VAE-HDC: Efficient and Secure Hyper-dimensional Encoder Leveraging Variation Analog Entropy

Boyang Cheng, Jianbo Liu, Steven Davis, Zephan M. Enciso, Yiyang Zhang, Ningyuan Cao
Department of Electrical Engineering, University of Notre Dame
Notre Dame, IN, USA

ABSTRACT

Hyperdimensional computing (HDC) is a bio-inspired machine learning paradigm utilizing hyperdimensional spaces for data representation. HDC significantly improves the ability to learn from sparse data and enhances noise robustness, and also enables parallel computation. Despite these advantages, HDC's reliance on high dimensionality and operational simplicity can lead to increased hardware costs and potential security vulnerabilities. This paper introduces a novel HDC encoding strategy using variation-based analog entropy (VAE), aiming to reduce memory footprint, lower power/energy consumption, and enhance security with physically-unclonable entropy generation. The VAE cell, with high entropy robustness (30.23 − 57.76 dB SNR) and a small footprint (10 transistors), allows HDC to achieve a 14.3× reduction in vector dimensions, a 4.4× decrease in unit entropy cell area, and a 2% increase in accuracy compared to binary/multi-bit HDC. These benefits lead to a 1.3 − 4.4× area and a 327× leakage power reduction when compared to an SRAM baseline. We have designed custom low-power circuits that enable end-to-end analog entropy storage, distribution management, binding, permutation, and bundling. This analog implementation prevents data conversion during feature vector encoding, thereby significantly enhancing energy efficiency (48.5nJ per query). Furthermore, with hardware-secured basis vectors, data security is significantly improved, as evidenced by the markedly degraded visual distinguish-ability of retrieved image data and maximum of 11 dB lower PSNR.

CCS CONCEPTS

• **Hardware** → **Analog and mixed-signal circuits**.

KEYWORDS

Hyperdimensional Computation, Physical Unclonable Function, Analog Computation, Variation Analog Computation, Probabilistic Computation, Process Variation

1 INTRODUCTION

Hyperdimensional computation (HDC) is a brain-inspired computation paradigm leveraging hyper-dimensional spaces for data representation and manipulation. The distributed representation of hyper-dimensional vectors can discern subtle patterns in data, thereby enhancing its ability to process abstract information (shown in Fig. 1). Nevertheless, its parallel and simplistic computation also render HDC the advantages in leveraging state-of-the-art machine learning acceleration hardware. For example, various HDC accelerators utilizing compute-in-memory of diverse memory types (e.g., SRAM [8], PCM [9], ReRAM [16], FeRAM [7]), have been proposed, demonstrating considerable HDC hardware efficiency and accuracy improvement. Despite the advancement, because of random

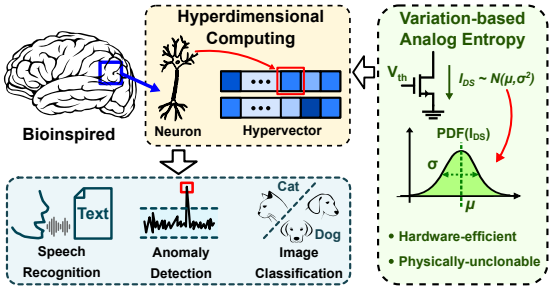


Figure 1: An overview of HDC, its applications, and variation-based analog entropy (VAE) for HDC.

variables of high-dimensionality, it remains the primary bottleneck to generate, store, access, and process the hyper-vectors, which often span thousands or tens of thousands of dimensions. Moreover, the simplistic linear operations also makes HDC's operation reversible and the model / data transparent, so that attackers can easily retrieve raw data [6] and apply adversarial attack [21].

To address these challenges, this paper introduces a novel HDC encoding scheme that harnesses the inherent analog randomness, found in transistor process variations, shown by Fig. 1. These variations, broadly applied in a physically unclonable function (PUF) for key generations [14], are explored for their potentials in symbolic representation within HDC. Utilizing such variation-based analog entropy (VAE) cells to encode random variables in HDC encoding has the potential to significantly lower memory footprint, static power consumption programming overhead and encoding energy against state-of-the-art solutions. Moreover, it presents a method for physically-unclonable generation and storage of HDC basis vectors , thus enhancing HDC's model security and data privacy.

