An Ultra-Lightweight Visual Privacy Protection System for Deep Optical Light Field Imaging Applications

Thesis submitted in partial fulfillment of the requirements for the award of degree of

Master of Engineering

in

Computer Science and Engineering

Submitted By

Abhishek Singh

(Roll No: 802332087)

Under the supervision of:

Dr. Mansi Sharma

Assistant Professor

Dr. Suresh Raikwar

Assistant Professor

THAPAR INSTITUTE
OF ENGINEERING & TECHNOLOGY
(Deemed to be University)

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR INSTITUTE OF ENGINEERING AND TECHNOLOGY

PATIALA – 147004

June 2025

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, **"An Ultra-Lightweight Visual Privacy Protection System for Deep Optical Light Field Imaging Applications"**, in partial fulfillment of the requirements for the award of the degree of Master of Engineering in Computer Science and Engineering submitted in the Department of Computer Science and Engineering at Thapar Institute of Engineering and Technology, Patiala, is an authentic record of my own work carried out under the supervision of Dr. Mansi Sharma and Dr. Suresh Raikwar and refers to other researchers' work which are duly listed in the reference section. The matter presented in the thesis has not been submitted for the award of any other degree of this or any other University.

Abhishek Singh

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

Dr. Mansi Sharma
Assistant Professor

Dr. Suresh Raikwar
Assistant Professor

ACKNOWLEDGEMENT

This project would not have been possible without the help of many people, and it is my pleasure to convey my gratitude to them for their various forms of support, encouragement, and assistance during the project's duration.

I would like to express my gratitude to my supervisors, **Dr. Mansi Sharma** and **Dr. Suresh Raikwar**, for allowing me to work under their capable guidance and for their unwavering support. This endeavor would not have been possible without their assistance and advice. They were the ones who first taught me topics like machine learning and deep learning, as well as provided me with extremely useful insights through regular discussions during this project. Continuous talks have aided me in acquiring a good understanding of this thesis.

I also would like to give my sincere thanks to Dr. Shalini Batra, Head of the Department, and to the entire faculty members of the department for their valuable feedback and suggestions.

Abhishek Singh

ABSTRACT

Light field imaging captures both spatial and angular information from a scene, thus enabling advanced computational photography applications such as post-capture refocusing, depth estimation and 3D reconstruction. Such capabilities make light field data extremely valuable for applications in areas such as healthcare, intelligent surveillance, virtual/augmented reality and robotics. However, 4D light field data is rich and very high dimensional, and it poses enormous threats to visual privacy, especially in sensitive personal or medical information scenarios. Classic encryption schemes are generally unable to handle the unique structure and bulk of the data streams that light fields generate in an efficient manner. In order to address this novel and unreleased threat, this thesis proposes PRESHMAC-256, a hybrid encryption scheme that combines the ultra-lightweight Present block cipher with the cryptographic robustness of HMAC-SHA256. The suggested method is able to encrypt the sub-aperture images extracted from light field captures with 64-bit blocks and with a 128-bit symmetric key derived securely from SHA-256 hashing. The encryption is designed to be lightweight and reversible, claiming a robust level of security with minimum computational and power overhead-an essential requirement for real-time and resource-constrained applications like embedded or mobile devices. The experimental validation carried out using the EPFL Light Field dataset to prove that the presented approach indeed works. Evaluation metrics considered are histogram analysis, information entropy, pixel correlation coefficients, PSNR, SSIM, key sensitivity analysis, occlusion attack resilience and avalanche effect measurements. The findings emerge favoring PRESHMAC-256 as not only ensuring good levels of image security and fidelity, but also decreasing model complexity and processing latency as compared to the traditional encryption schemes. Certainly, this work thus opens possibilities for such an application on the grounds of a fairly practical, highly scalable and secure environment in which data privacy and computation efficiency would both matter significantly.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background and Overview

Light field imaging is an innovative computational photography method capturing both spatial and angular aspects of light rays. In contrast to traditional two-dimensional (2D) cameras that capture only light intensity falling on the image sensor at every pixel, light field cameras can capture the entire plenoptic function—the quantity of light traveling in all directions through all points in space. This creates a four-dimensional (4D) data set in which the spatial location and angle of every light ray determine its description, allowing for a multi-dimensional and very detailed depiction of the visual scene. What really distinguishes light field imaging from traditional imaging is the provision of angular information. In a normal 2D image, every pixel captures information on light intensity in a specific direction, discarding all other directional information. Compared to this, light field imaging systems capture not only where the light is but also where it originated. This extra angular information opens up computational capabilities like digital refocusing, depth estimation, disparity-based segmentation and synthetic viewpoint generation. The description of light fields is commonly given in a two-plane parameterization (also referred to as the (u,v)-(s,t) representation), with the (u,v) plane being associated with the sensor plane and the (s,t) plane being associated with the angular plane or lens plane.The (u,v)-(s,t) representation is a two-plane model to describe light rays for light field imaging. That is (u,v) is the coordinates on the sensor plane—where the light ray hits. The coordinates (s,t) are the angular plane or lens coordinates, representing the direction of the incident ray. The spatial-angular sampling of the light field can thus be seen by way of the arrangement of sub-aperture images in Figure 1.1.

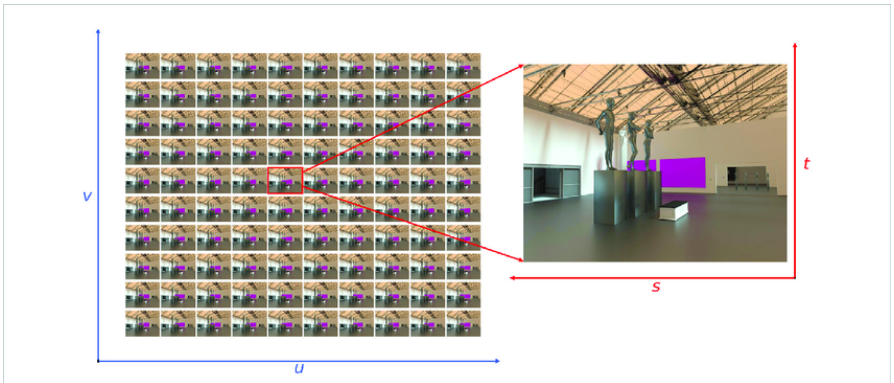

Figure 1.1: Sub-Aperture Image Array in a Light Field.

Recording both spatial and angular data, this 4D representation allows high-level post-processing tasks like refocusing, depth estimation, and novel view synthesis from a single scene recorded in a 4D light field. To obtain this 4D light field data, some specialized devices are used. Two such devices that have gained attention are the Lytro Illum and the Raytrix R8 cameras. The most common method used is the microlens array (MLA)-based camera, in which a microlens array between the sensor and the main lens records spatial as well as angular information in one shot to generate multiple sub-aperture views for sophisticated post-processing such as refocusing and depth estimation. This type of camera places a microlens array between the primary lens and the image sensor. Every microlens records light coming from a different direction, thus one exposure can capture several angular views of one scene. Lytro and Raytrix are instances of light field cameras commercially used with this design. The systems have the ability to successfully compromise angular and spatial resolution based on the microlens layout. The computed light field data is organized as a dense matrix of sub-aperture images, where each is a different view. The sub-aperture images are usually small grayscale or color regions and together comprise a 4D representation of the light field. The fact that such a collection can be analyzed enables algorithms to fake changes in focus, aperture, and viewpoint very much after the image has been taken.Figure 1.2 offers a clear visual representation of the focused light-field camera setup, helping to better understand its structure and functionality.

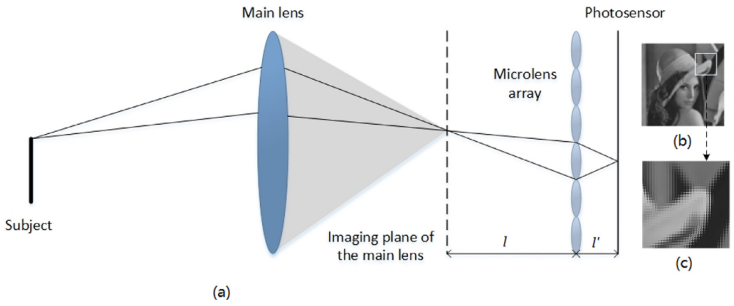

Figure 1.2: Diagram of a focused light-field camera. (a) is a schematic of the structure of a focused light-field camera. (b) is a light field image. (c) is an enlarged view of the square part of (b). (Zhang et al. [10])

The multi-dimensional nature of light field data supports sophisticated image synthesis and analysis operations but also brings challenges. Storage, transmission, and processing requirements are much greater than those of traditional images. Every light field acquisition may generate hundreds of sub-aperture images, leading to exponential growth in the amount of data. Additionally, angular correlations in the light field dataset impose the need upon algorithms to take into account the spatial-angular coherence while performing any kind of operation such as compression, enhancement, and particularly encryption.Figure 1.3 illustrates both the outer appearance and internal

layout of a standard light field camera, giving a clearer understanding of its physical build.

