06, preference: 58.06) was faster and more preferred than walk-in-place (speed: 16.3, preference: 25.2) and trackpad (speed: 46.92, preference: 33.1). Simulator sickness analysis across these methods showed significant differences in induced nausea, oculomotor effects, disorientation, and total sickness scores, with walk-in-place and trackpad often resulting in higher discomfort than arm swing.

The democratization of the digital realm has opened avenues for leveraging, analyzing, and enhancing cultural heritage using digital techniques, ranging from volume scanning to virtual restitution. However, despite the diverse applications, practical feasibility often takes precedence over public or expert access due to data complexity and computational limitations. The ReSeed project seeks to address this challenge by offering a holistic approach that combines semantic linking of objects with physical modeling, thereby preserving knowledge without filtration [13].

4. Advanced Encryption Methods for Data Security

Securing data within VR/XR systems is of utmost importance. Algorithm Evaluation entails assessing existing encryption algorithms to gauge their efficacy within the distinctive context of VR/XR environments. This approach ensures that encryption does not hinder real-time data processing while upholding robust security standards. Custom Algorithm Design tailors encryption algorithms

precisely for VR/XR systems, optimizing them to meet the high throughput and real-time demands of these technologies. Hybrid Encryption Models amalgamate the merits of various encryption techniques, offering a well-rounded approach to security and performance. This balance is vital for maintaining seamless VR/XR experiences without compromising data security.

During the VR user profiling framework development, user identification and profiling were conducted in both Augmented Reality (AR) and Virtual Reality (VR) scenarios, revealing higher accuracy in VR compared to AR [14]. Eye-tracking sensors proved particularly beneficial in VR, highlighting their potential for enhancing user profiling methodologies in virtual environments. A novel secure display system, which uses virtual cryptography, is introduced in [15]. Let us consider this system. T2VC, a tracking-tolerant visual cryptography system designed for AR or VR head-mounted displays (HMDs). Unlike traditional systems, T2VC splits confidential information into two shares displayed separately, allowing users to visually align and decrypt the message without relying on trusted computing bases (TCBs) or chinrests. Leveraging visual tracking modules, T2VC mitigates head jittering issues and enhances visibility through novel diffusion algorithms, making it practical and robust for real-time decryption.

The core concept of T2VC involves modeling the likelihood of misalignment between pixels from different shares using a 2D Gaussian distribution centered at each pixel. This approach prioritizes clarity over contrast in the fused result, particularly when encountering slight misalignments of one or two rows. The first step of the algorithm is preprocessing. Given a confidential visual image I, firstly a binary image Î is generated by thresholding every 2×2 block of pixels in I. Here, the authors denote F(Î) and B(Î) as the set of foreground (white) and background (black) pixels of Î, respectively. Next, they model the range of misalignment as an s×s square and generate an s×s 2D Gaussian kernel G (x, y,σ) at scale σ:

$$G(x, y, \sigma) = \frac{1}{2\pi\sigma^2} e^{-\frac{x^2+y^2}{2\sigma^2}} \tag{3}$$

In the experiment, the authors choose s = 3,σ = 1.0 and s = 5,σ = 2.0.

T2VC generates the initial share following the classical VC approach, where each 2 × 2 pixel block randomly selects one of six VC patterns. To address potential misalignments, two solutions are employed:

- T2VC*: In the second share, only foreground pixels are diffused, introducing a probability of misalignment with surrounding pixels. This darkens the foreground while leaving the background unchanged when both shares perfectly match.
- T2VC: In the second share, both background and foreground pixels are diffused to enhance contrast. Each pixel undergoes a probability of misalignment with its surroundings, facilitating improved contrast throughout.
- A custom C++ program is utilized to generate visual images at 1024x1024-pixel resolution employing both T2VC and classical visual cryptography algorithms under various conditions. The findings reveal:
- The classical visual cryptography algorithm struggles with even minor misalignments, rendering interpretation challenging when visual tracking is slightly off.
- T2VC* can tolerate one row or column misalignment (2 pixels) while maintaining comparable contrast to the original algorithm, albeit with some contrast reduction.
- T2VC demonstrates superior contrast retention compared to T2VC* when misalignment occurs, even accommodating two pixels misaligned both horizontally and vertically. Increasing the size and scale of the Gaussian kernel enables the detection of the secret message even with two rows (four pixels) of misalignment.

Another approach to ensure VR system security is data hiding. Ensuring both high security and effectiveness is crucial in transmitting data, especially for satellite remote sensing and medical images. To address this, the Completely Separable, Reversible Data Hiding in Encrypted Images (SRDH-EI) algorithms is proposed [16]. In this approach, the sender preprocesses the cover image by compressing pre-embedded pixels and embedding header data for marking. Subsequently, auxiliary and secret data are embedded in a forward and reverse "Z" shape before and after encryption, respectively. Experimental results demonstrate high embedding capacity and security for remote sensing images, maintaining entropy and enabling distortion-free recovery of the decrypted image. This approach offers promising applications for remote sensing images due to its complete separability at the receiver's end.

The encryption algorithm encrypts the marked image using encryption key Ke. Assuming that the range of pixelgrayscale values f(i, j) at the position (i, j) in the marked image is [0, 255]. Each pixel can be represented as bits bi,j,k, with k values [1, 8]. The relationship between the grayscale values f (i, j) and bi,j,k, is as follows:

$$b_{i,j,k} = \left\lfloor \frac{f(i,j)}{2^{k-1}} \right\rfloor mod\ 2, k = 1,2,\dots,8 \tag{4}$$

$$f(i,j) = \sum_{k=1}^{8} \left(b_{i,j,k} \times 2^{k-1}\right), k = 1,2,\dots,8 \tag{5}$$

Then, use *Ke* to generate a pseudo-random binary array $r_{i,j,k}$, and perform an XOR operation with $b_{i,j,k}$. The calculation is as follows:

$$b_{i,j,k} = \left\lfloor \frac{f(i,j)}{2^{k-1}} \right\rfloor mod\ 2, k = 1,2,\dots,8 \tag{6}$$

where $B_{i,j,k}$ is the results in encrypted bit form. The encryption key *Ke* also serves as the decryption key and has reversibility, ensuring complete restoration of the image content before encryption during the decryption phase. Through this step, the encrypted image can be obtained, and the content of the cover image is protected

An approach of data hiding, which can be widely used in healthcare related VR environments, is described in [18]. This research introduces significant advancements in medical image security: a double POB digital system is employed to concurrently facilitate data hiding and medical image authentication, offering a large data embedding capacity and a pixel-level, highly sensitive authentication process suitable for detecting minor tampering in medical contexts. Additionally, a novel method utilizing bit plane separation and cross-reorganization is proposed to safeguard sensitive information within medical images, strategically protecting high-bit sensitive pixels in the Region of Interest (ROI). Furthermore, the study introduces a tampering recovery technique for medical images based on compressed data repeated filling, allowing for the restoration of untampered areas if tampering is detected during the authentication phase. In this process, the brighter areas, known as the Region of Significance (ROS), contain crucial information, while the darker areas are mostly redundant. To preserve the quality of medical images, the image owner initially conducts preprocessing on the ROS before embedding secret data and authentication bits to create two shares. These shares are then sent to the receiver, who, upon authenticating the image, extracts the ciphertext information and achieves lossless recovery of the image.

