ViKey: Secure Door Access Control Using Passive Visible Light Tags

Jaskirat Sudan*,Fatima Qasem*,Hasky Fynn*†,Fatima Mohammed,Ashwin Sarvadey,Tian Xie‡,Ang Li,Xiao Zhang
University of Michigan-Dearborn, {jsudan, fqasem, fatimamo, sashwink, anglial, zhanxiao}@umich.edu
†Kwame Nkrumah University of Science and Technology, fynnhasky@gmail.com
‡Utah State University, tian.xie@usu.edu

***Abstract*—Door Access Control (DAC) plays a pivotal role in balancing security and convenience in modern infrastructures. However, current vision-based DAC systems exhibit limitations including privacy concerns (e.g., facial data leakage), performance degradation under suboptimal lighting conditions, high computational overhead and system costs. While RFID and Bluetooth-based alternatives exist, they exhibit vulnerabilities to attacks including replay attacks, signal cloning, and eavesdropping. Recent advances in visible light sensing and backscatter communication have enabled promising opportunities for secure, low-power access control systems with sub-dollar hardware costs. In this paper, we propose *ViKey*, the first visible light backscatter-based DAC system that utilizes polarized birefringence to generate 3D position-dependent color patterns as keys, enabling robust and contactless authentication. We design and implement a *ViKey* prototype using commercial off-the-shelf (COTS) components, with a tag cost of less than $0.2. Real-world experiments show that our current ViKey prototype can achieve an average authentication accuracy of 90.5% at 0.5m with our best patterns. These results demonstrate the effectiveness of our low-cost visible light backscatter technology for future smart DAC applications.**

I. Introduction

Modern security employs facial recognition, biometrics, and sophisticated software systems, yet physical locks remain the oldest security method. Dating back over 4, 000 years to wooden locks founded in Assyria's Nineveh, early designs used large wooden keys to lift pins, remarkably similar to modern pin tumbler locks. The Romans revolutionized locks by introducing iron and bronze warded locks [1], [2]. These required precisely notched keys to align with internal wards, which enhanced both security and durability. The design above dominated for centuries and inspired later innovations such as Barron's 18th-century lever lock. As advances in electrical technologies emerged, the growing security demand led to the development of electronic DAC systems. Unlike traditional locks, these systems did not rely on physical mechanisms for access, rather they operated entirely through digital and programmable methods [3], [4]. Reflecting this growing demand, the global access control systems market was valued at USD 8.72 billion in 2020 and is projected to expand at a compound annual growth rate (CAGR) of 8.2% from 2021 to 2028 [5].

Current modern DAC systems support various on-site methods, including keycard readers, PIN pads, mobile-based smart locks, and biometric authentication, which are commonly found in houses, cars, universities, hospitals, and more. Moreover, advanced cloud-based access control systems enable remote entry management. For both on-site and remote modern DAC systems, they provide administrators with granular access control capabilities. Permissions can be instantly granted or revoked from any location, while activity logs track all access events. However, these systems are vulnerable to hacking and unauthorized access when the network and cloud connections are not properly secured.

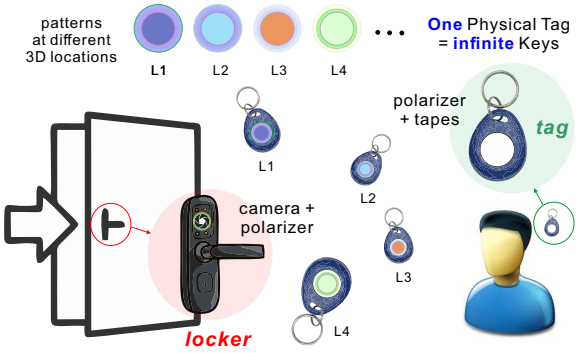

Fig. 1: ViKey is a low-cost yet robust smart door access control system with the core of 3D location-specified patterns. Unlike RFID (Radio Frequency Identification), ViKey offers a near-infinite key solution space while being resistant to replication.

As for biometric DAC systems, they also present unique security challenges. Specifically, fingerprint authentication is one of the most popular biometric-based DAC [6]. Fingerprints minutiae patterns are collected by capacitive or optical sensors, then encrypted before being retained in secure databases. However, fingerprint-based systems remains a critical security risk, particularly eavesdropping attacks. Fingerprint data can be intercepted during transmission or through sensor hardware exploits for cloning. Studies demonstrate that even latent fingerprints can be replicated using low-cost materials such as graphite powder, bypassing live detection systems [7]. The collected biometric data (e.g., fingerprints or facial scans) is highly sensitive and, unlike passwords, cannot be reset if compromised. This permanent vulnerability raises significant ethical concerns and security risks regarding data storage and protection protocols.

To summarize, current DAC systems have two fundamental vulnerabilities: (1) constrained key space, limiting unauthorized credential combinations, and (2) replay attack exposure,

*Co-primary authors, they made equal contribution of this paper.

allowing intercepted credentials to be reused for illegal access. For instance, traditional RFID systems primarily rely on static identifiers with limited combinatorial possibilities, making them vulnerable to brute-force enumeration attacks [8]. Dynamic key-updating mechanisms address this flaw. As demonstrated by [9], RFID tags utilizing cryptographic nonces (one-time random numbers) significantly enhance key diversity while mitigating replay attacks. However, the Non-Line-of-Sight (NLoS) propagation of RF signals inherently exposes all RF-based systems to interception risks, enabling adversaries to eavesdrop or jam communication. The other example is vision-based DAC systems. For example, QR-code-based DAC systems employ 2D spatial patterns, providing larger key space than conventional RFID systems but remaining constrained by static pattern generation. It has been demonstrated that QR codes with predetermined geometric layouts are vulnerable to spoofing attacks, where adversaries can replicate visible patterns using basic printing techniques.

Unlike NLoS propagation of RF signals (e.g., WiFi, Bluetooth, etc.), visible light signals features Line-of-Sight (LoS) transmission, which offers inherent advantages in optical path and spatial positioning [10]–[15]. Within confined spaces, visible light techniques provide inherent resistance to replay and jamming attacks. Besides, the spectrum of visible light signals shares 10, 000 broader than RF signals. Combined with these features of visible light signals and their LoS propagation in 3D space, it is promising to use visible light signals to increase larger key solution space in DAC systems.