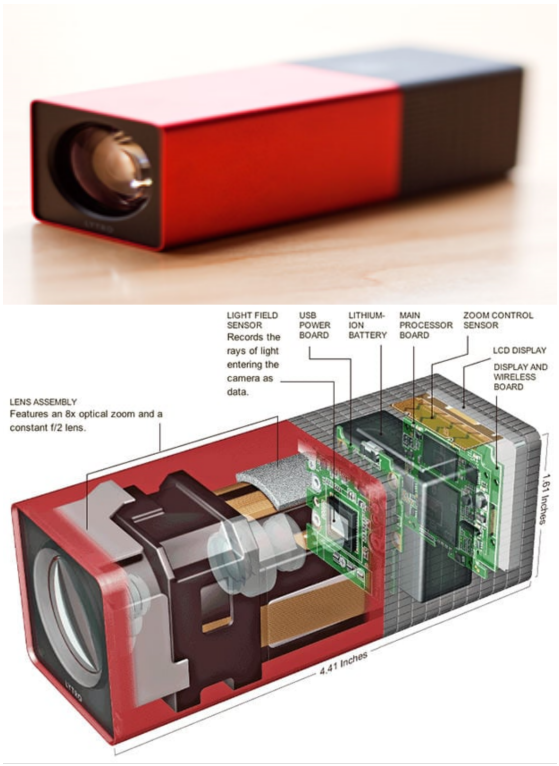

Figure 1.3: External and internal view of a light field camera.

These special features turn light field data into rich information but also a prime target for data privacy protection. The rich angular and spatial details can be manipulated to reconstruct 3D scenes or identify individuals with high accuracy, which brings a concern about unauthorized use or ill-intentioned reconstruction. Hence, maintaining the structural and visual coherence of light field data throughout encryption and decryption is crucial.

1.2 Relevance and Applications of Light Field Imaging

Light field imaging is more than just a research breakthrough; it is quickly becoming a standard component of production systems in the real world across industries. The capability to record, manipulate, and render scenes with angular and spatial accuracy is revolutionizing how we tackle a wide range of technical problems:

- **Medical Imaging:** Light field microscopy provides volumetric imaging of live biological samples. It is useful in examining dynamic processes in three dimensions without mechanical scanning. Applications lie in the field of oncology, neurology, and developmental biology.

- **Augmented and Virtual Reality (AR/VR):** Light field rendering allows true 3D scene visualization with natural depth cues, providing a more realistic and immersive experience. This is critical for next-generation headsets and telepresence systems.
- **Autonomous Vehicles:** Light field-based depth-aware cameras are applied in real-time environment sensing and obstacle detection, assisting vehicles in safe navigation.
- **Security and Surveillance:** Multi-perspective data capture makes it possible to identify and track in intricate scenes, even in the presence of occlusions. This enhances reliability in monitoring systems.
- **Robotics and Industrial Inspection:** Robots equipped with light field sensors can better comprehend object shape and orientation, improving automation accuracy.
- **Computational Photography and Cinema:** Methods such as synthetic aperture refocusing and focal stack synthesis enable photographers and filmmakers to gain post-capture creative control of focus and perspective.
- **Cultural Heritage and 3D Preservation:** Museums and institutions use light field scanning to digitally archive artifacts and archaeological sites, allowing future users to walk through them virtually in 3D.

1.3 Present Block Cipher Overview

The Present block cipher is a lightweight symmetric key block cipher designed purely for severely resource-constrained environments, e.g., embedded systems, IoT devices and wireless sensor networks. It was presented by Bogdanov et al. in 2007 and forms a part of the ISO/IEC 29192-2 standard for lightweight block ciphers. Present uses 64-bit plaintext blocks and accommodates 80- or 128-bit key sizes, and it is well-optimized for high-speed, low-profile encryption. Present differs from other conventional ciphers such as AES, which require more computational power and memory, as it uses a straightforward Substitution-Permutation Network (SPN) structure made up of three basic operations: bitwise XOR (AddRoundKey), nonlinear substitution through 4-bit S-boxes, and fixed permutation layer (P-layer) that provides good diffusion. These elements are repeatedly used in 31 rounds so that the cipher is resistant to linear and differential attacks while hardware and computational costs remain low. In this thesis, the Present cipher was chosen because of its perfect harmony between cryptographic security and lightweightness so that it is best suited for encrypting grayscale sub-aperture

images within a light field dataset. Because every light field capture is capable of producing a substantial amount of sub-aperture images (e.g., 13×13 or higher), encrypting the volume of data should be done using an algorithm that minimizes power as well as processing overhead without sacrificing security. Present's low gate count (<2,000 GE) and 8-bit microcontroller as well as FPGA-friendliness make it a prime candidate. Moreover, the deterministic and regular structure of Present also simplifies parallelization and hardware-accelerated implementations. We can see in Table 1.1 summarizes the popular block-stream ciphers and similar parameters among them in the aspect of the hardware implementation efficiency. The key parameters of this table include size of the key, block size and the number of processing cycles per block, throughput at a nominal operating frequency of 100 KHz, logic process technology (node of a logic process in μmm) and implementation area, all represented in GE and relative to the area.

Table 1.1: Comparison of Block and Stream Ciphers (adapted from Bogdanov et al.[15]

	Key size	**Block size**	**Cycles per block**	**Throughput @100KHz (Kbps)**	**Logic process**	**Area**	
						GE	**rel.**
Block Ciphers							
PRESENT-80	80	64	32	200	0.18μm	1570	1
AES-128 [16]	128	128	1032	12.4	0.35μm	3400	2.17
HIGHT [22]	128	64	1	6400	0.25μm	3048	1.65
mCrypton [30]	96	64	13	492.3	0.13μm	2681	1.71
Camellia [1]	128	128	20	640	0.35μm	11350	7.23
DES [37]	56	64	144	44.4	0.18μm	2309	1.47
DESXL [37]	184	64	144	44.4	0.18μm	2168	1.38
Stream Ciphers							
Trivium [18]	80	1	1	100	0.13μm	2599	1.66
Grain [18]	80	1	1	100	0.13μm	1294	0.82

PRESENT-80 is one of the block ciphers for lightweight applications with the best area efficiency-performance tradeoff. It has a small hardware requirement of 1570 GE, moderate speed of 200 Kbps, and 0.18 μm process implementation. It is a good candidate for resource-poor settings. Stream ciphers such as Trivium and Grain have comparable area efficiency but are limited to single-bit blocks, having only 100 Kbps throughput. The "Area" metric, which is further split into Gate Equivalent (GE) and relative area, offers a reasonable benchmark across various logic technologies. Such a comparison facilitates the selection of ciphers that suit particular application requirements, particularly where hardware expense and energy efficiency are paramount. Its flexibility to work with 64-bit block operations naturally fits in with the block-based encryption strategy used in this thesis, which can be directly integrated with the encryption pipeline for 4D light field data visual privacy preservation.

1.4 Overview of HMAC-SHA256

SHA-256 (Secure Hash Algorithm 256-bit) is a cryptographic hash function in the SHA-2 family, developed by the National Security Agency (NSA) and standardized by NIST. It produces a 256-bit fixed-length output from an input of arbitrary length, and is extensively used for data integrity, digital signatures, and secure key generation. SHA-256's mathematical design is based on bitwise logical operations, modular additions, and compression functions that alter the input data through 64 rounds of computation. Its rich avalanche effect makes it so that a one-bit change in input significantly changes the output, making it highly resistant to preimage, second preimage, and collision attacks.As shown in Figure 1.4, the SHA-256 hashing process transforms input plaintext into a fixed-length secure hash, ensuring data integrity and authenticity.

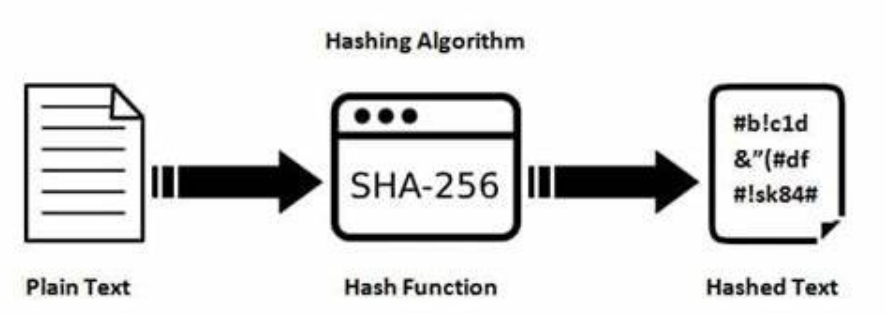

Figure 1.4: SHA-256 hashing process converting plain text into secure hashed output.

Unlike most checksum functions, SHA-256 is computationally secure and cryptographically robust and thus is a fundamental component of secure systems today. SHA-256 is utilized, in the context of this thesis, not for encryption but rather for secure key derivation using HMAC (Hash-Based Message Authentication Code). By mixing a user-specified base key with a salt and hashing it through the SHA-256 hash function, a high-entropy 128-bit key is generated to be used in the Present encryption algorithm. This makes the used keys not only unpredictable but also unique for every session or user-specified input, largely enhancing the security of the system.The hybrid of SHA-256 and Present therefore creates a hybrid encryption model where SHA-256 can offer cryptographic randomness and brute-force and dictionary attack protection, and Present offers efficient block-level data protection. This hybrid—PRESHMAC-256—is especially potent for use in applications such as light field image encryption where both speed and security are essential. This thesis presents PRESHMAC-256, a lightweight and effective hybrid encryption scheme for securely encrypting light field sub-aperture images. Through the combination of PRESENT block cipher with HMAC-SHA256-based key generation, the scheme facilitates block-wise encryption while being in accordance with the structural needs of light field data. The aim is to provide a strong solution to the twin challenge of preserving angular-spatial integrity and gaining com-

putational effectiveness in limited resource settings.

