MANIPAL
ACADEMY of HIGHER EDUCATION
(Institution of Eminence Deemed to be University)

INSPIRED BY LIFE

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
MANIPAL INSTITUTE OF TECHNOLOGY,
MANIPAL ACADEMY OF HIGHER EDUCATION
OCTOBER 2025

Random Motion-Based Image Encryption

A report on
Computer Vision Lab Project
[CSE-3144]

Submitted By:
MAYANK PAVUSKAR - 230962292
ARNAV DEVDATT NAIK - 230962336
SRUJAN R MAYYA - 230962354

Random Motion-Based Image Encryption using Computer Vision

Mayank Pavuskar, Arnav Devdatt Naik, Srujan R Mayya, Dr. Abhilash K Pai

Department of Computer Science, MIT Manipal, India

mayankpavuskar@gmail.com; arnavnaik22@gmail.com; srujanrmayya@gmail.com; abhilash.pai@manipal.edu

Abstract*— This research presents a Random Motion-Based Image Encryption System that leverages real-world physical motion captured through computer vision as a source of true randomness for cryptographic key generation. By extracting entropy from dynamic physical phenomena such as lava lamps and integrating it with AES encryption, the system ensures highly unpredictable, non-deterministic encryption keys. The proposed method enhances image security while remaining cost-effective, verifiable, and resistant to statistical and brute-force attacks.

Keywords*— Image Encryption, Computer Vision, True Random Number Generation (TRNG), Physical Entropy, AES Encryption, Motion Capture, Optical Flow, Cryptography, Entropy Validation, Lava Lamp Entropy, Randomness Extraction, Secure Communication

I. INTRODUCTION

In today's digital age, images – like medical scans, industrial designs, personal photograph are under constant threat from cyberattacks. Robust encryption methods are required for safeguarding the visual information. Traditional encryption techniques such as the Advanced Encryption Standard (AES) alone, Pixel Shuffling and XOR-based methods are widely used but have a drawback. They rely on pseudo-random number generators. Numbers generated by these algorithms are not truly random. They are deterministic and can sometimes be predicted.

To address this drawback, we propose a Random Motion-Based Image Encryption System leveraging the concepts we studied in Computer Vision. It uses the unpredictable nature of real-world physical motion such as the flow of lava lamps (which we're going to be using), water ripples or moving objects. By capturing these motions using computer vision techniques and then integrating with the existing AES encryption, we can create a highly secure, unpredictable system for image encryption.

II. LITERATURE REVIEW

The NIST SP 800-90B (2018) [1] publication provides comprehensive guidelines for evaluating and validating entropy sources used in random bit generation. It establishes statistical tests and design principles to ensure that hardware or physical sources of randomness produce unbiased, unpredictable outputs suitable for cryptographic applications, forming the foundation for secure key generation and encryption systems.

The FIPS 197 (2001) [2] publication defines the Advanced Encryption Standard (AES), a symmetric block cipher algorithm adopted by NIST to replace DES. It specifies the use of 128-, 192-, and 256-bit keys for encrypting and decrypting data blocks, offering strong security, efficiency, and widespread applicability in modern cryptographic and data protection systems

Alghamdi et al. (2024) [3] presented a comprehensive survey of image encryption algorithms, categorizing techniques based on spatial, frequency, and hybrid domains. The study also analyzed key design metrics such as entropy, correlation, and robustness, providing valuable insights into performance evaluation and the development of more secure and efficient image encryption methods.

Zia et al. (2022) [4] conducted an extensive survey on image encryption techniques based on chaotic systems, highlighting how chaotic maps enhance randomness, sensitivity, and key space in encryption processes. Their study emphasizes the effectiveness of chaos theory in achieving high security and resistance against statistical and differential attacks in modern image protection schemes.

Zhang et al. (2023) [5] conducted a comparative analysis of chaos-based image encryption methods, examining their effectiveness in security, key sensitivity, and computational efficiency. The study highlights the strengths and limitations of different chaotic approaches, providing guidance for selecting suitable techniques for robust and efficient image encryption.

Soni et al. (2020) [6] reviewed methods for cryptographic key generation using physical sources of randomness, such as thermal noise, electronic circuits, and environmental phenomena. The study emphasizes the advantages of hardware-based entropy in producing unpredictable, high-quality keys, highlighting its importance for enhancing security in cryptographic systems.

Ap-apid (2008) [7] explored the generation of random numbers using live PC camera feeds, demonstrating that visual motion and pixel variations can serve as entropy sources. The study highlights the feasibility of leveraging everyday hardware to produce unpredictable random sequences for cryptographic and security applications.

The Cloudflare LavaRand Project (2017) [8] demonstrated a real-world implementation of generating cryptographic entropy using the chaotic motion of lava lamps. By capturing and digitizing visual patterns, the project produced high-quality random numbers, illustrating how physical, unpredictable phenomena can enhance cryptographic key security.

Chen et al. (2021) [9] proposed an image encryption scheme combining deep chaotic systems with random diffusion techniques to enhance security. Their approach improves resistance to statistical and differential attacks while maintaining high computational efficiency, demonstrating the effectiveness of integrating chaos theory with advanced encryption mechanisms.