There are four key **motivations** behind our proposed new visible light based secure door access control (DAC) framework: **(1)** Current DAC systems suffer from limited key solution space and are vulnerable to replay attacks. **(2)** Other secure MFA solutions are often complex and impose non-trivial costs. **(3)** Utilizing passive visible light signals as keys presents a promising alternative, offering an infinite key space with low cost. **(4)** Even if an attack occurs, the LoS nature of light propagation makes it easier to identify malicious actors.

In this paper, we propose ***ViKey***, a novel and cost-effective approach that first exploits a passive visible light backscatter tag for secure door access control. ViKey requires only affordable polarizers, transparent tapes, and a COTS web camera. As illustrated in Figure 1, there are two polarizers: one mounted in the front of the webcam-integrated door lock assembly, the other affixed to the surface of the 3D-printed key substrate. On top of the key substrate, we layer multiple transparent tapes in concentric interleaved stacking. The camera acquires the distinct color pattern produced by ViKey backscatter tag when positioned at a specific 3D spatial location relative to the lock. The system will check whether this pattern is registered to an authenticated user. If so, it triggers door unlocking.

ViKey operates similarly to an optical Physical Unclonable Function (PUF), relying on the inherent randomness of tape thickness, orientation, placement, as well as the relative 3D location between the tag (key) and the reader (lock). These factors determine how the layered material interacts with polarized light, resulting in a unique pattern signature (invisible to naked eyes) that is extremely difficult to eavesdrop or replicate without exact knowledge of the original configuration.

Even if an attacker intercepts an authenticated user's position and steals that ViKey tag for replication or reuse, it is still hard to duplicate the exact same color patterns. This is because the authentication pattern depends not only on the tag's design but also on the relative positioning of two polarizers in both tag and the camera. Therefore, it is hard to perform a replay attack. Users can further enhance security through either: (1) periodic re-registration of ViKey patterns at novel 3D spatial positions, or (2) complete replacement with newly randomized ViKey designs at minimal cost.

Our **contribution** can be summarized as follows:

(1) This is the **first** work to utilize a passive visible light tag for door access control. By applying polarized light films and multi-layered transparent tapes, we generate location-dependent light patterns that serve as keys to unlock the door.

(2) ViKey explores various design schemes in case study including the number of layers, layering sequence, background colors, and tape shapes to increase the key solution space, ensuring reliable and secure door access control.

(3) We design real-time, lightweight computer vision algorithms to denoise and detect light patterns under varied light conditions and quickly verify whether they match a registered key (i.e., a light pattern from pre-authenticated user).

(4) We implement ViKey tag within $0.2 and ViKey reader with the commercial camera. Experiments show that the system achieves an average authentication accuracy of 90.5% for our best patterns at 0.5m under bright-light conditions.

The rest of the paper is organized as follows. Section II introduces background and the related work. Section III gives the system overview. Section IV-V illustrate visible light pattern generation and vision based real-time unlocking. Section VI presents the system implementation. Section VII and VIII report its performance and conclude the paper.

II. Background and Related Work

In this section, we introduce the background and the related work of our proposed ViKey system including door access control, backscatter, and the comparison between visible light and radio frequency technologies.

A. Door Access Control

There are generally two door access control categories: (1) traditional access control, and (2) electrical access control. For traditional access control, people use mechanical locks and keys, keypad, and physical switch and buttons. As for electric access control technologies, there are magnetic stripe, RFID/NFC, and biometric verification methods (e.g., fingerprint scanning, facial recognition, palm geometry), and Bluetooth/WiFi methods [16]–[18].

The fundamental security mechanisms underlying these door access control methods rely on three core principles: **(1) Unique Identity Verification.** For example, biometric identifiers (e.g., fingerprints) are theoretically and inherently

non-replicable. While tokens in token-based systems are technically replicable, the dynamic nature of these tokens with their short validity periods (e.g., 3 seconds) makes real-time replication practically infeasible, thus maintaining effective unique identification. **(2) Data Encryption.** The difficulty of intercepting or manipulating mechanical lock signals escalates progressively with the dimensional complexity of key patterns, evolving from basic 1D linear grooves to more sophisticated 2D surface contours and ultimately to advanced 3D depth-varying structures. **(3) Permission Management.** The system is designed to restrict access solely to authorized personnel. As an example, laboratory keys (whether mechanical or electronic) are distributed exclusively to verified lab members instead of public accessible, with all access events being recorded in detailed entry/exit logs.

By following the three design principles above, the system significantly raises the bar for attackers attempting to obtain functional keys (pre-attack mitigation). Even if a key is compromised, the system detects the breach in real time and initiates countermeasures (post-attack response).

B. Backscatter

Among existing door access control systems, RFID technology is widely adopted in daily life. It is commonly used for parking lot access, building entry systems, student identification cards, and similar applications. The core of RFID technology is the backscatter principle. Backscatter occurs when propagating electromagnetic waves, acoustic waves, or light waves encounter obstacles and are partially reflected back toward the signal source. When waves interact with obstacles, a fraction of the energy scatters back toward the source, modulated with target characteristics including materials, morphology, and range. In RFID system, the specially designed obstacles, are the RFID tags, which actively modulates the impedance of their antenna circuits. By switching between different resistive loads, the tags alter the characteristics of the reflected signals including the amplitude or phase.

However, these passive tags do not actively transmit signals with their own power supply. Instead, they rely on RF signals from the source (i.e., the RFID reader). As illustrated in Figure 2, the reader emits a continuous RF carrier wave, which provides the necessary energy to the passive tags through energy harvesting. The tags then rectify this energy to power

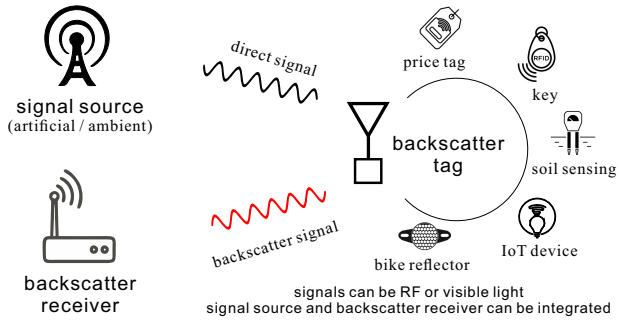

Fig. 2: Backscatter technologies and their applications.

their internal logic. This internal logic controls the modulation of the antenna impedance, allowing the tags to alter the characteristics of the backscattered signal. These modulated reflections carry encoded information, which is sent back to the reader for demodulation and decoding.