To enhance the protection of critical regions in the Region of Sensitive (ROS), it initially undergoes segmentation, with the OTSU algorithm determining the optimal threshold. Regions above this threshold are designated as the Region of Interest (ROI), while those below are termed the Region of Non-Interest (RONI). Following segmentation, the regions are restructured through bit plane separation. Specifically, the top five bits from the ROI and the bottom three bits from the RONI are merged to form a new 8-bit image named ShareA. Conversely, the bottom three bits of the ROI and the top five bits of the RONI are amalgamated to create another 8-bit image, ShareB. In this setup, ShareB, holding less critical pixel data, and the more crucial ShareA undergo a prioritization process,

with ShareB being used first in the information embedding stage to ensure the ROI's integrity in the medical image is maintained (Fig.2).

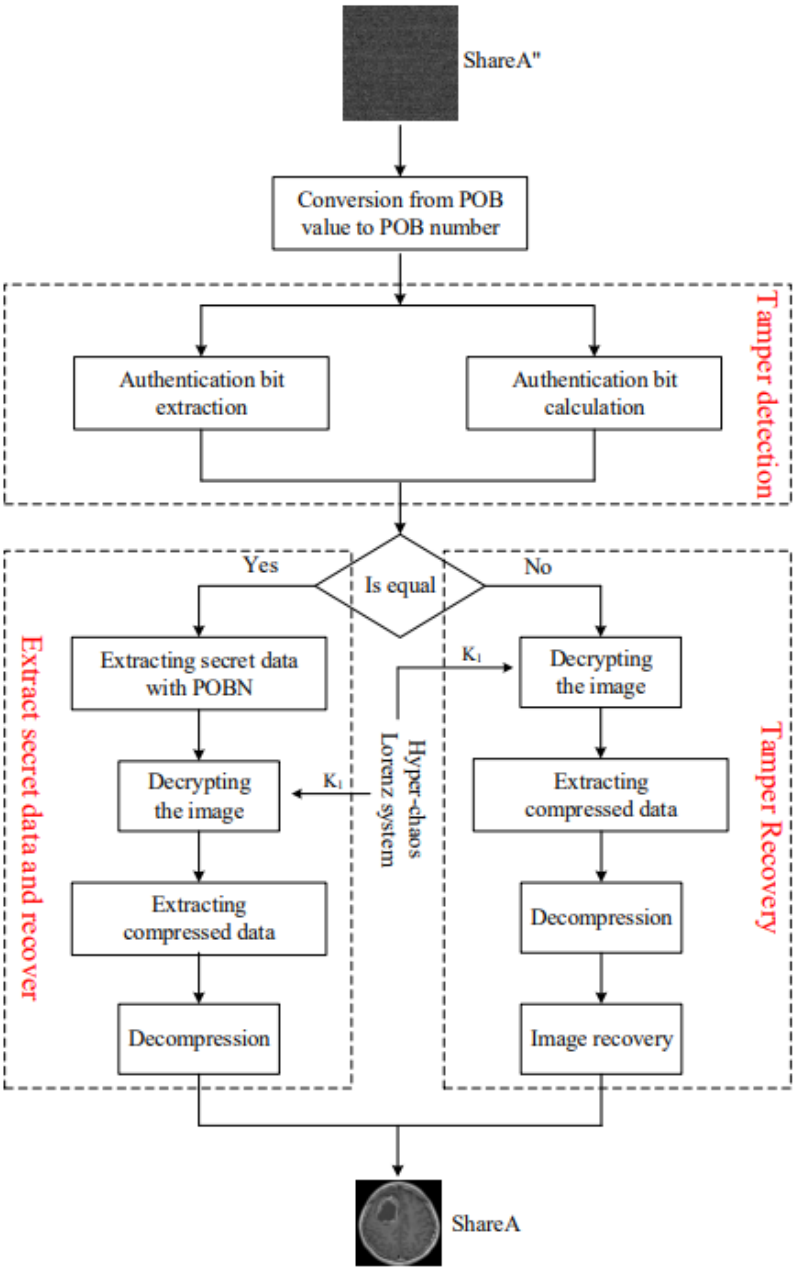

Figure 2: Process flow chart of extracting secret information and image recovery.

In telemedicine related VR systems, the risk of attacks aimed at tampering with, stealing, or forging patient private information or medical image content is a significant concern. Such malicious actions could result in incorrect diagnoses and potentially severe medical mishaps, which are unacceptable. To counteract these threats, the approach detailed in this paper embeds confidential information within the medical image while also conducting identity authentication, as illustrated. This dual-layered strategy not only safeguards patients' personal data but also upholds the integrity and security of the medical image itself (Fig.3).

This paper introduces a novel medical image hiding and authentication algorithm using a double POB system, enhancing security in healthcare-related VR systems. It involves extracting ROS, segmenting images into ROI and RONI, and employing bit plane separation and cross-reorganization to create encrypted shares. The algorithm embeds secret messages and authentication bits via the

POB number system, ensuring integrity through a verification process before image recovery. If untouched, the original image is restored; if tampered with, lossless recovery utilizes the filled data. This method boosts embedding capacity while maintaining image quality and effectively protects sensitive pixels. Although the double POB system incurs additional time due to simultaneous compression and re-encryption, its benefits in secure data embedding and recovery are notable, offering a promising approach for wide application in healthcare VR systems.