1.5 Research Motivation

While light field imaging has huge advantages, the sensitivity and extent of the data pose serious privacy and processing issues. Established encryption schemes like AES or RSA, while secure, are not well-suited for block-wise, multi-view character of light field data. Moreover, their computational expense makes them unfeasible for real-time systems or devices with constrained processing capabilities, like IoT sensors and mobile. Conversely, optical encryption methods such as Double Random Phase Encoding (DRPE) and chaos-based techniques, despite being innovative, tend to demand intricate optical setups or have limited scalability to high-dimensional digital data. Furthermore, they could fail to guarantee the structural integrity of light field datasets during encryption and decryption, particularly when sub-aperture images are required to be angularly coherent. There is a wide gap in the literature for a reversible, lightweight, and secure encryption algorithm that can be used effectively with sub-aperture images in light field datasets. Besides this, an increasing necessity is to face the security-specific challenges of light field data. These are the threat of visual information leakage via angular correlations, side-channel attacks using identifiable patterns in light field representations, and illicit reconstruction of 3D structures from incomplete data. Furthermore, the richness and high resolution of light field content make it more vulnerable to privacy invasions, particularly in applications like medical diagnostics and surveillance. Thus, protection of data confidentiality, integrity, and invulnerability to contemporary cryptographic attacks is all the more critical. Such a solution needs to provide:

- Cryptographic strength high enough to be resistant to statistical, differential, and brute-force attacks.
- Low computation overhead so as to work with real-time processing.
- Block-level scalability for working with large amounts of sub-aperture data.
- Integrity of the image so as to facilitate accurate decryption and usability of reconstructed light fields.
- Protection from structural exploitation that would allow reverse engineering or partial reconstruction of the original scene.

1.6 Overview of the Proposed Scheme: PRESHMAC-256

This thesis introduces PRESHMAC-256, a hybrid encryption scheme well-suited to the needs of contemporary light field imaging systems. By combining the Present block

cipher, which is power-efficient and hardware-friendly, with an HMAC key derivation scheme that uses SHA-256, the proposed scheme guarantees strong symmetric encryption. The process works as follows:

- Extract grayscale sub-aperture images from the light field representation.
- Flatten each sub-aperture image into 64-bit blocks.
- Generate a 128-bit encryption key using HMAC-SHA256 hashing.
- Encrypt each block using the PRESENT cipher with 30 iterative rounds of substitution, permutation, and key mixing.
- Reconstruct the encrypted dataset while preserving spatial-angular consistency.

The decryption process is a copy of the encryption pipeline to maintain full reversibility and visual quality preservation. Measures of evaluation including entropy, uniformity of the histogram, pixel correlation, PSNR, SSIM, key sensitivity (NPCR and UACI), and avalanche effect affirm the effectiveness of the scheme in offering visual privacy protection with no impairment in data usability. The rest of this thesis is based on this, and Chapter 2 gives a thorough overview of related work in light field image encryption and lightweight cryptography.

Chapter 2

Literature Review

Wei et al. [1] highlighted that the light field images enable excellent features such as post-capture focusing, depth perception, and 3D scene reconstruction, providing immersive representation of the environment. As a seamless transition, light field displays project multi-directional light rays, letting viewers perceive depth and parallax without the need for special glasses. The light fields have unlocked potential applications in virtual and augmented reality (VR/AR), medical imaging, surveillance, and various navigation systems. Light field visual privacy is important because light fields capture a lot more visual information than regular images or videos. The ability to rebuild precise 3D models of surrounding raises concern about unauthorized access and abuse, particularly in sensitive industries like healthcare and surveillance. Current security solutions usually fail to address the visual privacy issues associated with light field data, requiring the development of lightweight yet efficient privacy protection technologies. This paper aims to create an ultra-lightweight visual privacy protection system for light field imaging.

Wu et al. [2] integrated strong data processing methods with secure encryption techniques, the system attempts to protect privacy while maintaining the real-time capabilities required for modern light field applications. Traditional encryption algorithms were not built to handle the volume and complexity of light field data. Wang et al. [3] explained that light field pictures are made up of sub-aperture views that collect both angular and spatial information, which increases data volume and sensitivity. Kocarev et al. [4] suggested methods like chaos-based cryptography and transform-domain encryption. However, such approaches are computationally expensive, difficult to scale, and incompatible with real-time processing requirements. To overcome these restrictions, we have developed an ultra-lightweight visual privacy protection technique for light field imaging. Our technique makes use of the proposed block cipher, a basic and hardware-efficient encryption algorithm aimed at restricted-resource systems. We develop a secure and efficient encryption technique customized to the structure of light field data by performing block-wise encryption on sub-aperture images and generating keys with a SHA-256-based algorithm.

Wang et al. [5] stated that traditionally designed hash function SHA-256 are using simple nonlinear logical operations. Viola et al. [6] emphasized the growing need for efficient light field image encryption methods that can ensure privacy without imposing heavy computational costs. The proposed approach delivers a secure yet lightweight solution, making it particularly effective for real-world applications such as intelligent

surveillance, healthcare imaging, and portable camera systems. For image security applications, there are two categories of encryption approaches: optical encryption based methods and light field image encryption based methods. Optical encryption methods such as Double Random Phase Encryption (DRPE) which is presented by Faragallah et al. [7], fractional Fourier transform, and chaos-based encryption methods are mainly concerned with the security of two-dimensional (2D) images by utilizing the physical behavior of light fields and complex mathematical transformations. These methods work well for standard images, but are restricted for other more complex forms of data. Opposed to this, the light field image encryption methods are designed according to the inherent structure of light field images, which involve spatial and angular information together. Owing to higher dimensional light field structure, simple encryption methods based on single image are not suitable for the light field data. The spatial-angular dependencies require specific encryption methods to process multiple viewpoints in parallel for security and maintaining integrity of the data.

Lima et al. [8] indicated that light field imagery demands encryption schemes for tackling the complexity of spatial and angle management at once. Simultaneous encryption in space and angle through the method based on DFrFT coupled with Arnold transform offers improved robustness with respect to statistical attacks, but retains image integrity. Chaotic-based cryptography methods, such as the one demonstrated in study by Wei et al. [9], recently gained the spotlight, using logistic maps and double random phase encoding (DRPE) for scrambling those images so that no one can easily decrypt them in a straightforward manner. Zhang et al. [10] also contribute a gravity model technique, whereby sub-aperture images were fused into a single light field frame before being secured against an encryption scheme, thereby increasing the effectiveness of the method against occlusion attacks. Significant efforts are still required to develop encryption systems that are reliable, reusable, lightweight, and efficient for application with light field images. You et al. [11] proposes a complex encryption algorithm specifically designed for 3D color light field images. The suggested technique has great key sensitivity, good statistical security, and resistant to occlusion attacks. The experimental results suggest that encrypted data may be successfully reconstructed with varied focus lengths. Overall, the technology represents a possible choice for safe light field picture encryption in visual privacy applications.

Wen et al. [12] describe a safe encryption method meant particularly for 4D color light field images (LFI), which vary from natural pictures in respect to angular and spatial information. Experimental findings show that the scheme is very secure, resistant to differential and statistical attacks and preserves the visual quality of the original light field data. The approach has been shown to be resilient and appropriate to complex picture protection. Shao et al. technique [13] presents a hierarchical compression-encryption approach designed for light field pictures which uses multi-view image pro-

cessing. They used ZUC algorithm, chaotic systems, and pixel diffusion techniques. Experimental results show that the technique has a high compression efficiency while being highly resistant to statistical, differential, and noise. The light field is first divided into residual and center views using a predictive structure, then compressed using HEVC encoding and sequentially encrypted with ZUC. The encryption approach for 4D light field considered both spatial and angular domain properties, as compared to previous methods that only considered spatial elements. The results show that the suggested technique is effective, secure, and appropriate for LF data security. The paper also identifies potential future improvements, such as adaptive feature weighting and encryption during the camera acquisition step.

Niwa et al. [14] introduced a method for image encryption that utilizes light field encoding, leveraging the intrinsic visual characteristics of the individual visual system. The experimental findings indicate that unauthorized individuals are unable to view the designated image, thereby safeguarding privacy and controlling access to information. In this paper, we introduce an innovative hybrid encryption framework known as PRESHMAC-256, which integrates the lightweight Present block cipher with HMAC-SHA256 [15, 16, 17] to provide a secure, efficient, and robust solution for the protection of light field images. The proposed hybrid approach allows for strong key generation and lightweight encryption.

Chapter 3

Research Problem Statement

3.1 Research Problem

The advancement of light field imaging has brought forth a new era in visual information capture by enabling the acquisition of spatial and angular data from a scene. This high-dimensional data enables applications such as depth estimation, digital refocusing, and 3D reconstruction. However, it also raises significant challenges related to storage, processing, and most importantly, privacy protection. As the use of light field imaging becomes more widespread in sensitive fields such as medical imaging, surveillance, and augmented reality, safeguarding this data against unauthorized access becomes a matter of critical importance.

3.2 Gap Analysis

The key gaps identified in existing encryption methods for light field data are as follows:

- Current encryption algorithms, such as AES and RSA, were not designed with the complex structure and volume of light field data in mind.These techniques generally operate on 2D images or linear data streams and are optimized for traditional visual media.
- While effective for conventional image formats, the methods like AES become inefficient and impractical when applied to 4D light field data due to their inability to maintain spatial-angular consistency and their significant computational overhead.
- Additionally, optical encryption methods like Double Random Phase Encoding (DRPE), fractional Fourier transforms, and chaotic systems have been explored in literature.Although these approaches offer innovative techniques for encryption, they are typically limited to laboratory settings or static scenes due to high computational complexity, hardware requirements, or lack of real-time applicability.
- The encryption schemes like RSA often fail to address the integrity and reversibility requirements of encrypted subaperture images, leading to potential data degradation or loss of angular fidelity.

- Further, recent light field-specific encryption methods such as DFrFT-based algorithms or multi-view chaotic schemes have achieved improved performance in terms of robustness and statistical security. However, these methods often come at the cost of increased computational demand, making them unsuitable for deployment in real-time, embedded, or mobile environments where resources are constrained.