Similar to RFID tags, we have developed ViKey, a passive visible light tag that operates without traditional modulation. Instead of encoding bits through wave variations, ViKey controls light propagation characteristics using polarized films and transparent tapes to generate distinctive patterns. The system utilizes ambient light as its source and commercial cameras as readers. Due to the line-of-sight nature of light propagation, the random ambient light combined with the reader's 3D position creates unique backscattered signals with location-specific color patterns, which are the keys for DAC systems.

III. System Overview

There are three main **technical challenges** in ViKey system design and implementation. **C1: visible light backscatter pattern design**. We construct the visible backscatter tag using polarized films and layered transparent tapes. The key challenge lies in comprehensively modeling the light path and pattern generation process through these materials. **C2: extension of pattern space**. To enable secure and large-scale access control, the system must support a vast number of unique and distinguishable patterns as keys. **C3: reliable pattern matching**. Ensuring real-time, accurate pattern recognition under varying real-world conditions including different lighting environments and distances presents significant difficulties. Overcoming these challenges is crucial for guaranteeing reliable access control performance. We elaborate on how we address these challenges in following sections and a system overview here.

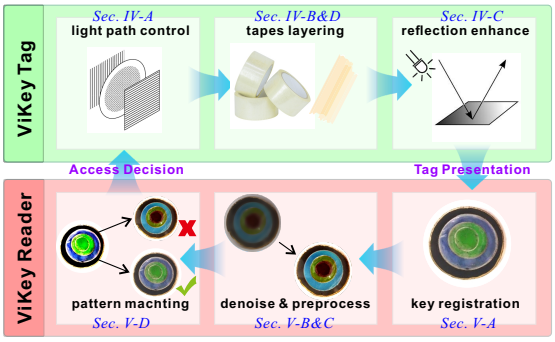

Fig. 3: The overview of ViKey system.

Overview. Our proposed ViKey system is composed of two parts: (1) passive visible light backscatter tag, (2) commercial camera reader, as illustrated in Figure 3.

- **ViKey Tags (Sec. IV):** The ViKey tag is a visible light backscatter based physical key for door access with low cost ($< \$0.2$). It features a white base with a polarizer and transparent tapes (varied numbers, shapes, sequence) layering on it. ViKey tags reflect ambient/artificial light.
- **ViKey Reader (Sec. V):** The ViKey reader utilizes a COTS camera with a front-mounted polarizing filter. The ViKey tag generates a unique visual signature through

polarized light interaction with the reader, remaining invisible to the naked eye without the reader. Functioning as a smart lock, the ViKey reader unlocks doors upon detecting registered tag patterns.

Workflow. The ViKey-enabled door access control system consists of four sequential steps:

1) **Tag Presentation**. The user simply holds the ViKey tag near the reader. While the tag looks normal to the eye, it secretly contains a hidden polarized pattern.
2) **Pattern Activation**. The tag is illuminated by the reader's camera, equipped with a polarizer film, with visible light. This reveals the hidden polarized pattern encoded into the tag's multi-layered structure.
3) **Pattern Verification**. The system verifies the pattern through a real-time computer vision pipeline: **(a)** *pre-processing*: we apply denoising to reduce ambient light interference, including bilateral and non-local means filtering, followed by CLAHE (Contrast Limited Adaptive Histogram Equalization) for contrast enhancement. **(b)** *feature extraction*: we use Scale-Invariant Feature Transform (SIFT) to identify robust key points of the pattern, **(c)** *pattern matching*: we apply Split-Channel Matching to independently extract features from each color channel (R, G, B) for matching. **(d)** *validation*: it is the number of feature matches that need to be strong across the RGB channels so that the system agrees with the pattern as being correct.
4) **Access Decision**. The system grants door access only when both the matched features and geometric confidence exceed **preset thresholds**, and this verification persists for at least 5 consecutive frames (minimum 1 s). Failed attempts trigger an intrusion alarm and capture the face image of the operator for security records.

Infinite solution space of ViKey. As the light path passes through polarized films and multiple layers of transparent tapes, dispersion of the incoming light occurs. While maintaining identical structures and layering of these optical materials, the captured light patterns vary with different viewpoints, as shown in Figure 4. Furthermore, varying structural parameters, including the number of transparent tapes, the angular alignment between polarized films, and the thickness of each tape layer, combined with material stacking configurations (e.g., shapes and sequences) create distinct optical effects. These light-path control variations and resulting pattern diversities within the 3D viewing space collectively establish ViKey's near-infinite solution space.

IV. Visible Light Pattern Generation

In this section, we introduce the design and pre-experiment of the visible-light ViKey tag, along with its working principle.

A. Light Path Control

The ViKey tag comprises three functional layers: (1) a rigid substrate with a single pure color, (2) a bottom polarizer, and (3) birefringent adhesive tapes. As shown in Figure 5, when paired with a top polarizer attached in front of the camera's lens, this assembly creates angle-dependent interference effects. The varying optical path differences (OPD) across the tag produce spatially modulated chromatic patterns that encode 3D positional information. We demonstrate how this polarized birefringence system generates position-dependent color-mixing phenomenon in ViKey's optical design below.

A polarizer is an optical device that converts unpolarized light (e.g., natural light or most artificial light sources) into linearly polarized light by selectively transmitting light oscillating in a specific direction while blocking others. Transparent adhesive tape exhibits birefringence due to anisotropy introduced by the stretching of its polymer structure during the manufacturing process. When polarized light passes through the tape, it splits into two components traveling at different speeds, resulting in an optical path difference given by

$$\Delta L = \Delta n \cdot d, \tag{1}$$

where Δn is the birefringence and d is the effective thickness. When the tape is placed between crossed polarizers, this path difference leads to interference effects that selectively enhance or suppress certain wavelengths. These interference effects result in vivid, position-dependent color patterns.