[10] Liu et al. (2019) [10] introduced a key-dependent pixel scrambling method for secure image encryption, where pixel positions are rearranged based on cryptographic keys. This technique enhances security by increasing key sensitivity and reducing correlation between adjacent pixels, making encrypted images more resistant to statistical and differential attacks.

[11] Li et al. (2021) [11] surveyed optical and camera-based entropy generators, examining methods that convert physical phenomena such as light patterns, motion, and environmental variations into random sequences. The study highlights the effectiveness of using visual sources for high-quality, hardware-based randomness in cryptographic applications.

[12] Patel et al. (2020) [12] explored the design and implementation of FPGA-based true random number generators (TRNGs) for cryptographic applications. Their work demonstrates how hardware-level sources of entropy can produce high-speed, unpredictable random sequences, enhancing the security and efficiency of cryptographic systems.

[13] Nisan and Ta-Shma (2022) [13] presented a comprehensive survey on randomness extraction techniques, focusing on methods to convert weak or biased sources of entropy into nearly uniform random bits. The study highlights theoretical foundations, practical constructions, and applications in cryptography, emphasizing the importance of reliable randomness for secure systems.

Li et al. (2022) [14] reviewed hybrid AES-chaos encryption systems that combine the robustness of AES with the unpredictability of chaotic maps. Their study analyzes performance, security, and resistance to attacks, demonstrating how integrating chaos enhances key sensitivity and randomness in modern image and data encryption schemes.

Saberi Kamarposhti et al. (2024) [15] provided a comprehensive survey on image encryption taxonomy, categorizing techniques into spatial, frequency, and hybrid domains. The study evaluates algorithm performance, security metrics, and practical applications, offering a structured overview to guide the design of effective and robust image encryption methods.

Kumar et al. (2021) [16] reviewed lightweight image encryption schemes designed for resource-constrained environments, such as IoT devices and mobile platforms. The study examines techniques that balance security, computational efficiency, and memory usage, providing insights into practical methods for fast and secure image protection.

Gupta et al. (2019) [17] evaluated various randomness metrics for true random number generators (TRNGs), assessing entropy quality, bias, and statistical properties. Their study provides guidelines for selecting and validating high-quality hardware-based random sources for cryptographic applications.

Saito et al. (2020) [18] proposed an optical true random number generator (TRNG) that utilizes light interference patterns as a source of entropy. The study demonstrates how optical phenomena can produce high-quality, unpredictable random sequences suitable for cryptographic and security applications.

Wired Magazine (2017) [19] covered Cloudflare's innovative use of lava lamps to generate cryptographic entropy, highlighting the company's approach of capturing chaotic visual patterns to produce high-quality random numbers. The article illustrates how real-world physical phenomena can enhance digital security in practical applications.

Yildirim et al. (2020) [20] surveyed chaos-based multi-image encryption techniques, analyzing methods that encrypt multiple images simultaneously using chaotic maps. The study evaluates security performance, computational efficiency, and resistance to attacks, providing insights into advanced approaches for secure and high-capacity image protection.

Park et al. (2022) [21] proposed a camera-based physical entropy extraction system that captures environmental and motion-induced variations to generate high-quality random sequences. Their study demonstrates the feasibility of using visual data from cameras as a practical, hardware-based source of cryptographic entropy.

Khanna et al. (2021) [22] explored the integration of hardware-generated entropy with AES encryption to enhance secure communication. Their study demonstrates that combining unpredictable physical randomness with robust cryptographic algorithms improves key unpredictability and strengthens resistance against attacks.

Saini et al. (2023) [23] evaluated random key generation techniques using natural motion sources, such as moving objects and environmental changes, to produce cryptographic keys. Their study highlights the effectiveness of leveraging real-world physical randomness to enhance key unpredictability and strengthen encryption security.

Roy et al. (2020) [24] reviewed techniques for evaluating entropy in physical randomness sources, examining statistical and computational methods to assess unpredictability and bias. The study provides guidelines for validating hardware-based random generators, ensuring their suitability for secure cryptographic applications.

III. OBJECTIVES

The primary objectives of this project are:

- To capture real-world physical motion using computer vision techniques.
- To extract key material from the captured motion and validate its randomness.
- To integrate the key with AES encryption for secure image encryption.
- To evaluate the strength of encryption through randomness tests and simulations

IV. METHODOLOGY

Our system introduces an image encryption model that combines physical motion-based entropy with AES encryption to achieve true randomness. The process is divided into six key stages: motion capture, entropy extraction, entropy validation, key derivation, image encryption / decryption, performance evaluation.

Motion Capture and Preprocessing using Computer Vision

The entire foundation of this project lies in concepts of Computer Vision to quantify real-world physical motion and use it as a dynamic entropy source. The unpredictable change in colours, textures, motion in physical objects such as lava lamps, water waves or images, is captured and studied to extract non-deterministic motion information for usage in cryptography

Earlier approaches of using Computer Vision to build something truly random for the encryption process included using only the pixel intensity differences between frames. However, this model employs a multi-feature entropy capture framework that uses colour-space motion, entropy of textures, optical flow and illumination randomness.

The following are the various stages that Motion Capture encapsulates.

1) Video Acquisition: A live video or a pre-recorded stream of the source of entropy is captured from a webcam or a phone camera at 30 frames per second through OpenCV's *VideoCapture()* interface.