- The current methods underscore the pressing need for a secure, lightweight, and structurally compatible encryption framework tailored for light field data.

3.3 Statement of the Problem

The central problem addressed in this thesis is the lack of a lightweight, secure, and structurally coherent encryption framework for grayscale sub-aperture images in light field datasets. Traditional encryption methods fall short when applied to 4D data due to their incompatibility with spatial-angular structures and their resource-intensive processing demands. Thus, the research question this thesis aims to answer is: "How can we design a lightweight hybrid encryption algorithm that ensures security and integrity for grayscale sub-aperture images in light field datasets, while remaining computationally efficient and suitable for real-time, resource-constrained environments?" This problem involves achieving a balance between strong cryptographic properties (such as resistance to statistical and differential attacks) and maintaining the angular-spatial coherence that is essential for the utility of light field images.

3.4 Justification from Literature Review

As analyzed in Chapter 2, the literature reveals that while there are several encryption schemes proposed for visual data, very few specifically address the encryption of 4D light field images. The reviewed works demonstrate limitations in scalability, reversibility, hardware dependence, and real-time feasibility. For example, chaos-based systems provide high confusion and diffusion but tend to be unstable in noisy environments or require complex key generation and synchronization mechanisms. Optical schemes often depend on physical hardware setups, limiting their practicality. Even recent light field-specific models, although promising, lack adaptability to constrained platforms and fail to preserve the full integrity of angular information. The PRESHMAC-256 framework proposed in this thesis directly addresses these gaps. It introduces a hybrid model that combines the Present block cipher, known for its hardware-friendly and low-resource nature, with a secure HMAC-SHA256-based key derivation method. This design ensures block-wise encryption with minimal overhead, offering a viable encryption solution specifically tailored for grayscale sub-aperture images.

3.5 Significance of Solving the Problem

Solving this problem has substantial practical implications. As light field imaging becomes integral to applications in real-time systems—such as medical diagnostics, surveillance, robotics, and AR/VR—ensuring visual privacy and data integrity becomes paramount. Developing an encryption system that provides robust protection without compromising performance enables broader adoption and safer deployment of light field technologies in sensitive environments. Moreover, the ability to securely store and transmit light field data without violating privacy policies or regulatory requirements will be crucial for the long-term success of this imaging paradigm. A lightweight encryption scheme also makes it feasible to incorporate security directly into embedded systems and edge devices, reducing reliance on centralized or cloud-based encryption mechanisms.

Chapter 4

Methodology

4.1 Overview

This chapter presents an overview of the method used to develop a solution to the research problem of designing a lightweight secure encryption scheme for light field sub-aperture image data. The section presents the conceptual basis, algorithmic structure, and encryption-decryption implementation procedures. It is to provide an example of how the research goals were achieved through systematic design and implementation procedures.

4.2 Light Field Image Dataset

The experimental dataset for testing the designed encryption scheme is the EPFL Light Field Dataset, which consists of light field images in high resolution of real scenes. Specifically, we use the "Bikes" image set of a 13×13=169 sub-aperture images. Each sub-aperture image is a single distinct angular view of the scene, recorded in a microlens array configuration. The images are cropped in uncompressed format and are converted to grayscale before encryption to avoid data dimensionality and computational costs. Every sub-aperture image in the data set is 625×434 pixels in dimensions, and it is vectorized as a 1D array for block-wise encryption. Padding is done for block compatibility with the cipher design to make the array length a multiple of 64 bits.

4.3 The Hybrid Encryption Scheme Design

The suggested encryption scheme, PRESHMAC-256, combines two cryptographical elements:

- Present Block Cipher (for lightweight symmetric encryption)
- HMAC-SHA256 (for secure key generation)

The combination of the two approaches allows secure, efficient block-wise encryption that preserves the structural integrity of light field sub-aperture data with real-time complexity.

4.4 Integration of Present and HMAC-SHA256

The hybrid model works as follows:

1. **Key Generation:** SHA-256 is applied on the concatenation of an 80-bit base key and salt to produce a 128-bit symmetric key.

2. **Block Processing:** Each sub-aperture image is converted to grayscale, vectorized, and segmented into 64-bit blocks.

3. **Encryption:** Each block is encrypted using the 128-bit key in the 31-round Present cipher pipeline.

4. **Reconstruction:** The encrypted blocks are reassembled to reconstruct the encrypted image.

This integration provides a strong trade-off between security, speed, and structural compatibility, ensuring the encrypted output preserves image dimensions and angular relations .

4.5 Encryption Process

Light-field images with 13 × 13 matrix, i.e., 169 sub aperture images were chosen. All the images first turned into grayscale images, and then encryption process starts using the proposed PRESHMAC-256 algorithm. The following process was adopted to encrypt the light field data:

Step 1: Vectorization of Sub-Aperture Images

Let $I(s,t)$ be a sub-aperture image at angular coordinates (s,t), where $s \in \{1,2,...,13\}$ and $t \in \{1,2,...,13\}$. The image is first reshaped into a one-dimensional array as given in Eq. 4.1:

$$I_{vec} = Vectorize(I(s,t)) \tag{4.1}$$

where, $Vectorize(I(s,t))$ rearranges sub-apertures in a columnwise manner to flatten into a sequence of pixels without applying any changes to any particular rows or columns. This vectorization enables efficient block-wise processing in the proposed scheme as illustrated in Fig. 4.1.

Step 2: Zero-Padding for Block Alignment

The processing works on 64-bit (8-byte) blocks. Consequently, the vectorized image data must be divided into blocks of equal size. If the length of the vector I_{vec} not divisible by 64, zero padding was appended to ensure that Eq. 4.2 is satisfied:

$$Length(I_{vec}) \equiv 0 \ (mod\ 64) \tag{4.2}$$

This keeps the block size equal and allows a secure transformation during encryption. The padded vector is then divided into n blocks $\{P_1, P_2, ..., P_n\}$, each containing 64 bits.

Step 3: SHA-256 Key Generation

The encryption method under discussion uses 128 bit key, which is the original key. The key was then combined with the SHA-256 cryptographic hash function and the new key generated to strength and enhance the security of the encryption process. SHA-256 based key expansion is a secure cryptographic hashing function that maps the data to a fixed 256-bit output. SHA-256 was chosen because even a small change to the input produces a completely different hash with large mathematical distinction. In the proposed algorithm, the original key is input into SHA-256 to yield a 256-bit hashed value as mentioned in Eq. 4.3:

$$K_{temp} = SHA256(\text{original key}) \tag{4.3}$$

where, K_{temp} represents 256-bit key obtained from Eq. 4.3. This offers increased randomness and unpredictability with respect to the original key, thereby giving an enhancement in the strength of the encryption. The encryption algorithm uses a 128-bit key, therefore, only the first 128 bits of the SHA-256 output are taken into consideration through Eq. 4.4:

$$K_{final} = K_{temp}[0:15] \tag{4.4}$$

where, [0:15] in Eq. 4.4 represents first 16 blocks of the K_{temp}. Thus, K_{final} will be a 128-bit key. The 128-bit key is then fed into the round key generation procedure embedded inside the algorithm for seamless and efficient encryption processing. Every 64-bit data block P_i from sub-aperture image has to undergo a defined set of transformations that shall incorporate substitution, permutation, and key mixing on it. This will ensure that the output would depend on both the content and the secret key in most complex ways. Fig. 4.1 shows the process steps.

Step 4: Initial Key Mixing

An initial key combination stage is applicable to each block prior to its introduction into the main transformation rounds.

$$S_0 = P_i \oplus K_0 \tag{4.5}$$

where in Eq. 4.5, P_i is the i-th block of the input plaintext with padding K_0. K_0 is the initial key derived from the 128-bit K_{final}. Here key $\oplus$ denotes the bitwise XOR op-

eration. The block is bounded with the K_{final} key ensuring that encryption is sensitive to changes in the key. Thus, every block is passed repetitively through 30 rounds of transformations, where in each stage, the same fundamental operations manifest with round-specific keys.

Step 5: Substitution of the Grayscale Image

In this stage, small piece of data (known as a nibble, which is 4 bits or 1 hex number) is replaced with another fixed value using Eq. 4.6:

$$S_j^{(1)} = \text{SBox}(S_{j-1}) \tag{4.6}$$

In this process of substituting, each block of the plain text is made to go under confusion in such a way as to render a pattern in the image less detectable after encryption. Eventually, this makes it very hard for an attacker to guess the original content.

Step 6: Permutation of the Grayscale Image

At this point in the process, the positions of each nibble (4-bit segment or 1 hex character) are rearranged in the current state. This rearrangement helps to mix up the data by dispersing values from nearby pixels throughout different sections of the block. This reduces observable patterns, making the encrypted image look more random. Eq. 4.7 helps in this permutation using a permutation $\pi(i)$ of the i-th bit.

$$S_j^{(2)}[\pi(i)] = S_j^{(1)}[i] \tag{4.7}$$

where, for each i, $\pi(i)$ indicates where the i-th nibble from the first state $S_j^{(1)}[i]$ should be placed in the second state $S_j^{(2)}[\pi(i)]$. This step does enough mixing across the block, thereby, eliminating local pixel correlations (Fig. 4.1). The rearranged state is then combined with a round-specific key using the XOR operation using Eq. 4.8:

$$S_j = S_j^{(2)} \oplus K_j \tag{4.8}$$

Each round uses a unique subkey K_j, which is derived from the K_{final} key through a rotation and transformation routine embedded in the algorithm. After the round key mixing, the key for the next round is generated by applying the key update function as shown in Eq. 4.9:

$$K_{j+1} = f(K_j) \tag{4.9}$$

where, $f(K_j)$ is defined in Eq. 4.10:

$$f(K_j) = Rotate(K_j) \oplus Constant \oplus SBox(K_j) \tag{4.10}$$

This operation updates the key for the next round based on the previous key K_j.