B. Concentric Interleaved Stacking

We explored various **shapes** for ViKey tag design including circle, triangle, and square. For each shape, we also try different **layer number** of transparent tapes in the set of (3, 4, 5). With each shape, the pattern formed matches the boundary of the shape. Circles create ring-like patterns,

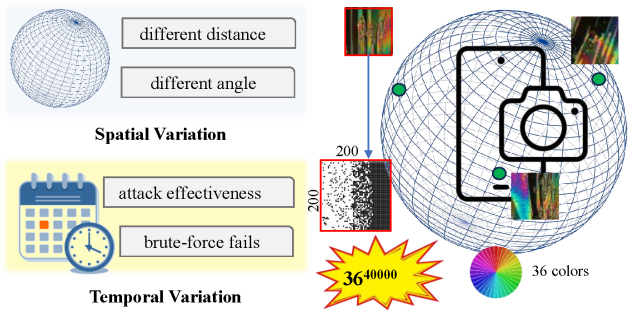

Fig. 4: Infinite key space illustration.

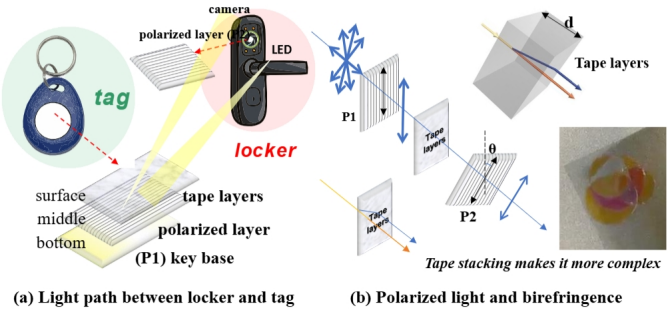

Fig. 5: Light path control and pattern principle.

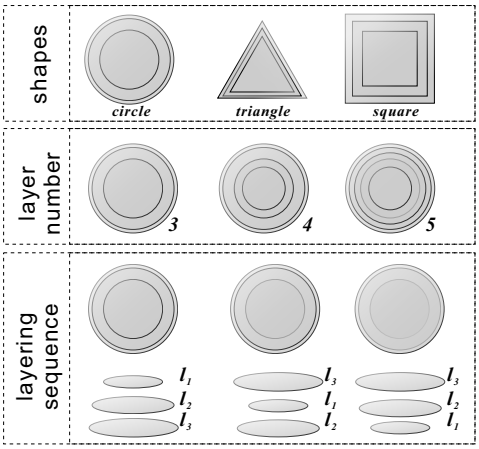

Fig. 6: Layer stacking illustration.

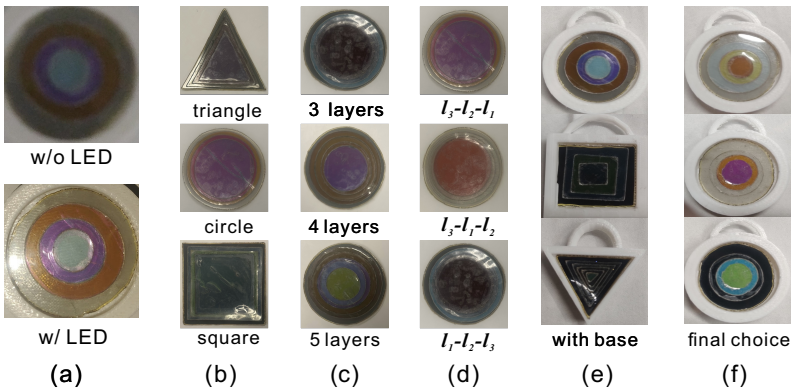

Fig. 7: Case study examples: (a) with/without light enhancement, (b) different shapes, (c) different number of layers, (d) different layering sequence, (e) with white base, (f) different patterns captured with one viKey tag.

squares create square-shaped patterns, and triangles create triangular patterns. The layers used in each shape were all different sizes. Each shape generates patterns that align with its contours: circles produce concentric rings; squares form rectangular borders; and triangles create angular arrangements, as shown in Figure 6. The tape layers can be placed in various **layering sequence starting from the base**: largest to smallest (l_3-l_2-l_1), smallest to largest (l_1-l_2-l_3), or in a different stacking order entirely (l_3-l_1-l_2). Even when the same form is used, the various stacking sequences help to provide varied visual effects. The position and size of each layer influence how light goes through and how the finished pattern appears.

C. Light Reflection and Enhancement

ViKey tags can leverage light from surroundings through multi-layer optical engineering introduced above, creating dynamic anti-tamper patterns without active illumination. The key component to enhance the reflected light is using the high-reflectivity colors such as white for the base and choose the clear transparent tapes to allow the light pass through. Besides, the base reflective layer directs light back through the tape layers, thus nearly doubling the optical path difference. In this way, color saturation and contrast are enhanced, enabling easy pattern recognition even in low light.

To further enhance the light reflection strength, we can also increase the incoming light to the tag by adding an LED on the tag reader side. The LED light intensity can be adjusted based on the optical environment to maintain a good signal-to-noise ratio (SNR). The comparison of the patterns with and without additional light is shown in Figure 7 (a).

D. Case Study

To choose the best design for ViKey tag, we explore different settings and make comparisons below under the same light condition. We present some of these examples for our case study, as shown in Figure 7 (b)-(f).

Different shapes. We explore three different shapes of tag including triangle, circle, and square. We set the base color is white, layer number is 3 and the layering sequence is l_3-l_2-l_1. The different shapes of the tag generate different patterns outlines. As shown in Figure 7 (b), the circle shape has most significant pattern generation while Triangle is the worst and the square shape the similar invisible patterns.

Different number of layers. We also try different number of layers in the range of (3, 4, 5) when we set the base color is white, layering sequence is l_3-l_2-l_1, l_4-l_3-l_2-l_1, and l_5-l_4-l_3-l_2-l_1. The shape is circle. As shown in Figure 7 (c), more layers can generate more pattern information. However, with the limited layers (i.e., 3), but with varied radius combination, it can still generate different patterns.

Different sequence of layering. We test the different sequence of layering when we set the base color as white, the number of layering is 3, and the shape is circle. As shown in Figure 7 (d), the layering sequence (l_1-l_2-l_3) has the most insignificant pattern feature while other two sequences have the similar and more significant features.