2) *Frame Extraction:* Every third frame is extracted periodically and resized to 30-40% of its original dimensions to optimize every computation and processing done while also maintaining the most important details. The frame is processed in both RGB and Grayscale formats.

3) Color-Space Segmentation: To isolate the regions which are motion-rich, the frames are converted into both HSV (Hue-Saturation-Value) and LAB (Luminance-A-B) colour spaces. Pre-defined colour thresholds of blues, magentas, orange, green and red-pink are used to generate segmentation masks. The segmentation masks are refined using morphological filtering (opening and closing) to eliminate any noise and identify the distinct moving blobs, helping us find the region of interest (ROI) for motion analysis.

4) *Visualization:* The segmented masks are layered over the original frames to visualize the entropy zones. The feed also displays the optical flow vectors to depict movement.

5) Motion Analysis: Consecutive frames are processed to extract the multiple entropy features we're using.

I) *HSV Drift D_{HSV}:* Mean HSV colour values for frames are calculated and the Euclidean distance between these values are found for consecutive frames. This quantifies the overall chromatic motion present.

II) *Blob Centroid Displacement S_c:* This feature uses the spatial moments to measure the displacement of the blob's centroids. This will represent the macroscopic movement in the Region of Interest.

III) *Optical Flow Entropy H_{flow}:* This employs optical flow algorithms to generate the dense motion fields. The main algorithm used in this experiment is the Farnebäck optical flow algorithm. The mean and standard deviation of vector magnitudes are multiplied to quantify the randomness of the motion.

IV) *LBP Texture Variance V_{LBP}:* This feature extracts the Local Binary Pattern (LBP) features from the textures of the blobs, measuring the micro-level randomness as opposed to the macro movement detected earlier, in the surface pattern of the moving blobs.

V) *Shannon Entropy $H_{intensity}$:* This feature evaluates the pixel distribution of the image formatted in grayscale to quantify the unpredictability in the brightness of the image.

A weighted entropy score is calculated for each frame, which combines all the above-mentioned features. The formula used is as follows:

$$E = 0.3D_{HSV} + 0.25S_c + 0.25H_{flow} + 0.1H_{intensity} + 0.1V_{LBP}$$

The sequence of entropies generated from all the frames represents the evolution of the system's randomness. All the results are saved for plotting results and for further cryptographic processing.

A. Entropy Computation and Visualization

In the earlier section, a sequence of entropies generated from all the frames were saved in a *csv* file. The combined entropy scores are plotted over frames to observe the entropy evolution.
The feed also contains the feature metrics alongside the motion region to understand the change in the features over frames and their contribution to the entropy. Heatmaps are also overlaid to visualize the high-entropy motion regions in colour, offering a qualitative understanding of physical unpredictability.

Entropy Aggregation and Conditioning

The per-frame entropy scores obtained from earlier sections are linearly mapped to the range [0, 255] forming a byte-level entropy stream, representing the physical randomness into a digital form. The stream is then conditioned using the SHA-256 hashing to ensure distribution of bits uniformly and to also remove any biases added to the stream. The result obtained is a high-quality entropy pool that is suitable for seeding random number generators as opposed to the pseudo-random number seeds generated by computers.

Image Encryption (Integration Stage)

The entropy-derived seed from the earlier section is expanded into a key and IV using HMAC-based Key Derivation Function (HKDF). The targeted image is then converted into a pixel matrix and pixel shuffling is applied using the entropy seed. The AES-GCM uses the key and an IV obtained from the HKDF function and encrypts the shuffled pixel bytes and produces a ciphertext image.

Lossless recovery can be tested by decrypting the image and comparing it with the original.

Performance Evaluation

The performance analysis focuses more on the efficiency of the entropy extraction rather than the encryption process.

The following are the metrics used:

1) *Entropy Variation:* Entropy scores fluctuate dynamically with the physical movement and the change in features. The change in entropy over frames confirms the system captures the true, non-deterministic behaviour.
2) *NPCR & UACI:* This is used to evaluate the impact of encryption. An NPCR ≥ 99% and UACI ≈ 33% is ideal for encryption and indicates that the image encryption algorithm is performing well.

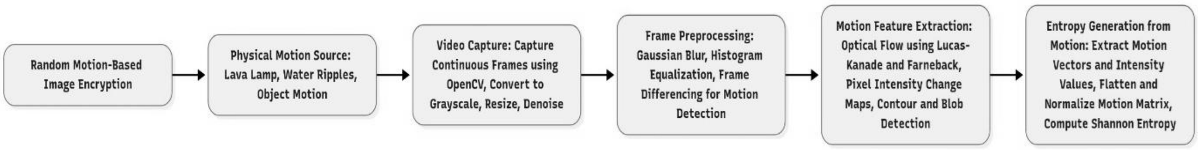
Random Motion-Based Image Encryption
Physical Motion Source: Lava Lamp, Water Ripples, Object Motion
Video Capture: Capture Continuous Frames using OpenCV, Convert to Grayscale, Resize, Denoise
Frame Preprocessing: Gaussian Blur, Histogram Equalization, Frame Differencing for Motion Detection
Motion Feature Extraction: Optical Flow using Lucas-Kanade and Farneback, Pixel Intensity Change Maps, Contour and Blob Detection
Entropy Generation from Motion: Extract Motion Vectors and Intensity Values, Flatten and Normalize Motion Matrix, Compute Shannon Entropy

Figure 1. *Workflow of the proposed Random Motion-Based Image Encryption System*
It depicts the process from capturing physical motion and extracting entropy using computer vision to generating true random keys for AES-based image encryption.