Step 7: Final Round Key Mixing

After 30th round of encryption is completed as illustrated in Fig. 4.1(a). The final step do not involve modifying values (replacement) or rearranging places (permutation). This was done in previous rounds. However, there is the last round key mixing in which the data is mixed with the round key together once again as seen in Eq. 4.11:

$$C_i = S_{30} \oplus K_{31} \tag{4.11}$$

The encryption block C_i will then receive its final form.

4.6 Decryption Process

The decryption process is intended to undo every step of the encryption in order to precisely reconstruct the original grayscale sub-aperture images. It mirrors the encryption procedure but in reverse, using the same cryptographic key and parameters to ensure accurate data restoration.

Step 1: Key Derivation

The first step in the decryption pipeline is the regeneration of the same 128-bit symmetric key used during encryption. This is achieved by applying the SHA-256 hash function to the concatenation of a base user-provided key and a predefined salt. The initial 128 bits of the resulting hash output are then extracted to form the decryption key. As outlined in Eq. (4.12), this guarantees that the key matches exactly with that used in the encryption phase:

$$K = \text{Truncate}_{128}(\text{SHA256}(K_{\text{base}} \| \text{salt})) \tag{4.12}$$

Step 2: Vectorization

Following key derivation, the encrypted sub-aperture image is flattened into a one-dimensional vector format. This restructuring is done to allow uniform block-wise processing. The flattened vector is then partitioned into consecutive 64-bit blocks, consistent with the block size utilized during encryption.

Step 3: Block-Wise Decryption

Each 64-bit encrypted block is decrypted using the inverse operations of the Present cipher. Specifically, for each round, the inverse permutation layer is applied first, followed

by the inverse S-box substitution. The round keys are XORed in the reverse sequence, thereby undoing the original encryption transformation. As described in Eq. (4.13), the decryption process concludes with a final XOR operation using the original key to retrieve the plaintext block:

$$B_i = SBox^{-1}(PLayer^{-1}(C_i^{31} \oplus K^{31})) \rightarrow B_i = D_i^0 \oplus K^0 \tag{4.13}$$

This step-by-step inverse mapping ensures the faithful reconstruction of the original image content from the encrypted ciphertext.

Step 4: Reshaping

All the decrypted individual blocks are then concatenated and reshaped to regain the original image format. This reconstructs the grayscale sub-aperture image to its original spatial configuration, thus effecting decryption. This restores the original image content for each grayscale sub-aperture. All 169 decrypted grayscale sub-images are then arranged back into 13×13 light field sub-aperture images.

4.7 Merits of the Proposed Work

1. **Security:** The combination of the lightweight Present cipher with the secure SHA-256 hashing function results in a high security of the proposed PRESHMAC-256 algorithm. The SHA-256 function helps in achieving cryptographically strong diffusion and avalanche properties so that even one single-bit change in the input key results in a totally different hash. This greatly reduces the likelihood of collision and enhances immunity against pre-image and second pre-image attack. The PRESENT cipher also incorporates confusion and diffusion layers by applying 30 rounds of substitution and permutation with small 4-bit S-boxes and then by using permutation layers. All these together ensure the imprinted image information has high entropy and is oblivious to cryptanalysis as well as unauthorized reconstruction.

2. **Lightweight:** The primary advantage of the new scheme, as its most significant strength, is lightweight. Both Present and SHA-256 are designed with efficiency in mind, specifically within embedded and hardware environments. Regarding low gate counts and memory overhead, especially with Present, it is really suited to be implemented within limited computational resources, such as smart sensors, IoT modules, embedded processors, and real-time control units. With the blending of using a block cipher like Present and then a traditional cryptographic hash function like SHA-256, this results in putting the system in between decent high-secured applications with low

processing demand; thus, most of the practical needs for the present lightweight applications can be achieved.

3. **Structural Integrity:** Unlike many classical schemes of encryption that would destroy the inherent angular and spatial interrelationships of sub-aperture images in light field data, PRESHMAC-256 is designed to retain that inherent structure of the data. Structural coherence is critical for any subsequent decryption-uses depth estimation, refocusing, and 3D reconstruction of images stored or transmitted under supersecure conditions. In ensuring angular coherence, encrypted images, even when decrypted, remain light field in nature; thus, it can be most optimally used in applications that rely on multi-view spatial data integrity, even after safe storage or transport.

4. **Robustness:** The encryption function is made very resilient to a wide variety of attack vectors. The major addition of a key post-expansion scheme based on SHA-256, along with the multiple rounds of the Present cipher transformations, strengthens the algorithm against brute-forcing and statistical attacks. Besides, the combination of non-linearity provided by the substitution-permutation network of Present and the randomness of SHA-256 provides very high resilience against differential and occlusion-based attacks. These features ensure even in the event of part of the encrypted image being lost or purposely altered, the remaining intact data is kept safe and is not exposed to leakage or reverse-engineering.

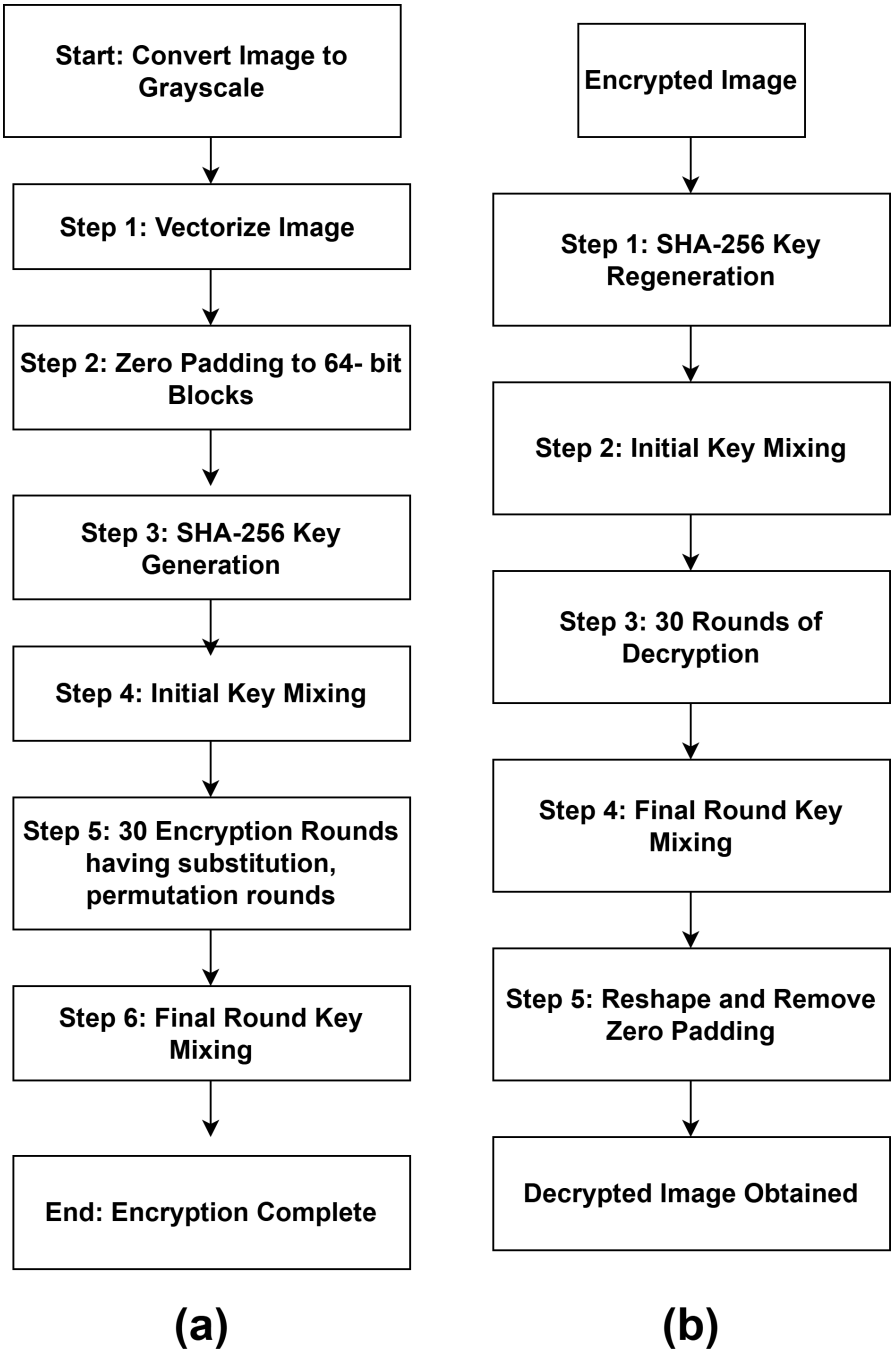

Figure 4.1: The complete workflow of the proposed scheme illustrating step-by step process of encryption (a) and decryption (b).

The pseudo code of the proposed scheme is given in Algorithm 1.