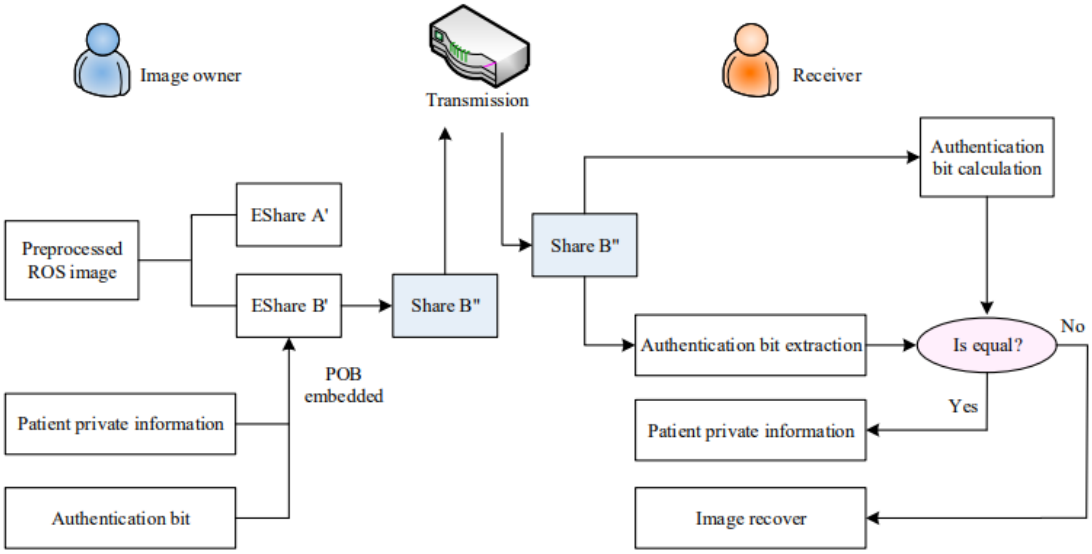

Figure 3: The application scenario of the proposed scheme.

5. Development of Resilient Firmware and Operating Systems

Broadly defined as technology enabling visualization of complex data sets or interactive exploration of spatial environments, VR immerses users in computer-generated realities through sensory input and output device. The approach proposed in [18] delves into the development of an operating system (VROS) primarily for immersive VR systems, while also considering ideas for augmented reality (AR) systems. VROS aims to leverage futuristic developments, including transparent and opaque displays, to usher in the fourth generation of head-mounted displays (HMDs). Focusing on hardware and software interactions, VROS serves as a fundamental enabler for fully utilizing and interacting within immersive virtual environments, addressing the need for a comprehensive operating system tailored to VR and AR experiences. Through assessing existing work, this approach aims to identify core features essential for immersive realities and outline the key functionalities of such an operating system.

In terms of VR firmware and OS development, it is crucial to mention intrusion detection capabilities. VR networks confront significant security challenges, including vulnerabilities to malicious interference and exploitation by illegitimate users. Attackers employ various tactics, including eavesdropping and immersive attacks like the "Human Joystick Attack," which manipulates users' VR experiences to potentially dangerous ends. Moreover, exploitation of system vulnerabilities and compromised devices poses risks to personal safety and critical infrastructure, manifesting in advanced persistent attacks (APTs) and other similar vectors [19]. The proposed AI-driven framework for threat detection and mitigation in non-immersive VR communication networks is illustrated in Fig. 7. By leveraging IoT data, including normal traffic and attacks like DDos and Dos Hulk, a deep learning (DL) model for intrusion prediction was constructed. The model comprises 5 layers, with an input layer of 17 dimensions and an output layer with 2 dimensions representing class labels (Benign or Attack). Hidden layers consist of 100 and 50 neurons, utilizing the rectified linear unit (ReLU). Integrated into users' head-mounted displays (HMDs), the self-defense framework analyzes incoming

network traffic for deviations and triggers alarms preemptively for early threat detection. To boost confidence in the model, SHAP is utilized for explainable artificial intelligence (XAI), providing both global and instance-specific explanations using game theory to estimate feature importance.

Since VR systems can be tightly intertwined with IoT environments, an approach of IoT intrusion detection, proposed in [20], can be used in development of the environment firmware and operating systems. NIDS (Network Intrusion Detection Systems) monitor internet traffic in IoT networks, serving as a frontline defense to identify and thwart intrusions and malicious attacks. It scrutinizes network traffic, user behavior, and detects both known and unknown threats, aiming to maintain network integrity by detecting unauthorized access and facilitating defensive measures like firewall rule implementation. NIDS alerts administrators to both internal attacks, initiated from compromised devices within the network, and external threats from outside sources. It operates on three core principles: observing network traffic, analyzing it for suspicious patterns, and detecting potential intrusions to trigger alerts. The development of effective NIDS for IoT is crucial, encompassing detection methods, placement strategies, understanding security threats, and validation approaches. MEC (Multi-Access Edge Computing) can be a resource to provide security for such environments.

Recently, there has been a surge in interest in Mobile Edge Computing (MEC) standardization, a priority for key telecommunication and network players, under the guidance of bodies like the European Telecommunications Standards Institute (ETSI) and the Open Edge Computing Initiative (OEC). NIDS, when applied in IoT environments, particularly in use cases involving MEC, demands high service quality, low latency, significant throughput, and real-time functionality. The preference for MEC over cloud computing in designing NIDS for IoT systems stems from the need to overcome cloud computing's notable latency issues. Key advantages of using MEC for NIDS in IoT include real-time security context-awareness, energy efficiency post-data transfer, and enhanced data privacy/security, addressing the concern of data ownership and potential leaks prevalent in cloud solutions.

Incorporating NIDS in VR applications within IoT ecosystems, especially when combined with MEC, can significantly enhance the security and user experience. By doing so, VR systems can benefit from reduced latency, ensuring a seamless, real-time virtual environment that is crucial for user immersion and interaction. Moreover, the integration of NIDS ensures robust security measures, safeguarding user data and interactions in the VR space, which is particularly vital given the sensitive data often processed in these applications. This synergy between NIDS, MEC, and VR in IoT frameworks heralds a new era in secure, efficient, and user-centric virtual experiences.

6. Stress Testing and Vulnerability Assessment

Stress testing and vulnerability assessment play a crucial role in ensuring the robustness and security of VR systems. By subjecting VR systems to various stressors and identifying vulnerabilities, organizations can proactively address weaknesses, mitigate risks, and enhance overall system resilience. This process helps to safeguard sensitive data, prevent potential cyber-attacks, and maintain a seamless and secure user experience in virtual environments [21].