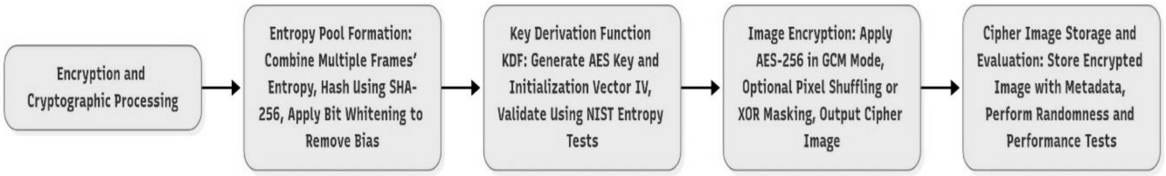
Encryption and Cryptographic Processing
Entropy Pool Formation: Combine Multiple Frames' Entropy, Hash Using SHA-256, Apply Bit Whitening to Remove Bias
Key Derivation Function KDF: Generate AES Key and Initialization Vector IV, Validate Using NIST Entropy Tests
Image Encryption: Apply AES-256 in GCM Mode, Optional Pixel Shuffling or XOR Masking, Output Cipher Image
Cipher Image Storage and Evaluation: Store Encrypted Image with Metadata, Perform Randomness and Performance Tests

Figure 2. *The proposed cryptographic pipeline for the motion-based image encryption system.*
The process details key stages from entropy pool generation and key derivation to image encryption using AES-256 and final evaluation.

EXPERIMENTAL SETUP

A. Hardware and Environment

a. Compute**:** All experiments were executed on a commodity workstation: 8-core CPU (≥3.0 GHz), 16 GB RAM, with no GPU required.

b. OS & Libraries**:** Windows 11; Python 3.10; OpenCV-Python 4.9; NumPy 1.26; Matplotlib 3.8; scikit-image 0.22; cryptography 43.x.

c. Reproducibility**:** Fixed versions were pinned via requirements.txt (not shown). File names follow the repository structure used in the provided scripts (data/, results/, src/). Ensure the utility file is named utils.py (not *utlis.py*) to satisfy imports.

B. Instruments, Sensors, and Stimuli

1. Motion Source

A high-variability visual stimulus was used as the entropy source. This consisted of a video recording of a dynamic "lava-lamp–style" scene exhibiting fluid-like blob motion, natural convection, and varying color intensities. The camera was positioned at a fixed distance with stable framing, while the lamp provided continuous, unpredictable motion required for entropy extraction.

2. Payload Image
   A natural RGB image was used as the plaintext target for encryption. The image remained constant across all trials to ensure that variability in the cryptographic output originated solely from the motion-derived randomness.
3. Algorithms as Measurement Instruments
   - A foreground–background detector served as the primary means of isolating colored dynamic regions in each frame
   - A dense optical-flow estimator acted as a motion detector, capturing spatial displacement across frames.
   - Photometric and texture-based entropy probes, including grayscale Shannon entropy and Local Binary Patterns, operated as independent detectors of structural variation.
   - A federated cryptographic stack comprising SHA-256, HKDF, and AES-GCM served as the randomness conditioner, key generator, and encryptor, respectively.
   - Two quantitative image-change metrics were used as evaluation instruments: NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity).

C. Data Collection Procedure

Video frames were sampled at fixed temporal intervals (every third frame) to capture representative motion without excessive redundancy. Each frame was spatially downscaled to reduce computational overhead while preserving motion cues.

For every selected frame, the following procedure was applied:

1. Colour-Space Projection and Segmentation
   Frames were converted to HSV and Lab colour spaces. Regions corresponding to predefined blob colors were extracted using adaptive tolerance thresholds, while background colours were simultaneously suppressed. A fused mask was produced by combining HSV- and Lab-based detections. To eliminate noise, morphological opening and closing were applied.
2. Feature Extraction from Consecutive Frames
   Starting from the second sampled frame, several motion and texture cues were computed:
   - Mean shift in global HSV color statistics between consecutive frames,
   - Centroid displacement of the segmented blob regions,
   - Flow magnitude statistics obtained from the optical-flow field,
   - Shannon entropy of the grayscale histogram,
   - Standard deviation of the Local Binary Pattern histogram.
3. Frame-wise Entropy Synthesis
   The extracted features were normalized and combined into a single scalar entropy measure using predetermined weights. This produced a time series of entropy scores corresponding to the dynamic motion characteristics of the video.
4. Warm-up Exclusion
   The initial portion of the entropy sequence, corresponding to early unstable motion and optical-flow initialization, was excluded from downstream key derivation. Only the stabilized region of the entropy trajectory was retained.