After the case study, we choose the design with circle, white base color, 3 tape layers, and random sequences for the following evaluation, as shown in Figure 7 (e)-(f).

V. Vision Based Realtime Unlocking

In this section, we present the design of the tag reader, including key registration, denoising under varying lighting conditions, pattern enhancement schemes, and a lightweight computer vision-based pattern matching algorithm.

A. Key Registration

The registration process of ViKey involves the user holding a specially designed (introduced in Section IV), unique ViKey tag and positioning it in front of the reader, facing the reader. The reader captures the generated pattern and stores it in its local database to serve as a reference for future user authentication. The system extracts circular ROIs using area and circularity filtering from patterns using contour analysis, then preprocesses each region through denoising, contrast enhancement, and resizing to 200×200 pixels. To boost matching robustness, it generates and stores random cropped versions alongside original templates, enhancing authentication accuracy through diversified descriptors.

During the registration process, the user needs to **remember** the 3D spatial position of the tag relative to the reader: the angle between the tag's plane and the reader's plane (i.e.,

two polarizers), the distance between the tag and the reader (z-coordinate), and the relative position (x and y coordinates relative to the center of the reader), as illustrated in Figure 5. Later, using the same tag and replicating the same 3D position, the user can access the door after the reader compares the newly captured pattern with the registered pattern. The user is also required to periodically (e.g., once a month) re-register the key to enhance security: to use the same ViKey tag and select a different 3D spatial position.

B. Denoising Algorithm for Registration

However, due to varying lighting conditions, the captured pattern may not be clear enough (e.g., if the reflected light is too weak or ambient light is too strong), causing the generated pattern to not match the registered pattern, even if the user is in the same 3D spatial position as during registration. To address these challenges, ViKey incorporates a dedicated denoising pipeline as part of its preprocessing flow. The system first applies bilateral filtering to suppress noise while preserving important edges and geometric details crucial for feature extraction. Subsequently, non-local means (NLM) filtering is used to further reduce background noise without introducing significant blurring artifacts. Additionally, contrast enhancement through CLAHE (Contrast Limited Adaptive Histogram Equalization) is employed to normalize brightness variations and improve the visibility of fine structural patterns.

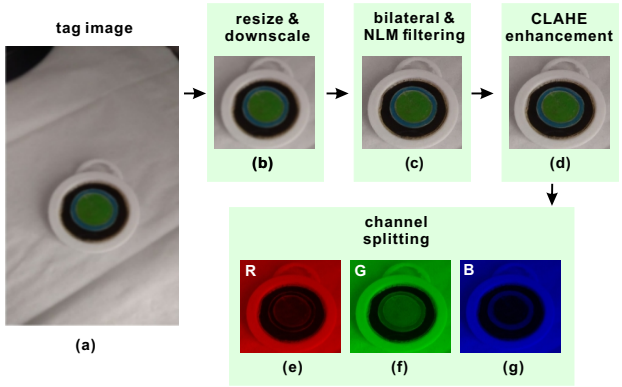

Fig. 8: Denoising in registration and detection at ViKey reader.

C. Pre-processing Flow in Detection

For the detection of the pattern key, the ViKey reader scans the visual pattern on the authentication surface and converts it into a digital format that the system can interpret. This allows the system to compare the pattern with the one saved during registration. The reader uses a camera with a polarizer to capture the tag's area and was developed using Python 3.9, with the OpenCV library (cv2) for computer vision and Tkinter (tk) for the graphical user interface (GUI). Once the pattern detection process begins, the system captures video frames, enhancing each one for analysis. A raw image of the tag area is then obtained and undergoes several preprocessing steps:

(1) Resizing: Every frame is resized to a fixed width and height (200×200) (unit: pixel) to ensure consistent dimensions regardless of camera position or zoom level, and to speed up the subsequent feature extraction process without losing important visual details.

(2) Denoising: In denoising for detection, the resized frame is converted to HSV, where bilateral filtering is applied on the saturation (S) channel and non-local means filtering on the value (V) channel. After merging, the frame is converted back to BGR, and contrast enhancement is performed using CLAHE on the L channel in Lab color space.

(3) Contrast Enhancement: CLAHE (Contrast Limited Adaptive Histogram Equalization) is applied to normalize brightness levels and improve feature contrast.

(4) Channel Splitting: Frames are split into its individual R, G, B channels, and feature extraction is done independently on each channel.

D. Feature-based Pattern Matching

After preprocessing, the system uses the Scale-Invariant Feature Transform (SIFT) algorithm to extract keypoints separately from each color channel. SIFT's robustness to scale, rotation, and lighting changes makes it especially suitable for real-time unlocking with ViKey in dynamic environments. Then, these keypoints are then matched with predefined templates using FLANN and filtered using Lowe's ratio test. A match is accepted if at least five good matches are found across the three channels. To confirm the match, the system calculates a confidence score based on the quality of feature matches and template alignment, using RANSAC to ensure spatial consistency. If the confidence is high, a bounding box is drawn. To improve speed and accuracy, the system uses parameter tuning, frame skipping, region-of-interest (ROI) processing, and parallel processing. These optimizations reduce feature extraction time, increase processing speed, and lower false positives by dividing the workload across multiple threads. The **detailed** major developments are:

(1) Feature Extraction: After capturing a polarized pattern with a polarization-sensitive camera, the image is preprocessed through resizing, denoising, and contrast enhancement (CLAHE) to reduce lighting effects and improve feature clarity. The image is then split into R, G, and B channels, and SIFT is applied independently to each channel to extract robust keypoints and descriptors. These features help make the polarized patterns more distinctive, boosting recognition accuracy in varying conditions.

(2) Feature Matching: To match features in the current image with registered templates, the system applies a FLANN-based matcher independently on each RGB channel. Lowe's ratio test is applied within each channel to reject ambiguous matches [19]. The filtered matches from all three channels are combined, and a match is accepted when the total number of good matches across the channels is at least 5. This multi-channel matching strategy improves robustness under challenging illumination and color conditions.

(3) Geometric Verification: Once sufficient feature matches are found, a geometric verification step is performed using RANSAC to estimate homography. This ensures the spatial consistency of matched features, filtering outliers and aligning

the matched patterns with the real-world pattern, which is crucial for accurate and secure authentication.