Technologies like virtual reality offer innovative ways to study human behavior and enhance skill training across various fields such as sports, medicine, and safety industries. However, the widespread adoption of VR for training often precedes thorough testing and validation, risking effectiveness. To ensure successful implementation for training and experimentation, it is crucial to assess whether VR simulations accurately replicate real-world tasks and elicit realistic behaviors. A taxonomy and practical methods for testing and validating VR environments, emphasizing the importance of fidelity and validity in enabling successful learning transfer to real-world contexts can be proposed[21] (Fig.4).

In recent decades, the public release of numerous regional and global digital elevation models (DEMs) has provided researchers with a variety of options for their studies, including the use of these

DEMs for creating derived products like orthorectification. However, comparing these DEMs is complex. For accurate quantitative analysis, DEMs must align in the same coordinate reference system (CRS), adhere to the same grid specifications, and be calibrated to the same vertical reference system (VRS). Fortunately, a variety of open-source tools are available to facilitate these complex transformations with precision and ease. Yet, even with these adjustments, there might still be local or global planimetric differences observed across DEMs, which can introduce significant errors in elevation comparisons or in the analysis of derived features such as slope and aspect. As such, ensuring planimetric accuracy of DEMs is a critical preliminary step in any comparative analysis. The paper [23] introduces an enhanced disparity analysis method that achieves sub-pixel accuracy by interpolating linear regression coefficients within a specified exploration window, offering a refined approach to DEM comparison.

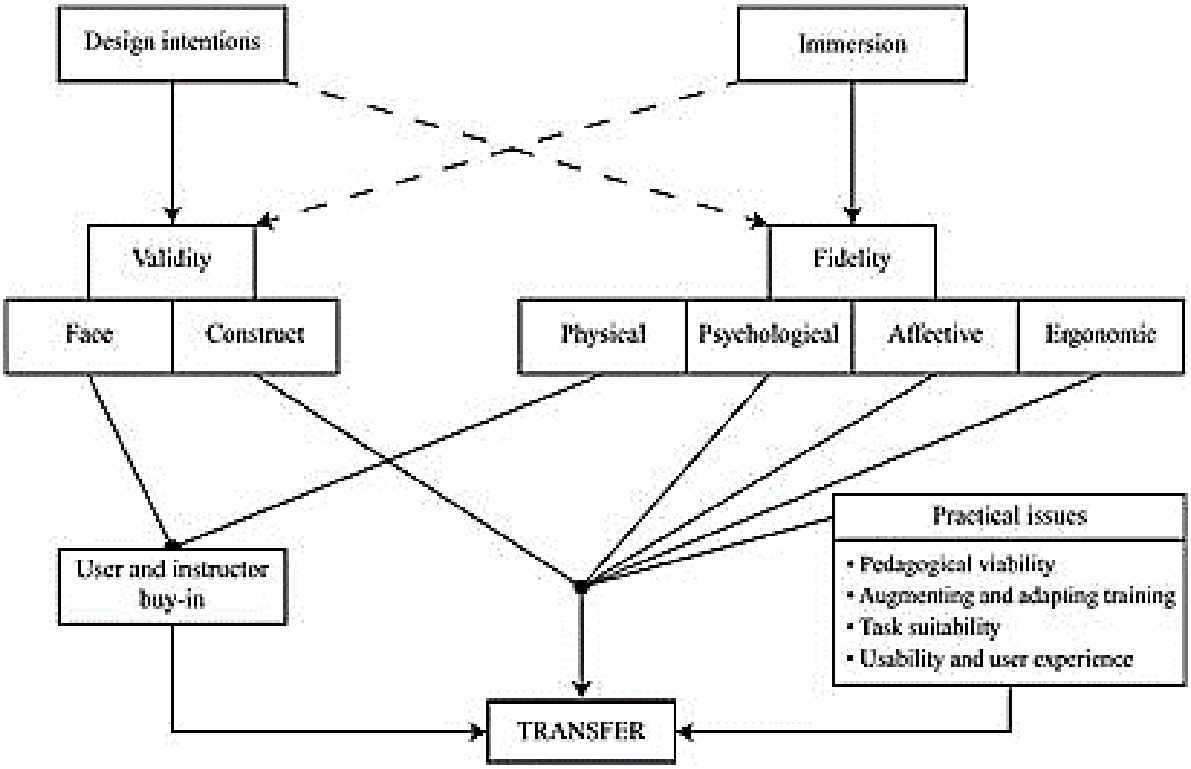

Figure 4: Taxonomy of fidelity and validity and successful transfer of learning from VR. We propose that construct validity and psychological, affective and ergonomic fidelity.

To implement the algorithm, it is essential that the input DEMs be on a level playing field, meaning they should share the same coordinate reference system (CRS), vertical reference system (VRS), and pixel grid alignment. Often, this necessitates transforming one or more of the input DEMs to align with these standards (Fig. 5).

The analysis compares two DEMs (referred to as DEM1 and DEM2) and is influenced by two key parameters: the sizes of the exploration window (ex,ey) and the correlation window (cx,cy). The exploration window determines the range within which the algorithm searches for corresponding pixels, with a larger window accommodating the detection of bigger displacements. Meanwhile, the correlation window defines the area over which the DEMs are compared to find matches, influencing the precision and reliability of the detected displacements. Using these settings, the analysis generates two displacement maps in pixel units (dP for horizontal and dL for vertical shifts), indicating how to adjust DEM1 to align with DEM2.

For every pixel in DEM1, the algorithm identifies a matching pixel in DEM2 that shows the closest local configuration. This search happens within the exploration window, centered on the

corresponding pixel's location in DEM1. The matching process involves calculating the normalized cross-correlation (NCC) between correlation windows centered on the pixel in DEM1 and moving across potential matches in DEM2. Through this process, applied across all pixels in DEM1, the algorithm calculates planimetric displacement as the distance (in pixels or meters) between the exploration window's center and the matching pixel's center in DEM2.