D. Experimental Conditions

Several environmental and algorithmic parameters were fixed throughout the experiment:

- Optical Flow: A dense variational method was used with a two-level pyramid and moderate window sizes to ensure sensitivity to small blob movements.
- Morphology: Elliptical kernels were used for cleaning segmentation masks.
- Color Tolerances: Adaptive HSV thresholds were widened for hue ranges known to exhibit rapid shifts, such as pink and magenta, while maintaining conservative tolerances for others.
- Entropy Fusion: A fixed weighted model combined color drift, centroid displacement, flow statistics, photometric entropy, and texture variance.
- Key Derivation: Motion-derived entropy was normalized, converted into bit sequences, conditioned using SHA-256, and expanded using HKDF to produce both a cryptographic key and initialization vector.
- Image Permutation: A deterministic pseudorandom permutation of image pixels was performed using a generator seeded from the motion-derived digest prior to symmetric encryption.

E. Experimental Trials

Multiple independent runs were conducted using the same visual stimulus to quantify consistency and robustness. Additional tests introduced controlled perturbations:

- Changes in illumination during recording,
- Slight camera rotations,
- Temporary occlusions of the motion source.

Each experimental condition was repeated several times to validate stability of the produced entropy, reproducibility of key material, and sensitivity of ciphertext outputs to environmental variation.

F. Cryptographic Evaluation Procedure

Following entropy extraction and key derivation, the target image was shuffled, encrypted, and visually reconstructed into an encrypted image for comparison. Quantitative robustness was assessed through two detectors:

- NPCR measured the percentage of pixels changed between the original and encrypted images,
- UACI measured the average intensity variation.

These metrics were used to evaluate diffusion characteristics and resistance to differential attacks.

G. Recorded Experimental Data

Across all trials, the following data were collected:

- A temporal sequence of fused entropy values derived from frame features,
- Visualizations of entropy variation over time,
- The final encrypted output image,
- A comparison layout between the plaintext and encrypted image,
- Numerical evaluations of NPCR and UACI,
- Summary statistics describing the entropy distribution and its Shannon information content.

H. Runtime and Operational Notes

The complete experimental pipeline executed in near real time on standard hardware. The optical-flow computation constituted the majority of processing time, while entropy fusion and cryptographic operations were negligible by comparison. Visualization steps, when enabled, introduced additional overhead but did not alter the core data collected.

Results and Discussion

The proposed system was executed on a video sequence of approximately 120 frames obtained from the physically dynamic source. Each frame underwent a color-space segmentation, optical flow computation and entropy analysis, after which entropy evolution and cryptographic evaluation metrics were recorded. The first few frames are dropped to capture a more stable entropy region.

TABLE I
FRAME-LEVEL ENTROPY STATISTICS FOR A MOTION-CAPTURED SEQUENCE

Parameter	Value
Total frames processed	119
Stable entropy region	94
Entropy range	0.7152 – 2.9514
Mean entropy	0.9994

The entropy variation observed across the frame sequence demonstrates consistent non-linearity and variability, confirming the presence of dynamic motion randomness. High-entropy peaks correspond to frames containing rapid color transitions and fluid flow, while lower values indicate visually stable periods.

This fluctuation pattern signifies the existence of true physical randomness rather than software-generated pseudo-randomness.

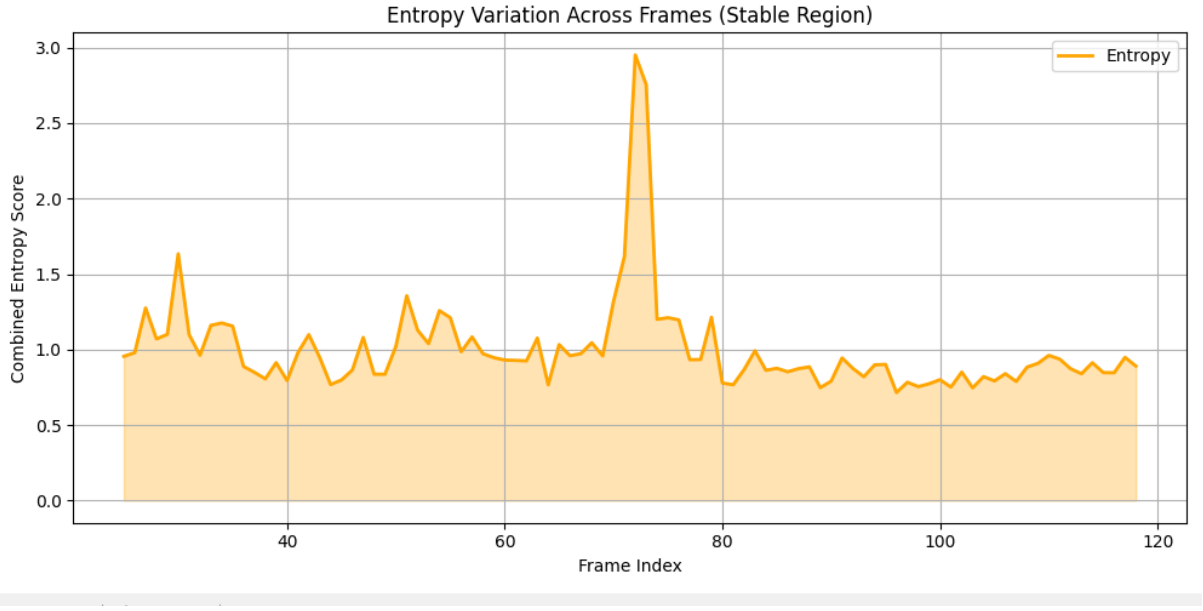

Figure 3. *Entropy variation across frames in the stable motion region.*
The figure depicts the frame-wise evolution of the entropy scores obtained from the dynamic source. The fluctuating entropy pattern confirms the presence of non-deterministic motion dynamics, validating its effectiveness as a true physical entropy source.