Algorithm 1 Encryption and Decryption Procedure

Require: Light Field sub-aperture images $I_{s,t}$

Ensure: Encrypted and decrypted sub-aperture images $\hat{I}_{s,t}$

Organize 169 sub-aperture images into a 13×13 grid
Define 80-bit hexadecimal key: $K_{\text{in}} = \texttt{ffeeddccbbaa99887766}$
Generate random 8-digit salt value: $S = \text{Random}()$
Concatenate key and salt: $M = K_{\text{in}} || S$
Compute SHA-256 hash: $H = \text{SHA256}(M)$
Extract final 128-bit key: $K_{\text{final}} = H[0:15]$
for each grayscale sub-aperture image $I_{s,t}$ **do**
    Convert image to vector: I_{vec}
    Pad image if not divisible by 64 bits: $I_{\text{pad}} = \text{Pad}(I_{\text{vec}})$
    for each 64-bit block P_i in I_{pad} **do**
        Initial round key addition: $S_0 = P_i \oplus K_0$
        for $j = 1$ to 31 **do**
            Substitute: $S_j = \text{SBox}(S_{j-1})$
            Permute: $S_j = \pi(S_j)$
            Add round key: $S_j = S_j \oplus K_j$
            Update key:
                $K_{j+1} = f(K_j)$, where
                $f(K_j) = \text{Rotate}(K_j) \oplus \text{Constant} \oplus \text{SBox}(K_j)$
        end for
        Final round key addition: $C_i = S_{30} \oplus K_{31}$
    end for
    Reshape encrypted blocks to image format and save
end for
Repeat the same process in reverse for decryption

Chapter 5

Results and Analysis

The proposed scheme performance was evaluated using real light fields captured by plenoptic cameras. The results prove that the encrypted pictures are very secure and are also seen to be vastly different from the original images, making it hard for unauthorized users to read them. Visual analysis, such as histograms and pixel-to-pixel comparison, confirms that the encryption methodology is robust and shows no visible pattern in the encrypted light field image. This makes the method a reliable choice for protecting light field photos in privacy-sensitive applications. The full explanation of the experiments conducted inside the suggested encryption and analysis framework is described in the following subsections:

5.1 Overview of Dataset

We have employed an encryption framework with real light field data from a plenoptic camera. The light field image used was given as Bikes and it's from the EPFL Light Field JPEG Pleno database [18], which is considered a standard benchmark in light field image processing. The raw plenoptic image was processed so that 13×13 sub-aperture images, having a spatial resolution of 625×434 pixels each, could be extracted. The current analysis was limited to middle 13×13 views, excluding outer sub-aperture images because images at the edges are mostly distorted and blurred due to the lenslet based acquisition process. Moreover, these edge images are less informative and could deteriorate performance for recon struction or encryption tasks. Thus, encryption, decryption, and subsequent analysis were based on considering the inner sub-aperture views for a fair evaluation.

Table 5.1: Technical Specifications of Light Field Dataset.

Parameter	**Value**
Dataset Name	Bikes Light Field Dataset
Number of Views	169 (Grid: 13 × 13)
Resolution per View	625 × 434 pixels
Pixel Count per Image	271,250 pixels
Total Pixel Count	45,396,250 pixels (625 × 434 × 169)
Aspect Ratio	1.44 (Landscape)
Number of Channels	3 (RGB)
Bit Depth	48-bit
Image Format	PNG
Data Type	uint16
Total Dataset Size	230.71 MB
Average File Size per Image	1.37 MB
Source	JPEG Pleno Light Field Dataset – Lenslet Lytro Illum Camera [18]

5.2 Analysis of the Proposed Encryption Method

In this section, we analyze the strength of the proposed encryption scheme:-

5.2.1 Histogram Analysis

A good encryption algorithm should mask the frequency distribution of gray levels in an image in such a way that information does not leak out through statistical attacks. The histogram of the original central image from the light field dataset exhibited distinct peaks and patterns, which reveal the structured nature concealed in its grayscale values. The proposed encryption method leaves the histogram of the encrypted image with indicative, rather uniform distributions of pixel values throughout the range, an indication of randomization having occurred. The randomization ensures that the encrypted image loses any significant information on the original light-field image. The histogram of the decrypted image closely matches the original light field image, which can be seen in Fig 5.1. This demonstrates that the decryption process has performed the restoration of the image accurately. The central image was selected for this analysis as it is a representative of the light field data. Although the analysis focused on the central image, similar results were observed in other sub-aperture images, confirming the robustness of the encryption and decryption.

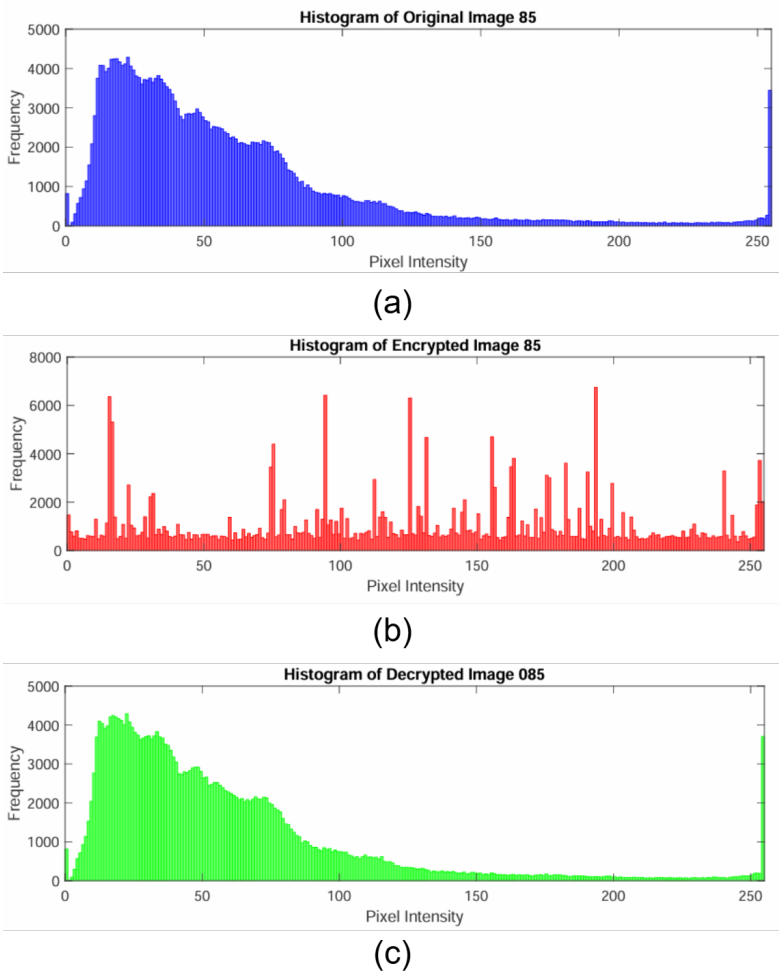

Figure 5.1: Histogram analysis of the original, encrypted, and decrypted versions of central image.

5.2.2 Adjacent Pixel Analysis

Adjacent pixels found in natural images are highly correlated, as neighboring pixels normally have similar gray levels. Hence, attackers can exploit this correlation to predict pixel values; breaking this correlation is therefore a requisite for any encryption algorithm. Analyzing this correlation in the Bikes dataset, we computed, for the central image, the correlation coefficients of neighboring pixels in the horizontal direction for the original, encrypted, and decrypted images. The correlation coefficient value was found to be **0.9545** for the original image, indicating a strong correlation between adjacent pixels. For the encrypted image, the coefficient dropped to **-0.0050**, showing that the correlation had been effectively removed and the pixel values appeared random. This was supported by an examination of the pixel distribution. The original image exhibited a pattern where adjacent pixels clustered together, whereas the encrypted image showed a highly dispersed and nearly uniform distribution of pixel values. Upon

decryption, the correlation coefficient computed is **0.9545**, very close to that of the original image as documented in Table 5.2.

This confirms that the proposed encryption scheme successfully decorrelates the adjacent pixels during encryption and accurately restores the original structure during decryption as illustrated in Fig. 5.2. The statistical metric used for this evaluation, as outlined in Eq. (5.1), is defined as:

$$r_{xy} = \frac{E[(x - \mu_x)(y - \mu_y)]}{\sigma_x \sigma_y} \tag{5.1}$$

where E represents the expected value, μ_x and μ_y denote the mean intensities of pixels x and y, respectively, and σ_x, σ_y are the standard deviations.

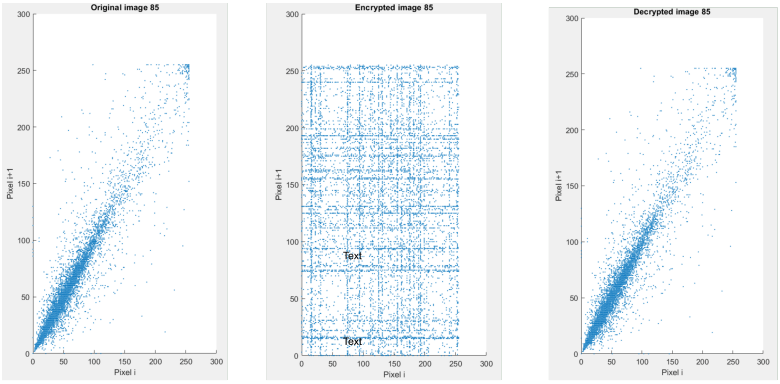

Figure 5.2: Adjacent pixel distribution and horizontal correlation coefficient analysis of central image.

Table 5.2: Horizontal Correlation Coefficient.

Image Type	**Correlation (%)**
Original (%)	0.9545
Encrypted (%)	-0.0050
Decrypted (%)	0.9545

5.2.3 Information Entropy Analysis

The central image from the Bikes light field dataset was evaluated to analyze the level of randomness induced through encryption. Information entropy was employed as the key metric for this assessment. The entropy values obtained for the original, encrypted, and decrypted images are tabulated in Table 5.3. The original and decrypted images

exhibited nearly identical entropy values of **7.0271** and **7.0274**, indicating effective decryption fidelity. Conversely, the encrypted image achieved a higher entropy of **7.5443**, nearing the ideal maximum value of 8. This highlights the significant randomness introduced by the encryption scheme. The corresponding bar chart in Fig. 5.3 visually emphasizes this contrast in entropy. To quantify this property, the entropy $H(m)$ is computed using Eq. (5.2), which is mathematically expressed as:

$$H(m) = -\sum_{i=0}^{255} p(m_i) \log_2 p(m_i) \tag{5.2}$$

where $p(m_i)$ indicates the probability of occurrence of a gray level m_i. Higher entropy values signify greater unpredictability, crucial for defending against statistical attacks.