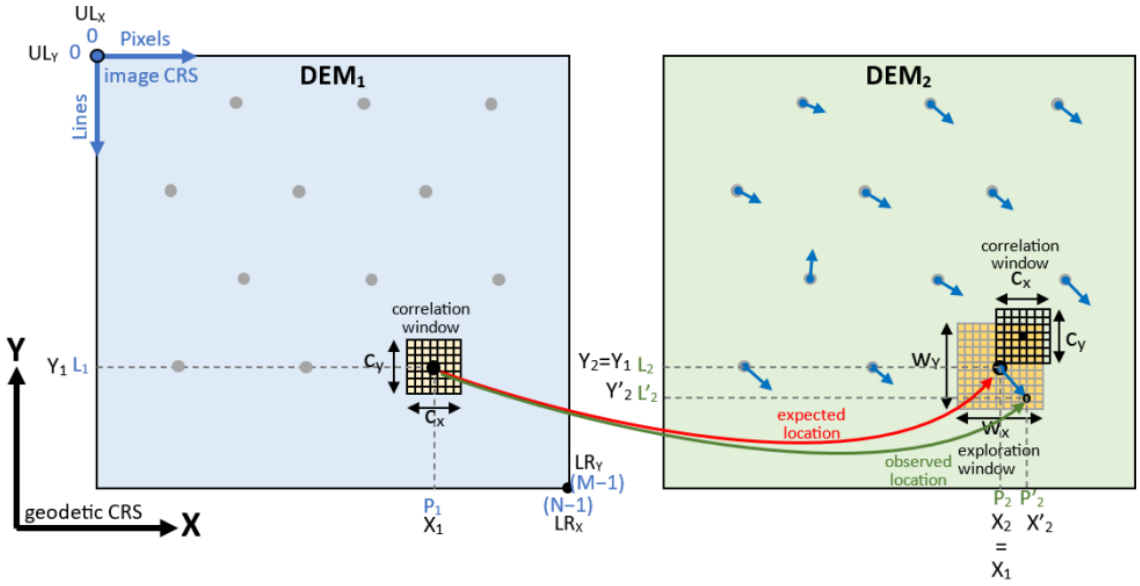

Figure 5: Principle of disparity analysis—pixel level displacement retrieval.

Validation of this novel method demonstrates accurate sub-pixel displacement detection, influenced by the disparity analysis parameters and the bicubic resampling pre-processing step. This resampling, crucial for co-gridding input DEMs, allows fine-tuning via the Best BiCubic (BBC) parameter, optimizing error minimization in displacement retrieval. Results show significant error reduction in displacement measurements across various terrains, with errors ranging from 3.653 m in France to 5.825 m in Croatia, notably lower than the Copernicus DEM GLO-30's pixel size. The method's efficacy varies with terrain, showing different BBC parameters for mountainous versus flat areas. A study across 67 European locations found a logarithmic correlation between terrain roughness and the BBC parameter. This method's accuracy in capturing sub-pixel displacements makes it a valuable tool for future DEM comparisons, potentially aiding in the detection, quantification, and correction of planimetric misregistrations, especially with the advent of high-resolution reference DEMs (Fi.6).

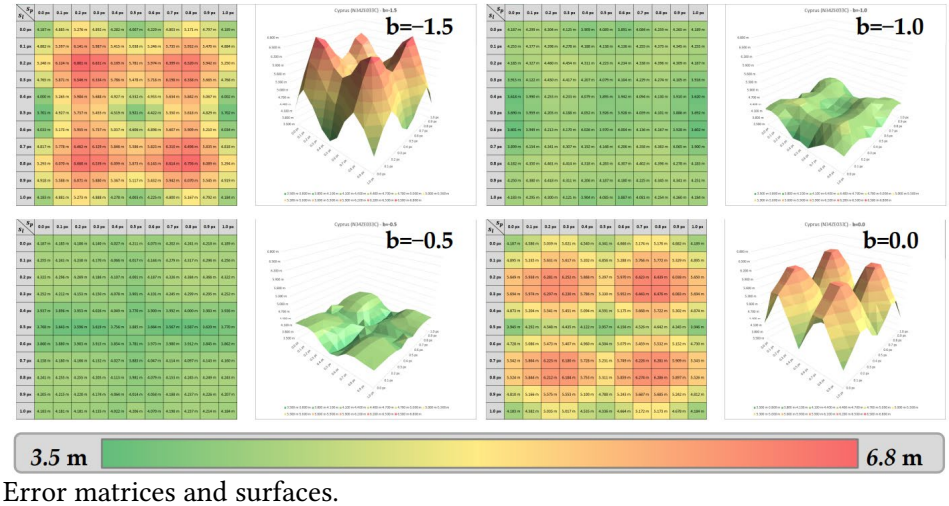

Figure 6: Error matrices and surfaces.

7. Hardware Redundancy and Fault Tolerance

Hardware redundancy and fault tolerance are paramount in VR systems to ensure uninterrupted and reliable user experiences. Given the immersive nature of VR and its reliance on complex hardware components, any failure or downtime can significantly disrupt user engagement and productivity. By incorporating redundant hardware components and fault-tolerant mechanisms, VR systems can mitigate the risk of system failures and maintain seamless operation even in the event of hardware malfunctions or errors. This not only enhances user satisfaction and trust but also safeguards critical applications such as medical simulations, training exercises, and mission-critical operations, where uninterrupted functionality is imperative. Therefore, hardware redundancy and fault tolerance are indispensable strategies for ensuring the reliability and resilience of VR systems. The ways to achieve hardware redundancy are common between general-purpose computer system and VR; however, there are some special approaches related to digital image processing.

In harsh environments like space, electronic circuits are prone to faults due to radiation. Redundancy is commonly used to mitigate these faults, along with considerations for low power and small size to enhance energy efficiency and reduce weight and cost. Triple modular redundancy (TMR) is a favored approach, but it consumes more area and power compared to a single circuit. Alternative strategies like selective TMR (STMR) and majority voting-based reduced precision redundancy (VRPR) offer promising solutions, particularly for error-tolerant applications like digital image processing relevant to space systems. However, these approaches may not be suitable for control logic implementation. This study evaluates TMR and VRPR performance for digital image processing, providing MATLAB-based and physical implementation results using a 28-nm CMOS technology [24].

Using FPGA based hardware redundancy techniques can also significantly help in creating fault tolerant digital filters for VR environment hardware. The increasing reliance on communications and signal processing in daily life drives the need for more reliable devices with minimal transient fault errors. To this end, the 5-modular redundancy technique is employed, enhancing the dependability of hardware prone to failure. In the realm of digital signal processing, FIR digital filters are pivotal, facilitating complex computations, multiplications, and frequency selection for various applications. Chosen for their stability and straightforward implementation, FIR filters, consisting of multipliers, adders, and delay units, play a crucial role in signal processing, including noise reduction through signal denoising. The implementation of these filters is further refined using FPGA methods with Xilinx Vivado EDA [25]. Configurations such as 5MR as TMR (XOR-MUX), 5MR as Cascaded TMR, 4 to 1 MUX and Vedic multiplier were reviewed in terms of their additional redundancy capabilities.