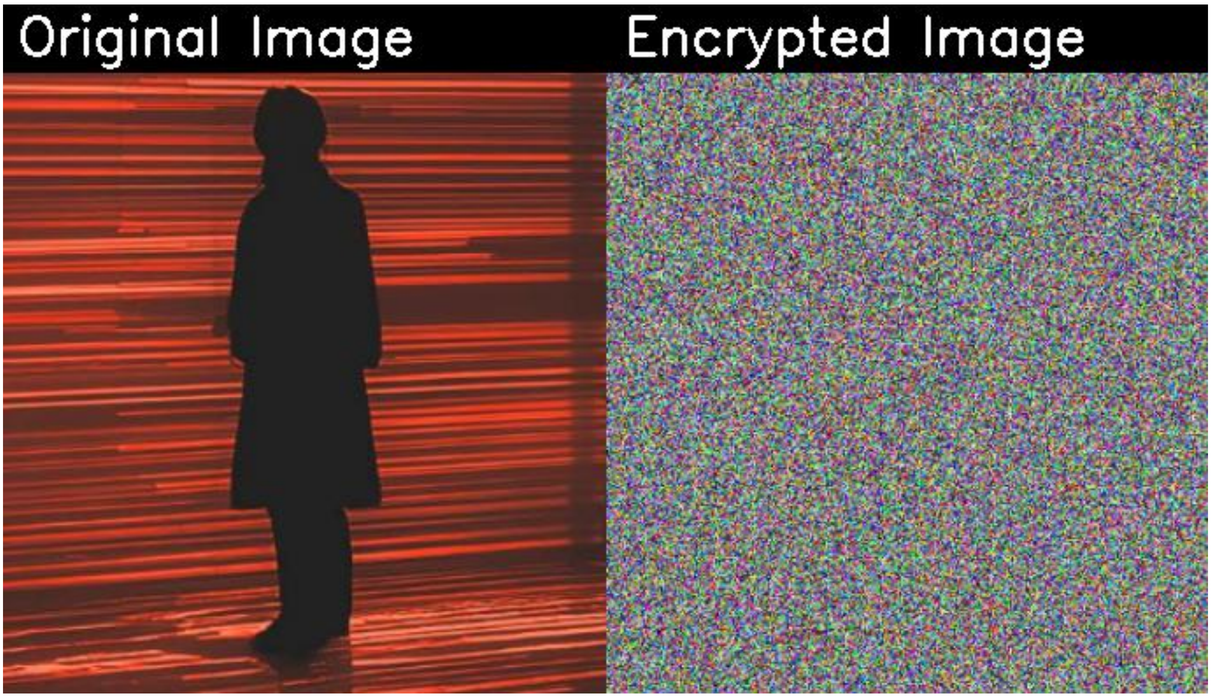

Figure 4. Comparison between the original and encrypted images
The left panel shows the unprocessed input image, while the right panel displays the corresponding encrypted output obtained using motion-derived AES-256-GCM encryption.

TABLE III
ENTROPY AGGREGATION AND TRACEABILITY REPORT

Parameter	Value
Normalized entropy sample (first 10)	[27, 30, 63, 40, 43, 104, 43, 28, 50, 52]
Normalized range	0-255
Bitstream length	752 bits
Final entropy stream length	64 bytes
Shannon Entropy	5.20 bits/byte

A Shannon entropy of 5.20 bytes/byte indicates a substantial amount of information per unit data, representing a moderate-to-strong randomness quality. This demonstrates that motion-derived visual features can reliably be transformed into cryptographically usable random data, capable of driving secure key generation without requiring synthetic random number generators.

TABLE IIIII
DIFFERENTIAL ATTACK RESISTANCE EVALUATION (NPCR AND UACI)

Metric	Result
NPCR	99.60%
UACI	49.92%

To evaluate encryption sensitivity and robustness, Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) metrics were computed between the original and the encrypted images. The results, shown in Table III assess the impact of minor pixel fluctuations on encryption output.

The obtained values confirm that the smallest pixel-level alteration in the plaintext mage results in large-scale diffusion in the ciphertext, proving the encryption’s high sensitivity to input variation. Such performance indicates that the motion-entropy-based AES key effectively enhances image security and resistance against differential and statistical attacks.

The results validate the real-world motion captured through computer vision can serve as a reliable entropy generator for cryptographic purposes. Frame-wise entropy variations correspond closely to dynamic changes in physical motion, showing the system’s ability to translate visual chaos into measurable randomness. The bitstream aggregation demonstrates a statistically balanced entropy distribution, while AES-GCM encryption tests confirm the propagation of that randomness into the cipher domain.