(4) Decision and Real-Time Functioning: The decision algorithm calculates a confidence score based on the number of good matches and how well they align spatially. To ensure stable detection, the system requires the pattern to appear consistently for at least 5 consecutive frames. Once stable, a 2-second timer starts. If the pattern remains matched during this time, access is granted. This temporal check helps avoid accidental or brief detections by requiring a steady bounding box. The detection pipeline maintains high frame rates, balancing speed, security, and accuracy.

VI. System Implementation

In this section, we present our implementation of finalized prototype of ViKey tag and the ViKey reader.

Tag. The ViKey tag was designed using 3D modeling and printed in three shapes—circle, triangle, and square—using white filament. However, the square and triangle patterns were unclear with layered tape, so the final design uses only the circle. Each 6mm-high tag has a 2mm-deep cavity that matches the shape and holds the optical components: a polarizing film and three layers of birefringent tape arranged in a shape-specific way. The 1-inch tag is compact and portable, with a half-circle handle for easy keychain use. The ViKey tag prototypes are shown in Figure 9 (a).

Reader. Current ViKey reader prototype comprises two PC-powered components: (1) a camera with an attached polarizing film, and (2) an activation LED that automatically illuminates in low-light conditions. The camera is door-mounted at an ergonomic position for tag presentation, while all image processing (registration, preprocessing, and pattern matching) is handled by the laptop. For eventual real-world deployment, the system can be upgraded to microcontroller-based embedded solutions like Raspberry Pi or BeagleBone.

Cost. The polarizing film with size of 6x6 (inch) is $1.7, which can make 25 polarizer for a tag (the polarizer material for a ViKey tag costs $0.07). One clear tape costs $2.5, which can be used for >100 ViKey tags (tape unit price is $0.025). The 3D printing white filament (1000g) costs $17, can print 160 ViKey tag bases (base unit price is $0.10). The unit price of a ViKey tag is $0.20. The details are summarized in Table I. The ViKey reader (locker) costs more than the ViKey tags (keys), which is the same as other door access systems, and the prices are similar. The current cost (without microcontroller) is less than $20, including a web camera and an LED source.

TABLE I: Components in a ViKey tag.

Component	Price ($)	Details
polarizer	1.7	one film can make 25 tags
clear tape	2.5	can make >100 ViKey tags
white filament	17	can print 160 tags
Unit price	< 0.20	can be cheaper as products

Setup. The authentication process initiates when users present their keychain-compatible ViKey tag to the camera. Then the reader captures the optical pattern immediately, processes the image, and compares it against the registered pattern in the database. The experiment scenario is shown in Figure 9 (b). Upon successful matching, the system authenticates the user and triggers door unlocking. We conducted experiments to evaluate our ViKey system performance with 3 different tags when rotated for 3 different angles, creating 3 patterns for each tag, as shown in Figure 9 (c).

VII. Performance

In this section, we report: (1) recognition accuracy under varied illumination and (2) end-to-end performance. We also discuss about potential attacks and the limitations.

A. Pattern Recognition

ViKey's robustness was also evaluated by testing its authentication accuracy in a matrix of conditions: nine different patterns were used at four different distances from the camera (30, 50, 70, and 90 cm) under three lighting levels (bright, medium, and low). For every combination, the system processed 500 video frames. This produced 108 different accuracy readings. Throughout Figure 10, the impact of the system under various illumination is the main subject. In order to accomplish this, the accuracy results of the four distances for each pattern-light combination were summed up so that the sole effect of ambient light condition on performance can be easily seen.

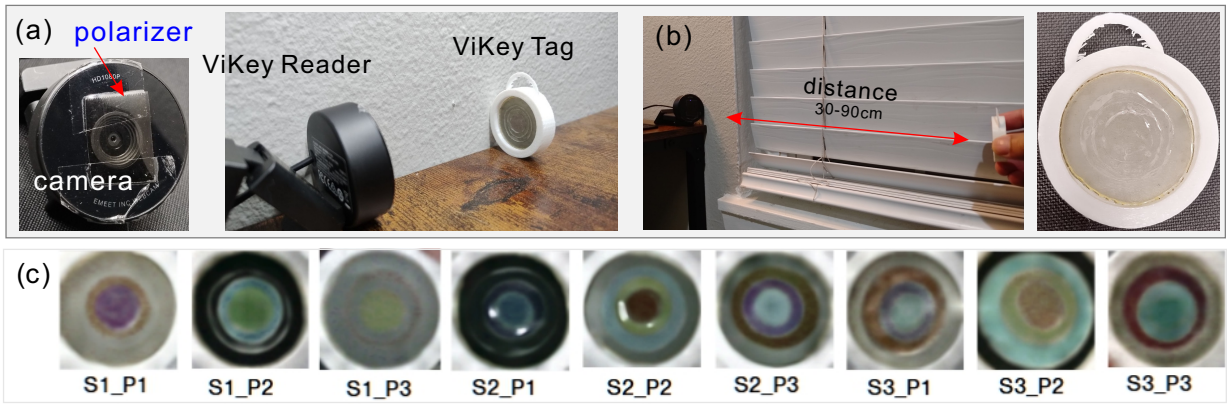

Fig. 9: (a) ViKey tag and reader prototype (b) Experiment scenario (c) Three tag samples (S1, S2, S3) and their three patterns for each (_P1, _P2, _P3) created by rotating them for 3 different angles used for evaluation.

*1) **recognition accuracy under different illumination**:*

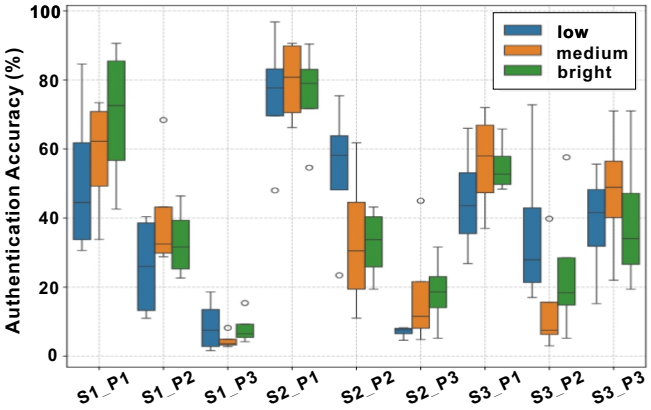

Fig. 10: Box plot of ViKey's accuracy by illumination (each box contains samples under all 4 varied distances mentioned.)