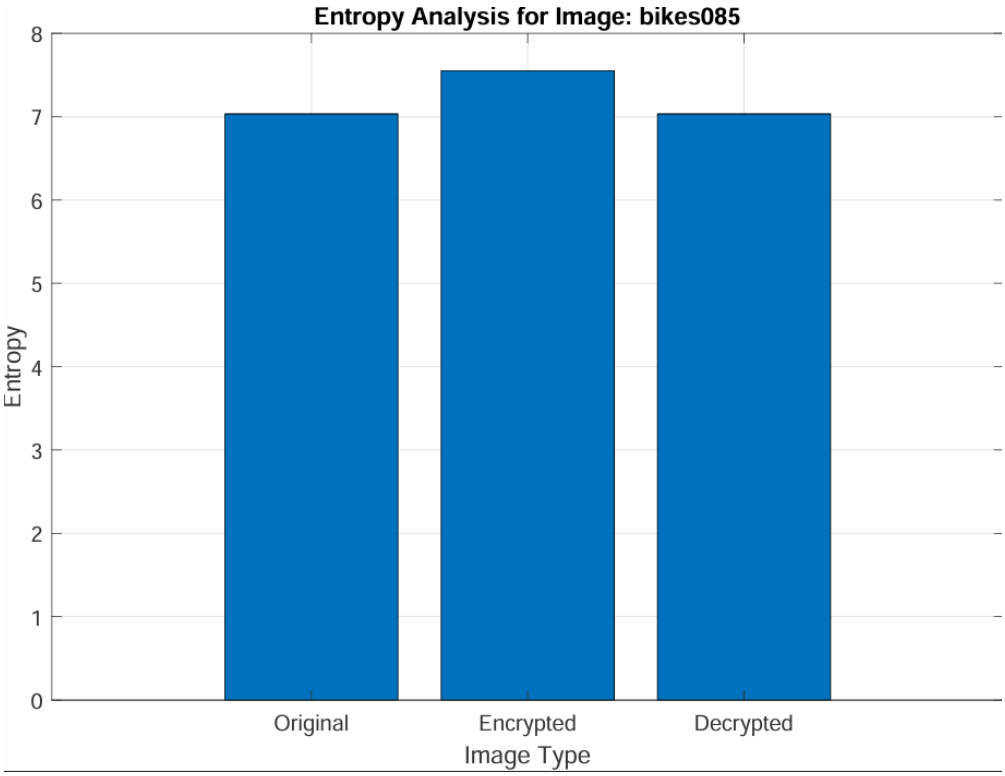

Figure 5.3: Information entropy analysis of the original, encrypted, and decrypted images for central image.

Table 5.3: Information Entropy Analysis.

Image Type	**Entropy (%)**
Original (%)	7.0271
Encrypted (%)	7.5443
Decrypted (%)	7.0271

5.2.4 Key Space Analysis

An essential requirement for a robust cryptographic system is the presence of a vast key space, rendering brute-force attacks impractical. The Present block cipher utilized in this scheme supports an 80-bit key. The total number of distinct keys available is computed as shown in Eq. (5.3):

$$2^{80} \approx 1.21 \times 10^{24} \text{ possible keys} \tag{5.3}$$

Assuming a scenario in which one million keys can be tested per second, the approximate time required to perform an exhaustive key search is given in Eq. (5.4):

$$\frac{2^{80}}{10^6 \times 60 \times 60 \times 24 \times 365} \approx 3.84 \times 10^{10} \text{ years} \tag{5.4}$$

For comparison, the estimated age of the universe, stated in Eq. (5.5), is:

$$1.38 \times 10^{10} \text{ years} \tag{5.5}$$

These values confirm the impracticality of brute-force key recovery and affirm the strength of the key space provided by the encryption scheme.

5.2.5 Key Sensitivity Analysis

The robustness of the proposed scheme was tested by altering a single bit in the encryption key. Two keys, Key1 and Key2 (with only one bit difference), were used to encrypt the same grayscale image.

The resulting encrypted images, illustrated in Fig. 5.4, appear completely distinct from each other. This validates the system's high key sensitivity. The NPCR value of **99.8278%** and UACI of **35.5987%** listed in Table 5.4 further support this claim, indicating a large variation in pixel values even for minor key changes.

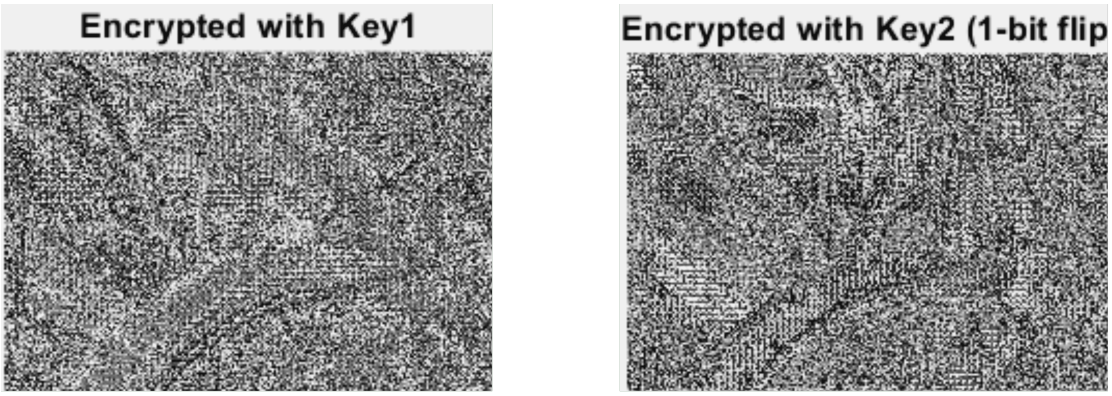

Figure 5.4: Key sensitivity analysis: Comparison of encryption using Key 1 and Key 2.

Table 5.4: Analysis of encrypiton key 1and 2.

Image Type	**(%)**
NPCR (%)	99.8278
UACI (%)	35.5987

5.2.6 Analysis of Occlusion Attacks

The encryption scheme's resilience to data loss was tested using occlusion attacks. Various fractions of the encrypted image (10%, 20%, 30%, and 50%) were occluded to mimic corruption or missing data. Upon decryption, it was observed that even when substantial parts were lost, the reconstructed images retained meaningful content, as shown in Fig. 5.5. This demonstrates the algorithm's partial reconstruction capability under occlusion.

5.2.7 Decryption Quality: PSNR and SSIM Evaluation

To quantify image quality after decryption, we computed PSNR and SSIM between the original and decrypted images. These metrics provide objective measurements of reconstruction accuracy.

PSNR quantifies the ratio between the maximum possible power of a signal and the power of corrupting noise. The formula used for PSNR is shown in Eq. (5.6):

$$PSNR = 10 \cdot \log_{10} \left(\frac{MAX_I^2}{MSE} \right) \tag{5.6}$$

where MAX_I is the maximum pixel value (255 for 8-bit images), and MSE is the mean squared error.

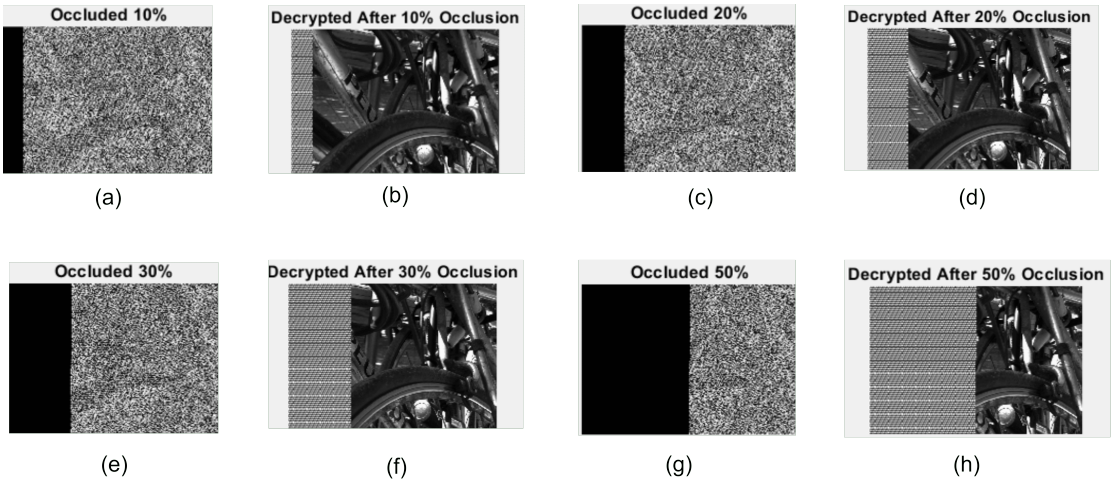

Figure 5.5: Occlusion attack simulation on encrypted central image at different occlusion levels: 10%, 20%, 30%, and 50%.

Similarly, SSIM is used to measure structural similarity and is calculated using Eq. (5.7):

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \tag{5.7}$$

Here, μ_x and μ_y are average intensities, σ_x^2, σ_y^2 are variances, σ_{xy} is the covariance, and C_1, C_2 are constants.

From Table 5.5, the decrypted images achieved high PSNR and SSIM values, demonstrating effective preservation of visual quality.

Table 5.5: Quality Encryption of Decrypted Image.