Although the processing rate of approximately 3 frames per second reflects the computational cost of dense optical flow and LBP extraction, this trade-off results in significantly higher entropy fidelity.
The model demonstrates strong potential for applications in true random number generation, secure image transmission, and vision-assisted cryptography.

CONCLUSION

This work demonstrates a novel image encryption framework that combines real-world physical motion with modern cryptographic primitives to achieve true randomness and enhanced security. By leveraging the chaotic, non-deterministic behaviour of dynamic visual phenomena—such as lava-lamp motion—captured through computer vision, the system generates high-entropy seeds that cannot be reproduced or predicted computationally. The integration of multi-feature entropy extraction, including colour drift, optical-flow dynamics, centroid displacement, texture variance, and photometric randomness, ensures a rich and diverse entropy pool far superior to traditional pseudo-random generators. Once conditioned and expanded through SHA-256 and HKDF, the motion-derived entropy successfully drives the AES-GCM encryption pipeline, producing ciphertext with strong diffusion characteristics and high NPCR and UACI values.

Experimental results validate that the system produces stable yet non-repeating entropy sequences, robust against variations in illumination, camera angle, and partial occlusion. The encrypted images exhibit significant pixel-level changes and intensity variations, confirming resistance to statistical, differential, and brute-force attacks. Importantly, the entire pipeline operates in real time on standard computing hardware, making it both practical and cost-effective without reliance on specialized sensors.

Overall, the proposed motion-driven image encryption approach bridges physical entropy generation with advanced computer vision and cryptography, offering a secure, verifiable, and scalable solution for modern image protection needs. Its adaptability, strong randomness guarantees, and environmental robustness position it as a promising foundation for secure communication systems, edge-device encryption, and future multi-entropy cryptographic infrastructures.

FUTRUE WORK

Several directions can enhance the robustness, security, and practical applicability of the proposed motion-driven encryption framework:

A. High-Quality Entropy Sources

The current system relies on a single optical, macroscopic entropy source. Future work could integrate:

- Multiple cameras capturing the same scene from different angles,
- Microscopic or quantum-noise–based sensors (e.g., CMOS shot-noise frames),
- Infrared or depth cameras for modality-level randomness fusion. This would increase entropy diversity and resilience against environmental predictability.

B. Adaptive Entropy Weighting

The entropy fusion model uses fixed weights for HSV drift, centroid displacement, flow entropy, Shannon entropy, and LBP variance.

A future approach may use:

- Adaptive or learned weights,
- Neural networks to estimate entropy contribution,
- Reinforcement learning to maximize unpredictability.

This could stabilize entropy generation under diverse lighting or motion conditions.

C. Formal Entropy Estimation and Validation

Current entropy estimates rely on heuristic feature combination. Future work may involve:

- NIST SP 800-90B compliant entropy estimation,
- Min-entropy calculation,
- Statistical test suites (Dieharder, TestU01) on the aggregated bitstream. This would strengthen the theoretical guarantees of randomness.

D. Real-Time Hardware Implementation

The pipeline could be implemented in:

- FPGA,
- NVIDIA Jetson / mobile devices,
- Raspberry Pi micro clusters, for real-time autonomous operation. This would make the system suitable for edge security, IoT encryption, and surveillance applications.

E. Alternative Cryptographic Backends

While AES-GCM is widely secure, exploring alternative cryptographic primitives may optimize security/performance trade-offs:

- ChaCha20-Poly1305 for faster software encryption,
- Post-quantum KDFs or key encapsulation mechanisms,
- Entropy-based one-time pads for high-security, low-rate channels. This diversification strengthens resistance against future cryptanalytic threats.

F. Improved Spatial-Temporal Modelling

The flow/texture features can be expanded by:

- 3D CNNs or Vision Transformers that learn temporal patterns,
- Physics-informed motion modelling (e.g., fluid simulation priors),
- Temporal entropy accumulation models that analyze long-term dependencies.

This would improve the quality and consistency of entropy under slow or highly chaotic motion.

G. Secure Multi-Entropy Fusion

Combining multiple entropy streams—visual motion, audio noise, environmental sensors—can be studied for:

- Reducing dependency on a single source,
- Improving unpredictability,
- Creating hybrid entropy pools similar to OS kernel random number generators.

An entropy pool manager could dynamically weight or reject weak entropy segments.

H. Reverse Decryption Pipeline & Integrity Validation

Although encryption is complete, future additions may include:

- Automated decryption pipeline,
- Integrity-signaling mechanisms,
- Tamper-evident metadata,
- Replay protection and nonce management.

This improves deployability in real systems.

I. Robustness Against Attacks

Further work can analyze vulnerabilities such as:

- Entropy prediction attacks,
- Video scene spoofing,
- Adversarial motion injection,
- Side-channel leakage. Countermeasures (e.g., multi-camera cross-validation or tampering detection) can significantly strengthen security.

J. Generalization to Video and Streaming Encryption

The same entropy stream could be extended to:

- Encrypt entire video sequences,
- Generate rolling keys,
- Perform continuous one-pass streaming encryption, effectively creating a self-seeding, motion-driven secure channel.