In a situation with intense illumination, some patterns of ViKey are very reliable. More specifically, S1_P1 and S2_P1 show the highest performance with the accuracy of about 80%. Generally, ViKey confirms its strongest performance in high brightness conditions, where the accuracy is usually between 50% and 60% for the majority of patterns.

Darkening of the environment causes the influence of the pattern to be more pronounced on the performance so that the system reveals more fluctuations under medium and low light. It is particularly evident for the patterns such as S1_P3, S2_P3, and S3_P3 which hit the lowest accuracy scores. To give an example, S1_P3 and S2_P3 drop significantly (less than 5%) in some cases. Besides that, certain patterns like S1_P2 and S3_P1 are more stable, providing a more moderate range of accuracy (40–66%) but with the higher level of fluctuations.

On the other hand, a considerable discovery is that, regardless of the intensity of light, a good number of patterns are capable of keeping its accuracy on a high level. For example, S1_P1 is able to keep the accuracy well above 80%, while S2_P2 apparently even beats its performance of bright light, being higher than 75% in the median. It means that the patterns with definitely strong contrast gradients and well-matched polarization responses, such as S1_P1 and S2_P2, would allow more reliable keypoint extraction and matching even in difficult conditions.

*2) **end-to-end latency**:* The system's latency is measured for two primary phases: the registration of new ViKey tags and the real-time authentication process. When a new ViKey tag is introduced, the system goes through a one-time registration process. It begins by resizing, which takes about 0.04 s. Following SIFT algorithm extracts keypoint descriptors in 0.01 s, bringing the total registration time to 0.05 s. Since this is a one-time setup, it imposes no burden on daily use.

Figure 11 presents ViKey's authentication speed across varying distances and lighting conditions. Each subplot corresponds to one distance, with three curves representing performance under different light levels. At 30 cm, ViKey is fastest under low and medium light, with over 90% of authentications completing under 75 ms across multiple patterns (S1_P1, S1_P3, S2_P3). At 50 cm, ViKey performs most consistently across all lighting conditions, with nearly all events finishing below 75 ms, and the curves are steepest here, indicating stable latency. Patterns such as S1_P1 and S1_P3 show particularly fast and consistent results at this distance, regardless of lighting. As the distance increases to 70 and 90 cm, latency spreads out. Under bright light at 70 cm, ViKey achieves about 90% completion within 80 ms, with Pattern 1 and 6 performing best. Performance declines to about 70% under medium light (e.g., S1_P2, S2_P1, S2_P2). At 90 cm, bright light maintains 85% completion (<90 ms), while medium light introduces higher delays, particularly for S2_P1 and S3_P3.

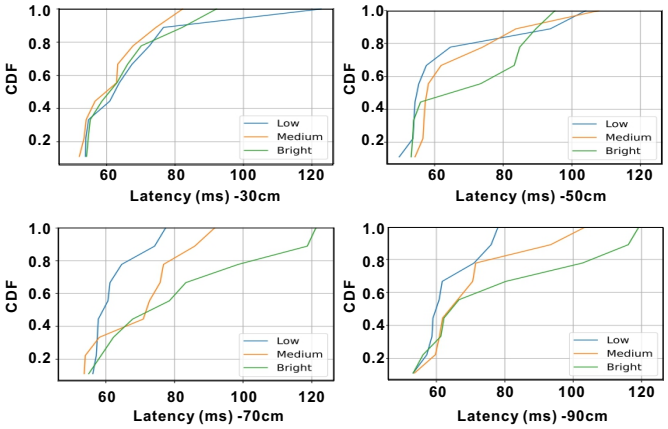

Fig. 11: CDF of ViKey's latency by distances.

ViKey's latency (consistently <100 ms, worst-case 93.7 ms) outperforms existing visible light communication systems (e.g., 500 ms in prior work [20]), representing an 81% reduction. This stems from efficient computer vision algorithms, avoiding deep learning overhead.

*3) **computing overhead**:* To evaluate ViKey's real-world performance in door access systems, we deployed the system in a lightweight Ubuntu 20.04 virtual environment configured with 2 vCPUs and 2GB RAM. While this setup is less efficient and may not meet the resource constraints of common edge devices, such as Raspberry Pi 4 or Jetson Nano, which are typically used in IoT access control applications-it provides a conservative benchmark.

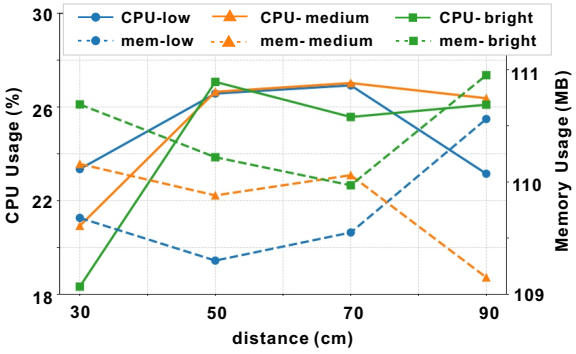

Fig. 12: ViKey's CPU and memory usage measurement.

As shown in Figure 12, ViKey maintains low computing overhead under different lighting conditions and distances.

CPU usage stays below 30% of total system capacity, and memory usage remains stable between 109 MB and 111 MB (normalized to a four-core device). At 30 cm, CPU usage is slightly higher under medium lighting (27%) than in low light (23%), suggesting that dimmer conditions may simplify the visual scene. Interestingly, under bright light at the same distance, CPU usage drops to 18%, indicating that good lighting also reduces processing effort. Memory usage remains consistent across all lighting levels at this distance, ranging from 109.68 MB (low light) to 110.69 MB (bright light). At distances between 50–90 cm, CPU usage remains efficient across all lighting conditions, ranging from 23% to 27%. This shows that ViKey's image processing and pattern matching scale well with distance without increasing processor load. Memory usage also stays steady, mostly between 109 MB and 111 MB, with the highest value (110.95 MB) under bright light at 90 cm. ViKey runs well within the limits of modern edge hardware, thanks to its lightweight computer vision design that avoids resource-heavy deep learning while ensuring accuracy and real-time performance.