A 4x4 Vedic multiplier, represented in binary, is executed using Verilog code to minimize delay. This multiplier is constructed with nine full adders and a unique 4-bit adder, enhancing its efficiency. The architecture of the Vedic Multiplier is depicted.

The simulations and implementations were carried out to facilitate effective comparisons. For the proposed FIR filters, the focus was on comparing ECG signal noise rejection with that of other signals. The architectures utilized in the EDA were those reported in the literature alongside valid ones. The performance of these architectures was compared based on the number of look-up tables (LUTs), slices, and flip-flops. On the flip-flops bar chart, bars 1 through 5 mean Conventional 5MF configuration, TMR (XOR), TMR (XNOR), Cascaded TMR and 4 to 1 MUX accordingly.

The Fault-Tolerant Digital filters employing 5MR configurations utilize FIR filters across various setups, including conventional 5MR, 5MR with TMR using XOR/XNOR as MUX, cascaded 5MR with TMR, and 5MR with a 4 to 1 MUX configuration. The architecture incorporates a Vedic Multiplier for high-speed operation, ensuring minimal latency. This FIR architecture, combining the Vedic multiplier and carry-save adder, stands out for its low power and space requirements compared to other FIR structures in literature. Post-simulation, all 5MR configurations effectively reduce ECG signal noise using the Xilinx EDA tool while optimizing area usage. Integrating these configurations

into VR hardware could significantly enhance stability and reliability, ensuring smoother and more immersive virtual reality experiences.

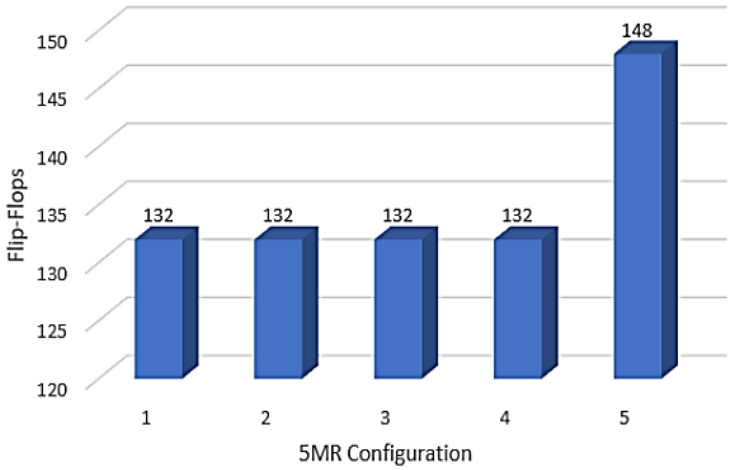

Figure 7: Flip flops bar chart.

8. User Privacy Protection in VR/XR Environments

User privacy protection in VR/XR environments is of paramount importance due to the immersive nature of these technologies. As users engage in virtual experiences, they may unknowingly disclose sensitive personal information or behaviors. Ensuring robust privacy measures safeguards users from potential risks such as unauthorized data collection, tracking, or exploitation of personal data. It fosters trust in VR/XR platforms, encouraging users to fully immerse themselves in virtual experiences without fear of privacy breaches. Additionally, prioritizing user privacy aligns with ethical principles and regulatory requirements, contributing to the responsible development and adoption of VR technologies. Immersive technologies represent a groundbreaking advancement, offering users unparalleled experiences blending virtual and real elements. In such environments, user privacy and security are paramount due to the sharing of sensitive information, making user authentication crucial. This paper conducts a systematic literature review of recent research on user authentication mechanisms in immersive technologies. Through analysis of 36 publications identified from a Scopus search conducted in September 2023, three main authentication types emerge knowledge-based, biometric, and multi-factor methods. Categorizing and scrutinizing these methods, this review serves as the first comprehensive consolidation of user authentication in virtual, augmented, and mixed reality environments [26].

The rise of virtual reality (VR) technology has led to its widespread adoption across various sectors, including medicine, education, and manufacturing. As VR devices become more advanced and widely used, the need for secure user authentication methods has become increasingly important. In the research [27], the authors propose a novel approach to user identification in VR environments, leveraging natural kinesiological cues captured by integrated eye tracking and gesture controllers. By achieving an accuracy of 98.6%, surpassing previous methods, they address the demand for robust and non-intrusive identification solutions suitable for multi-user VR scenarios. Despite the growing popularity of VR applications, user privacy and security remain overlooked aspects. Traditional authentication methods, like PIN or SWIPE, are impractical in VR due to unique interaction patterns and limited awareness of the external environment. To address this gap, the study focuses on leveraging distinct kinesiological behavioral patterns exhibited by users in VR environments for biometric identification. BioMove, a system designed to capture and analyze head, limb, torso, and eye movement patterns as biometric authentication factors in VR, is introduced. The findings offer

promising insights into enhancing the security and usability of VR systems, paving the way for future advancements in immersive technology authentication.

During the experiment, participants engage in multiple tasks within the VR environment, with varying completion times for each task. To standardize the dataset across participants, the data is resampled. Each task is characterized by a sequence of movement vectors captured at a rate of 25 vectors per second (25 Hz). For instance, if Participant A completes Task 1 in 50 seconds and Participant B in 100 seconds, Participant B's data contains 2500 movement vector readings, while Participant A's has 1250. The resampling process ensures that all participants have an equal number of movement vector readings, selecting 1250 readings from Participant B's data to achieve consistency.

- Session: A Session S is a set of tasks T:

$$S = \{t_1, \dots, t_6\}, where\ cardinality\ |S| = 6 \tag{7}$$

- Task: A task T is a set of movement vectors m:

$$T = \{m_1, \dots, m_n\}, where\ cardinality\ |T| = n \tag{8}$$

- Median: The median D of the cardinality of movement vectors |T| for each type of tasks {t1, ..., t6} across all sessions S in the experiment are determined as follows: For Each Task type Tx (where $1 \leq x \leq 6$) in the Experiment

$$D_x = Median(|T_x|_1, \dots, |T_x|_n) \tag{9}$$

  where |Tx| is the cardinality of a set of movements of task type x.