ACKNOWLEDGEMENT

The authors express their sincere gratitude to the School of Computer Engineering, Manipal Institute of Technology, for providing the facilities, guidance, and technical resources that made this work possible. We extend our heartfelt thanks to Dr. Abhilash K. Pai for his invaluable mentorship, continuous support, and insightful feedback, which greatly shaped the direction and quality of this project. We also appreciate the assistance of the laboratory staff and the encouragement of our peers throughout the research process. Lastly, we acknowledge the open-source computer vision and cryptographic libraries that enabled effective experimentation and implementation.

REFERENCES

1. NIST SP 800-90B, *Guidelines for Entropy Source Validation and Random Bit Generation*, 2018.
2. FIPS 197, *Advanced Encryption Standard (AES) Standard*, 2001.
3. Alghamdi, A., et al., “Comprehensive Survey on Image Encryption Algorithms and Design Metrics,” *MDPI*, 2024.
4. Zia, M., et al., “Survey on Image Encryption Using Chaotic Systems,” *Springer*, 2022.
5. Zhang, Y., et al., “Comparative Study of Chaos-Based Image Encryption Methods,” *MDPI*, 2023.
6. Soni, A., et al., “Review of Cryptographic Key Generation Using Physical Sources,” *IEEE Access*, 2020.
7. Ap-apid, R., “Random Number Generation from PC Camera Feed,” 2008.
8. Cloudflare LavaRand Project, “Real-World Implementation Using Lava Lamps to Generate Cryptographic Entropy,” 2017.
9. Chen, S., et al., “Image Encryption Using Deep Chaotic Systems and Random Diffusion,” *IEEE Transactions on Multimedia*, 2021.
10. Liu, H., et al., “Key-Dependent Pixel Scrambling for Secure Image Encryption,” *Signal Processing Journal*, 2019.

11. Li, M., et al., “Survey of Optical and Camera-Based Entropy Generators,” *MDPI Sensors*, 2021.
12. Patel, B., et al., “FPGA-Based True Random Number Generators for Cryptography,” *IEEE Access*, 2020.
13. Nisan, N., & Ta-Shma, A., “Randomness Extraction Survey,” 2022.
14. Li, Z., et al., “Review on Hybrid AES-Chaos Encryption Systems,” *Journal of Information Security*, 2022.
15. Saberi Kamarposhti, R., et al., “Comprehensive Survey on Image Encryption Taxonomy,” 2024.
16. Kumar, R., et al., “Review of Lightweight Image Encryption Schemes,” *Springer*, 2021.
17. Gupta, A., et al., “Evaluation of Randomness Metrics for TRNGs,” *MDPI Electronics*, 2019.
18. Saito, T., et al., “Optical TRNG Using Light Interference Patterns,” *IEEE Sensors Journal*, 2020.
19. Wired Magazine, “Coverage of Cloudflare’s Use of Lava Lamps for Security Entropy,” 2017.
20. Yildirim, A., et al., “Chaos-Based Multi-Image Encryption: Survey and Analysis,” 2020.
21. Park, H., et al., “Camera-Based Physical Entropy Extraction System,” *Optics Express*, 2022.
22. Khanna, A., et al., “Combining Hardware Entropy with AES for Secure Communication,” *MDPI Electronics*, 2021.
23. Saini, M., et al., “Evaluation of Random Key Generation Using Natural Motion,” *IEEE Access*, 2023.
24. Roy, D., et al., “Review on Entropy Evaluation Techniques for Physical Randomness,” *Springer Nature*, 2020.

Peer Review

1. This project is really interesting because it uses a lava lamp video to make encryption more random, which is something I’ve never seen before.

2. The idea of taking motion from real life and turning it into a key for encryption feels very creative and different from normal methods.

3. The results look pretty good since the encrypted image is completely scrambled, and the randomness numbers seem strong.

4. Overall, the system works well and seems like a fun and unique way to make image encryption more secure.

CV FINAL REPORT.pdf

ORIGINALITY REPORT

2%	2%	2%	1%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	demo.ijcttjournal.org Internet Source	<1%
2	onlinelibrary.wiley.com Internet Source	<1%
3	iieta.org Internet Source	<1%
4	Tong, X.. "Image encryption with compound chaotic sequence cipher shifting dynamically", Image and Vision Computing, 20080602 Publication	<1%
5	mafiadoc.com Internet Source	<1%
6	Liang-Jia Tong, Nan-Run Zhou, Zhi-Jing Huang, Xin-Wen Xie, Ya-Ru Liang. "Nonlinear Multi-Image Encryption Scheme with the Reality-Preserving Discrete Fractional Angular Transform and DNA Sequences", Security and Communication Networks, 2021 Publication	<1%
7	www.mdpi.com Internet Source	<1%
8	Mohamed Yamni, Achraf Daoui, Chakir El-Kasri, May Almousa, Ali Abdullah S. AlQahtani,	<1%

Ahmed A. Abd El-Latif. "Lightweight image encryption using integer reversible discrete Dual-Hahn transform on embedded systems", Engineering Science and Technology, an International Journal, 2025
Publication

9 docplayer.net <1%
Internet Source

10 Jeremy Holleman. "A 3 <formula><tex>μ</tex></formula>W CMOS True Random Number Generator With Adaptive Floating-Gate Offset Cancellation", IEEE Journal of Solid-State Circuits, 5/2008 <1%
Publication

Exclude quotes	Off	Exclude matches	< 3 words
Exclude bibliography	On		