Metric	**Value**
PSNR	54.8186
SSIM	1.0000

Table 5.6: Avalanche Effect Analysis.

Parameter	**value(%)**
Total Bits	2170048
Differing Bits	1136715
Avalanche Effect (%)	52.38

5.2.8 Avalanche Effect

The avalanche effect, which is a very important property of secure encryption algorithms, specifies how a small change to plaintext or key will cause a large amount of

change in the ciphertext, and this change will be unpredictable. To evaluate the impact of the proposed block cipher within our system, a single bit perturbation was applied to the plaintext, and the resulting changes in the encrypted output were observed. Number of dissimilar bits and calculated avalanche percentage have been presented in Table 5.6 . The detected avalanche percentage is nearly 50%, the ideal one, which shows that the proposed block cipher has strong diffusion. That is, any small variation in input will produce a vastly different ciphertext, thereby strengthening the security of the encryption mechanism against differential attacks and adding to the overall robustness of visual privacy protection system proposed here.

Chapter 6

Conclusion and Future Scope

6.1 Conclusion

In this thesis, we researched the issue of visual privacy protection for high-dimensional light field imaging systems and introduced a novel encryption scheme called PRESHMAC-256. Light field images with their spatial-angular nature and 4D character offer unmatched capabilities like depth estimation, multi-view rendering, and refocusing after capture. But this very richness offers a new avenue for attack, and visual privacy becomes a prime concern. Existing cryptographic measures either are not structurally harmonious with light field data or are too resource-intensive to be deployed in real-time.

Hence, the primary objective of this research was to create a lightweight yet resilient encryption strategy specifically tailored for sub-aperture images in a light field. To do this, we proposed PRESHMAC-256, a hybrid encryption scheme combining the Present lightweight block cipher with HMAC-SHA256 for key derivation. The scheme provides secure and efficient block-wise encryption, taking advantage of the hardware-friendliness and simplicity of Present, with further key unpredictability provided through the secure cryptographic properties of SHA-256. In Chapter 3, we explained the methodology, including remarks on the dataset, the theoretical basis of the cryptographic primitives, and a detailed analysis of the encryption and decryption pipeline, optimized for grayscale sub-aperture images. The implementation also considered compatibility through bit-padding and reshaping mechanisms for maintaining angular structure after post-processing.

Chapter 4 delved into an empirical analysis of the suggested scheme, using the EPFL Light Field Dataset as its data source. We conducted various statistical and visual tests to validate the system's security and efficiency. Histogram analysis showed uniform pixel distribution in the encrypted images, thereby making them statistically robust. The correlation between neighboring pixels decreased from 0.95 in the original images to nearly zero after encryption, a very good indicator of robust decorrelation. Information entropy of the encrypted images was near the maximum value of 8, ascertaining the randomness of the pixels. PSNR and SSIM values also validated high-quality reconstruction after decryption, with values 54.81 dB and 1.0, respectively—much higher than acceptable values. Key-sensitivity and avalanche effect experiments have determined that even a single-bit simple modification of either the key or input could result in completely different cipher output.

Finally, simulation of occlusion attacks revealed that the encrypted data had partial recoverability, indicating the robustness of the scheme even in the presence of malicious tampering. The project managed to accomplish a number of the initial goals that were established at the commencement of this research. First, it provided low-latency and lightweight operation, an ideal fit for being deployed on edge devices and embedded systems. In return, it offered high resilience against brute-force and statistical attacks, a confirmation that was experimentally and mathematically verified. Third, the scheme maintained the structural integrity of light field data during decryption, enabling subsequent visual processing or analysis.

6.2 Future Scope

In spite of these developments, there are still certain limitations, and possible directions for future investigation. One such limitation is the inflexibility of the pipeline. Future models would benefit enormously from adaptive methods of encryption, where different parts of the image are given different levels of encryption based on the sensitivity of the material. This would reduce computational overheads while enhancing security where it is most required. The second path for the future is to extend this work to full-color light field data and 5D plenoptic functions with temporal and depth dimensions. Color image encrypting and preserving their angular coherence poses new challenges, and multi-channel ciphering schemes or vectorized block ciphers must be used. Aside from this, the deep learning potential may be employed to dynamically guide or optimize encryption. For instance, neural networks could be employed to predict in which areas of the light field contain more sensitive data so that the cipher can change its encryption level in real time.

Finally, its deployment on hardware platforms such as FPGA or GPU-based system could significantly speed up processing and enable opportunities for commercial applications in fields such as augmented reality, surveillance, and medicine. In conclusion, PRESHMAC-256 is a promising path towards light field image encryption that finds a balance between security, speed, and structural awareness compatibility. The work opens avenues for the development of future-generation more intelligent and adaptive encryption systems for computational imaging technologies.

List of Publications

Conference Paper

A. Singh, M. Sharma, and S. Raikwar, "PRESHMAC-256: A Lightweight Hybrid Block Cipher for Secure Light Field Image Encryption," *14th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO)*, Noida, India, Aug. 2025, pp. 1–6. **(Accepted for publication)**

References

[1] K. Wei, W. Wen, and Y. Fang, “Light field image encryption based on spatial-angular characteristic", Signal Processing, Vol. 185, Aug. 2021, 108080.

[2] G. Wu et al., “Light Field Image Processing: An Overview,” IEEE Journal of Selected Topics in Signal Processing, vol. 11, no. 7, pp. 926–954, Oct. 2017, doi: https://doi.org/10.1109/JSTSP.2017.2747126.

[3] Y. Wang, L. Wang, J. Yang, W. An, J. Yu, and Y. Guo, “Spatial-Angular Interaction for Light Field Image Super-Resolution,” *Lecture Notes in Computer Science*, pp. 290–308, Jan. 2020. Available: https://doi.org/10.1007/978-3-030-58592-1_18.

[4] L. Kocarev, “Chaos-based cryptography: a brief overview,” IEEE Circuits and Systems Magazine, vol. 1, no. 3, pp. 6–21, 2001, doi: https://doi.org/10.1109/7384.963463.

[5] J. Wang, G. Liu, Y. Chen, and S. Wang, “Construction and Analysis of SHA-256 Compression Function Based on Chaos S-Box,” IEEE access, vol. 9, pp. 61768–61777, Jan. 2021, doi: https://doi.org/10.1109/access.2021.3071501.

[6] I. Viola, M. Rerabek, and T. Ebrahimi, “Comparison and Evaluation of Light Field Image Coding Approaches,” IEEE Journal of Selected Topics in Signal Processing, vol. 11, no. 7, pp. 1092–1106, Oct. 2017, doi: https://doi.org/10.1109/jstsp.2017.2740167.

[7] O. S. Faragallah et al., “Block-Based Optical Color Image Encryption Based on Double Random Phase Encoding,” IEEE Access, vol. 7, pp. 4184–4194, 2019, doi: https://doi.org/10.1109/access.2018.2879857.

[8] V. S.Lima, F. A. B. S. Ferreira, F. Madeiro, and J. B. Lima, “Light field image encryption based on steerable cosine number transform,” Signal Processing, vol. 202, p. 108781, Sep. 2022, doi: https://doi.org/10.1016/j.sigpro.2022.108781.

[9] K. Wei and W. Wen, “Light Field Image Encryption Based on Pixel Substitution and Double Random Phase Encoding,” pp. 13–17, Jun. 2019, doi: https://doi.org/10.1145/3338472.3338477.

[10] W. Zhang, X. Zhang, S. Han, X. Wei, and X. Wan, “Multiple-image encryption based on light-field imaging and gravity model,” Op-

tics and Lasers in Engineering, vol. 141, p. 106565, Feb. 2021, doi: https://doi.org/10.1016/j.optlaseng.2021.106565.

[11] S. You, Y. Lu, W. Zhang, and B. Yang, "3-D color light field image encryption based on micro-lens array," Optical and Quantum Electronics, vol. 48, no. 8, Jul. 2016, doi: https://doi.org/10.1007/s11082-016-0670-3.

[12] W. Wen, K. Wei, Y. Zhang, Y. Fang, and M. Li, "Colour light field image encryption based on DNA sequences and chaotic systems," Nonlinear dynamics, vol. 99, no. 2, pp. 1587–1600, Nov. 2019, doi: https://doi.org/10.1007/s11071-019-05378-8.

[13] J. Shao, E. Bai, X. Jiang, and Y. Wu, "Multi-View Light Field Images Compression and Encryption Using Enhanced 3D Chaotic System and Pixel-Bit-Scrambling," IEEE Access, vol. 12, pp. 156471–156491, Jan. 2024, doi: https://doi.org/10.1109/access.2024.3481230.

[14] R. Niwa, Fumihiko Sakaue, and J. Sato, "Encrypted image display based on individual visual characteristics," Nagoya Institute of Technology, pp. 386–394, 2020, Accessed: Jun. 18, 2025. [Online]. Available: https://pure.nitech.ac.jp/en/publications/encrypted-image-display-based-on-individual-visual-characteristic

[15] A. Bogdanov et al., "PRESENT: An Ultra-Lightweight Block Cipher," Cryptographic Hardware and Embedded Systems - CHES 2007, pp. 450–466, 2007, doi: https://doi.org/10.1007/978-3-540-74735-2 31.

[16] H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication," www.rfc-editor.org, Feb. 1997, doi: https://doi.org/10.17487/RFC2104.

[17] S. and and E. Barker, "Secure Hash Standard (SHS)," NIST, May 11, 1993. https://www.nist.gov/publications/secure-hash-standard-shs-0 (accessed Jun. 18, 2025).

[18] JPEG Pleno. "JPEG Pleno Light Field Datasets According to Common Test Conditions." https://plenodb.jpeg.org/lf/pleno_lf (accessed June 17, 2025)