A higlhy accurate participant identification within the VR environment was achieved, with an average processing speed of 0.035 ms per classification on a Windows 10 PC (Intel Core i7-6700, 128GB RAM, NVIDIA GeForce 1080) with the GPU clocked down to 1600 MHz. This speed ensures near-instantaneous response from the user's perspective. The cross-validated classification accuracy reached 98.6%, with an error rate of 1.4%. A confusion matrix summarizes the performance of the kNN algorithm, revealing correct classifications and types of errors.. A whitebox penetration test showed that attackers impersonating valid participants achieved less than 50% accuracy, suggesting that an accuracy threshold above 80% effectively protects against false positive identifications. This test also indicated higher accuracy for attackers resembling valid participants physically (see Figure 10).

Some related works also consider identifying users through tracking data and concerns about VR privacy [28]. For instance, participants engage with 360-degree VR videos and complete questionnaires within the VR environment. Tracking data is processed using three machine-learning algorithms. One limitation, however, is the collection of participant data within a short timeframe, typically around 10 minutes and never exceeding 30 minutes, without removing the headset or resetting the virtual environment. Consequently, some captured features may reflect session similarities rather than individual differences.

Future research could address this by incorporating velocity, acceleration, and rotation data, as demonstrated in previous studies. Additionally, this study focused on tasks involving minimal motion, limiting generalizability to more dynamic VR activities like tennis. Utilizing raw positional time series data and exploring neural network approaches may offer more robust identification features. Further research could investigate inferring demographic information such as gender, age, or VR experience from tracking data to build user profiles.

Finally, the development of privacy-preserving methods in VR data collection and utilization should be prioritized, considering the potential for misuse given the increasing accuracy and abundance of body tracking data in VR environments.

9. Conclusions

To conclude on the aspects of VR hardware resilience and security enhancement we have considered, it is evident that each component—from in-depth analysis of current hardware architecture to user privacy protection in VR environments—plays a crucial role in fortifying the overall system. However, the varied nature of these aspects suggests that a one-size-fits-all solution is impractical.

A comprehensive approach to enhancing VR hardware resilience and security should recognize the unique challenges posed by each aspect. For instance, the in-depth analysis of hardware architecture requires a keen understanding of physical and logical design vulnerabilities, while advanced encryption methods for data security demand robust algorithms and key management practices that are impervious to emerging threats. Similarly, the development of resilient firmware and operating systems calls for a design that can withstand and recover from attacks or failures, and stress testing and vulnerability assessment are paramount in identifying and mitigating potential risks before they can be exploited [29].

An in-depth examination of hardware architecture necessitates a thorough understanding of both physical and digital vulnerabilities, laying the groundwork for targeted enhancements. Implementing advanced encryption is not just about adopting new algorithms; it involves a comprehensive strategy for key management and data protection, adaptable to counter evolving cyber threats.

Developing resilient firmware and operating systems requires a design philosophy focused on durability and recovery, ensuring these systems can resist and bounce back from malicious attacks or technical failures. The role of stress testing and vulnerability assessments is crucial in this ecosystem, acting as a preemptive measure to uncover and address potential weaknesses.

On the hardware front, integrating redundancy and fault tolerance ensures that the VR system remains operational, even when individual components falter. This level of reliability necessitates strategic planning and the incorporation of backup elements ready to take over seamlessly during failures.

Addressing user privacy in VR environments involves a nuanced approach, balancing immersive experiences with stringent data protection standards. This aspect demands constant vigilance and a proactive stance on privacy matters, ensuring users' data is handled with the utmost care and respect.

Ultimately, while there is no silver bullet solution for VR security and resilience, the path forward involves a synergistic approach. Combining various strategies and practices, adaptable to the fast-paced evolution of VR technology, is essential. Collaboration across disciplines—uniting hardware engineers, cybersecurity specialists, and privacy advocates—will foster innovative solutions. By leveraging their collective expertise, a comprehensive, layered security strategy can be devised, offering robust protection against a spectrum of threats and ensuring a secure, reliable VR experience.

Adopting a multi-layered security strategy, continuous system updates, user education on security practices, and adherence to international standards form the cornerstone of this approach. Such a holistic strategy is pivotal in navigating the intricate security landscape of VR, ensuring resilience amid a constantly evolving array of threats.

Hardware redundancy and fault tolerance are essential in ensuring that systems can continue to operate even when parts of the hardware fail. This requires careful planning and the integration of redundant components that can take over in the event of a failure. Finally, user privacy protection in VR environments must navigate the delicate balance between immersive user experience and the stringent requirements of data privacy regulations.

In essence, while there is no universal method that can singularly address all these aspects, the goal should be to develop a suite of complementary methods and practices. These methods should be flexible enough to adapt to the rapid advancements in VR technology and resilient enough to cover most vulnerabilities. Collaboration between hardware engineers, cybersecurity experts, and privacy advocates will be essential in crafting these multifaceted solutions. The intersection of their expertise

can lead to the development of sophisticated, layered security strategies that fortify VR systems against a wide array of threats, thereby ensuring a secure and reliable virtual reality experience.

To enhance VR hardware resilience and security, adopting a multifaceted strategy is essential. A robust VR system should integrate layered security that spans from hardware to application levels, ensuring continuous protection even if one layer is breached. Encryption should be adaptive and hardware-supported for data protection, while redundancy in system design safeguards against component failures.

Regular updates and rigorous testing are crucial for maintaining system integrity against emerging threats. Privacy should be embedded from the onset of system design, respecting user data throughout the VR experience. Additionally, educating users on security best practices, continuously monitoring system activities, and having a swift incident response can greatly mitigate risks.

Compliance with international security standards will guide these efforts, and ongoing research collaborations will help stay ahead of the curve in security advancements. Such a comprehensive approach, without relying on a singular solution, is key to securing VR systems in a constantly evolving threat landscape

10.References

[1] C. Bell, Cloud computing. MicroPython for the Internet of Things: A Beginner's Guide to Programming with Python on Microcontrollers. Berkeley, CA: Apress, 2024. p. 413-424.

[2] G. Markowsky, O. Savenko, S. Lysenko, A. Nicheporuk, The technique for metamorphic viruses' detection based on its obfuscation features analysis. CEUR-WS 2104 (2018).pp. 680–687.

[3] K. Bobrovnikova, S. Lysenko, B. Savenko, P. Gaj, O. Savenko, Technique for IoT malware detection based on control flow graph analysis. Radioelectronic and Computer Systems, 2022(1), pp. 141–153.

[4] S. Lysenko, O. Savenko, K. Bobrovnikova, DDoS Botnet Detection Technique Based on the Use of the Semi-Supervised Fuzzy c-Means Clustering. CEUR-WS 2104 (2018), pp. 688-695.