B. Potential attacks

1) Eavesdropping: When a user unlocks with ViKey, if an observer records the 3D position of the tag (including distance and angle) and also obtains the tag (by stealing or accurately replicating it), an attack could theoretically unlock the lock. However, accurately capturing the distance, orientation, and especially the angle between the two polarizers is very difficult. If an attacker uses brute-force search, replicating these parameters would take much longer than the normal unlocking time, making the attempt easily detectable by the system, which can trigger a warning or prompt a key change. Changing the key, either by using a new tag or a new 3D position, incurs minimal cost for the user.

2) Deny of Service: An attacker can interfere with the ViKey reader's camera by directing additional light beams toward it, disrupting the capture of the pattern generated by the tag and causing the unlocking process to fail. However, since light travels in straight lines, such additional beams can be easily detected. Therefore, these DoS attacks are easily fail.

C. Limitations

Our current tag prototype is manually made, which affects the accuracy of recognition. In the future, we can use laser cutting to improve the precision of the shape and edges. We will also test the impact of ambient light. The tag cost can be reduced significantly to the level of $0.01 with a better design.

VIII. Conclusion

In this paper, we present ViKey, a visible light backscatter tag enabled door access system that uses polarized films and multi-layered tapes to generate unique location-based patterns for authentication. With the commercial camera and efficient algorithms, it achieves 90.6% at 0.5m, and to achieve 96.8% maximum success rate under bright-light while overcoming privacy and security limitations of existing DAC systems. Its low-cost tapes design creates an unlimited key space, resisting replay and eavesdropping attacks. As the first passive visible-light access solution, ViKey provides a cost-effective alternative to RF and vision-based DAC systems.

References

[1] J. Konicek and K. Little, *Security, ID systems and locks: The book on electronic access control*. Butterworth-Heinemann, 1997.

[2] J. P. Masly, "170 years of "lock-and-key": Genital morphology and reproductive isolation," *International Journal of Evolutionary Biology*, vol. 2012, no. 1, p. 247352, 2012.

[3] W. Alsabbagh and P. Langendörfer, "Security of programmable logic controllers and related systems: Today and tomorrow," *IEEE Open Journal of the Industrial Electronics Society*, vol. 4, pp. 659–693, 2023.

[4] D. Koblah, R. Acharya, D. Capecci, O. Dizon-Paradis, S. Tajik, F. Ganji, D. Woodard, and D. Forte, "A survey and perspective on artificial intelligence for security-aware electronic design automation," *ACM Transactions on Design Automation of Electronic Systems*, vol. 28, no. 2, pp. 1–57, 2023.

[5] G. V. Research. (2023) Access control market size, share & trends analysis report. [Online]. Available: https://www.grandviewresearch.com/industry-analysis/access-control-market-report

[6] Y.-Y. Chen and M.-L. Tsai, "The study on secure rfid authentication and access control," in *Current Trends and Challenges in RFID*, C. Turcu, Ed. Rijeka: IntechOpen, 2011, ch. 20. [Online]. Available: https://doi.org/10.5772/20750

[7] P. Adole, J. M. Mom, and G. A. Igwue, "Rfid based security access control system with gsm technology," *American Journal of Engineering Research*, vol. 5, no. 7, pp. 236–242, 2016.

[8] P. Tuyls and L. Batina, "Rfid-tags for anti-counterfeiting," 02 2006, pp. 115–131.

[9] L. Lu, J. Han, L. Hu, Y. Liu, and L. Ni, "Dynamic key-updating: Privacy-preserving authentication for rfid systems," vol. 2012, 03 2007, pp. 13–22.

[10] X. Zhang, G. Klevering, X. Lei, Y. Hu, L. Xiao, and G.-H. Tu, "The security in optical wireless communication: A survey," *ACM Computing Surveys*, vol. 55, no. 14s, pp. 1–36, 2023.

[11] X. Zhang, G. Klevering, and L. Xiao, "Posefly: On-site pose parsing of swarming drones via 4-in-1 optical camera communication," in *2023 IEEE 24th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*. IEEE, 2023, pp. 67–76.

[12] Y. Yang and J. Luo, "Composite amplitude-shift keying for effective led-camera vlc," *IEEE Transactions on Mobile Computing*, vol. 19, no. 3, pp. 528–539, 2019.

[13] X. Zhang, H. Guo, J. Mariani, and L. Xiao, "U-star: An underwater navigation system based on passive 3d optical identification tags," in *Proceedings of the 28th Annual International Conference on Mobile Computing And Networking*, 2022, pp. 648–660.

[14] X. Zhang, G. Klevering, J. Mariani, L. Xiao, and M. W. Mutka, "Boosting optical camera communication via 2d rolling blocks," in *2023 IEEE/ACM 31st International Symposium on Quality of Service (IWQoS)*. IEEE, 2023, pp. 1–4.

[15] X. Zhang, L. Xiao, and M. W. Mutka, "Holocube: 3d opitcal iot connections via software defined pepper's ghost," in *2024 IEEE 32nd International Conference on Network Protocols (ICNP)*. IEEE, 2024, pp. 1–12.

[16] L. Golightly, P. Modesti, R. Garcia, and V. Chang, "Securing distributed systems: A survey on access control techniques for cloud, blockchain, iot and sdn," *Cyber Security and Applications*, vol. 1, p. 100015, 2023.

[17] S. Parkinson and S. Khan, "A survey on empirical security analysis of access-control systems: a real-world perspective," *ACM Computing Surveys*, vol. 55, no. 6, pp. 1–28, 2022.

[18] S. Dramé-Maigné, M. Laurent, L. Castillo, and H. Ganem, "Centralized, distributed, and everything in between: Reviewing access control solutions for the iot," *ACM Computing Surveys (CSUR)*, vol. 54, no. 7, pp. 1–34, 2021.

[19] M. Muja and D. G. Lowe, "Fast approximate nearest neighbors with automatic algorithm configuration." *VISAPP (1)*, vol. 2, no. 331-340, p. 2, 2009.

[20] S. H. Yoon, K. S. Lee, J. S. Cha, V. Mariappan, K. E. Young, D. G. Woo, and J. U. Kim, "Iot open-source and ai based automatic door lock access control solution," *International Journal of Internet, Broadcasting and Communication*, vol. 12, no. 2, pp. 8–14, 2020.