[5] O. Pomorova, O. Savenko, S. Lysenko, A. Kryshchuk, A. Nicheporuk, Technique for detection of bots which are using polymorphic code. Communications in Computer and Information Science, 431 (2014), pp.265-276.

[6] K. Pyun, J. Rogers, S. Ko, Materials and devices for immersive virtual reality, Nature Reviews Materials 7 (2022). doi: 10.1038/s41578-022-00501-5

[7] T. Riemann, S. Kronin, J. Metternich, Guidelines for the Systematic Selection of Virtual Reality Hardware for Learning Factories, Proceedings of the 12th Conference on Learning Factories (2022). doi: http://dx.doi.org/10.2139/ssrn.4074046

[8] K. Manis, D. Chloi, The virtual reality hardware acceptance model (VR-HAM): Extending and individuating the technology acceptance model (TAM) for virtual reality hardware, Journal of Business Research Vol. 100 (2019) 503-513. doi: https://doi.org/10.1016/j.jbusres.2018.10.021

[9] C. Sagnier, E. Loup-Escande, D. Lourdeaux, I. Thouvenin, G. Vallery, User Acceptance of Virtual Reality: An Extended Technology Acceptance Model, International Journal of Human-Computer Interaction, vol. 36 (11), pp.993-1007, 2020.

[10] M. Otto, E. Lampen, P. Agethen, M. Langohr, G. Zachmann, E. Rukzio, A Virtual Reality Assembly Assessment Benchmark for Measuring VR Performance & Limitations, Procedia CIRP Vol. 81 (2019) 785-790. doi: https://doi.org/10.1016/j.procir.2019.03.195

[11] T. Liu, S. He, S. Huang, D. Tsang, L. Tang, J. Mars, W. Wang, A Benchmarking Framework for Interactive 3D Applications in the Cloud, IEEE/ACM International Symposium on Microarchitecture, MICRO 2020 (2020).

[12] K. Marky, K. Ragozin,K. Kunze, Y. Pai, MazeRunVR: An Open Benchmark for VR Locomotion Performance, Preference and Sickness in the Wild, CHI 2020, April 25–30, 2020, Honolulu, HI, USA (2020). doi: https://dl.acm.org/doi/pdf/10.1145/3334480.3383035

[13] F. Laroche, From semantic reverse-engineering to virtual reality tool box for digital heritage objects, Heritage for the Future, Science for Heritage, A European Adventure for Research and Innovation (2022).
[14] P.P. Tricomi, F. Nenna, L. Pajola, M. Conti, L. Gamberini, You Can't Hide Behind Your Headset: User Profiling in Augmented and Virtual Reality, IEEE Access, Vol. 11 (2023)
[15] R. Du, E. Lee, A. Varshney, Tracking-Tolerant Visual Cryptography, IEEE Conference on Virtual Reality and 3D User Interfaces (VR), Osaka, Japan, 2019, pp. 902-903, doi: 10.1109/VR.2019.8797924.
[16] R. Liu, Q. Zhou, J. Liu, Y. Zhang, Z. Hui, X. Zhang, Separable Reversible Data Hiding in Encrypted Images for Remote Sensing Images, Entropy, 2023, doi: 10.3390/e25121632
[17] F. Ren, X. Shi, E. Tang, M. Zeng, Data Hiding and Authentication Scheme for Medical Images Using Double POB, MDPI Applied Science, vol. 14(6), 2024, doi: 10.3390/app14062664
[18] A. Kapoor, S. Sharma, Implementation of a Virtual Reality Operating System (VROS) for the Next Generation of Computing, 6th International Conference - Cloud System and Big Data Engineering (Confluence) (2016). doi:10.1109/confluence.2016.7508216
[19] U. Izuazu, D. Kim, J. Min Lee, Unravelling the Black Box: Enhancing Virtual Reality Network Security with Interpretable Deep Learning-Based Intrusion Detection System, The 14th International Conference on ICT Convergence, 2023. doi: 10.1109/ICTC58733.2023.10392826
[20] E. Gyamfi, A. Jurcut, Intrusion Detection in Internet of Things Systems: A Review on Design Approaches Leveraging Multi-Access Edge Computing, Machine Learning, and Datasets, Sensors, 2022, doi: 10.3390/s22103744
[21] O. Höft, Ethical Hacking of a Virtual Reality Headset, EECS, p.44, 2023.
[22] D. Harris, J. Bird, P. Smart, M. Wilson, S. Vine, A Framework for the Testing and Validation of Simulated Environments in Experimentation and Training, Frontiers Psychology, sec. Cognitive Science, vol. 11, 2020, doi: 10.3389/fpsyg.2020.00605
[23] S. Riazanoff, A. Corseaux, C. Albinet et al., Best BiCubic Method to Compute the Planimetric Misregistration between Images with Sub-Pixel Accuracy: Application to Digital Elevation Models, International Journal of Geo-Information, vol. 13(3), p. 96, 2024, doi: 10.3390/ijgi13030096
[24] P. Balasubramanian, Analysis of Redundancy Techniques for Electronics Design—Case Study of Digital Image Processing, Technologies, vol. 11, p. 80, 2023. doi: 10.3390/technologies11030080
[25] S. Sakthivel, O. Sathvik Reddy, Fault Tolerant Digital Filters on FPGA Using Hardware Redundancy Techniques and Denoiusing ECG Signals, 2017 International conference of Electronics, Communication and Aerospace Technology (ICECA), 2017, doi: 10.1109/ICECA.2017.8212811
[26] I. Anastasaki, G. Drosatos, G. Pavlidis, K. Rantos, User Authentication Mechanisms Based on Immersive Technologies: A Systematic Review, Information, vol. 14(10), p.538, 2023. doi: https://doi.org/10.3390/info14100538
[27] I. Olade, C. Fleming, H. Liang, BioMove: Biometric User Identification from Human Kinesiological Movements for Virtual Reality Systems, Sensors, 20(10), p. 2944, 2020. doi: 10.3390/s20102944
[28] M. Miller, F. Herrera, H. Jun, J. Landay, J. Bailenson, Personal identifiability of user tracking data during observation of 360-degree VR video, Scientific Reports, 10 (2020).
[29] O. Pavlova, A. Bashta, M. Kovtoniuk, Augmented Reality Based Information Technology for Objects 3D Models Visualization, Computer Systems and Information Technologies,vol. 1, 2023, doi: 10.31891/csit-2023-1-9.