We brief our contributions as follows:

• **Hardware Entropy for HDC**: We present a VAE-based HDC encoding method using inherent transistor randomness to simultaneously reduce hardware overhead and enhance data security. Our analysis compares VAE with state-of-the-art memory circuits / devices for HDC encoding, detailing design considerations for such variation-based symbolic representation.

• **Hardware-Efficient Encoder**: We validate the VAE-HDC's hardware efficiency with circuit-/system-level verification. The employed VAE cell with high-SNR (30.23 − 57.76dB) and small-footprint (10 transistors) decreases the HDC encoding dimensions by 14.3× (vs. 1-bit), the cell area by 4.8× (vs. 8-bit), and improves accuracy by 2% (vs. 1 and 2-bit). When target high performance (e.g., 95% accuracy on UCIHAR data), such gains lead to a 2 − 8× reduction in total transistor count compared to SRAM baselines.

• **Unclonable Basis Vector**: By integrating device-specific transistor randomness into the HDC encoders, our approach prevents direct decoding using any known or compromised basis vectors, without incurring perturbation-induced performance degradation [11].

Our experimental results on the MNIST data-set have shown markedly enhanced data privacy evidenced by significantly degraded visual distinguish-ability of retrieved image data and maximum of 11 dB lower PSNR, when the basis vectors are secured.

• **Custom Analog Circuit and Evaluation**: This work presents custom circuits designed for low-power encoding that are compatible with analog entropy. Key modules include VAE-based item memory, analog distribution management, charge-domain bidning / permutation, and time-domain bundling / conversion. Implemented with a 65nm process design kit (PDK), these circuits yield a 2.57× area reduction and a 339.7× leakage power decrease compared to SRAM baselines, while maintaining an encoding efficiency of $48.5nJ$ per query by eliminating data conversions during encoding process. Furthermore, it also shows efficiency advantages when compared state-of-the-art HDC encoder beyond CMOS baselines.

2 BACKGROUND AND DISCUSSION

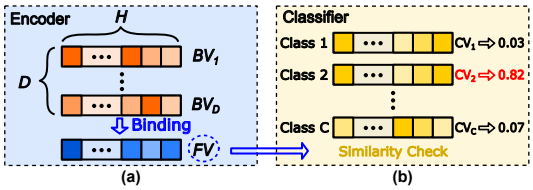
2.1 HDC Algorithm

HDC begins by encoding input data into a hyperdimensional space. An input sequence $\mathcal{X} = \{x_1, x_2, ..., x_m\}$ of m samples is encoded into a feature vector $\mathcal{FV}$, preserving both the value and the order of the samples. The encoder generates D basis vectors $\mathcal{BV}_1, \mathcal{BV}_2, ..., \mathcal{BV}_D$, which represent D quantized levels for each input sample x. Each basis vector $\mathcal{BV}$ consists of H i.i.d random variables, which may be binary, multi-bit, or real-valued; these vectors constitute what is known as the item memory. Without loss of generality, we use N-gram encoding as an example, which captures the sequence's order by permuting the basis vectors so that the basis vector $\mathcal{BV}_N$ of the N^{th} sample is permuted $N-1$ times. The feature vector given by:

$$\mathcal{FV} = \mathcal{BV}_1 \cdot \rho(\mathcal{BV}_2) \cdot ... \cdot \rho^{N-1}(\mathcal{BV}_N)$$

where ρ denotes permutation (vector circular shift), and $\cdot$ represents the element-wise binding operation [6].

During HDC training, K class vectors $\mathcal{CV}_1, ..., \mathcal{CV}_K$ are formed by aggregating feature vectors $\mathcal{FV}$ from the same class. In the inference phase, a query vector $\mathcal{QV}$ is compared against these class vectors to find the highest similarity $\delta(\mathcal{CK}_k, \mathcal{QV})$, typically employing Hamming distance [8] for binary vectors or cosine similarity [10] for multi-bit or real-valued vectors. The algorithm is shown in Fig. 2 (a) and (b).



(a) (b)

BV entropy storage	SRAM	FeFET	PCM	RRAM	VAE
non-volatility	X	✓	✓	✓	✓
area efficiency	X	✓	✓	✓	✓
no retention drift	✓	X	X	X	✓
low static power	X	✓	X	X	✓
write-free	X	X	X	X	✓
unclonability	X	X	X	X	✓
programmability	✓	✓	✓	✓	X

(c)

Figure 2: (a) An overview of HDC encoding and (b) classification. (c) A comparison table of VAE versus state-of-the-art storage circuits / devices for HDC encoding.

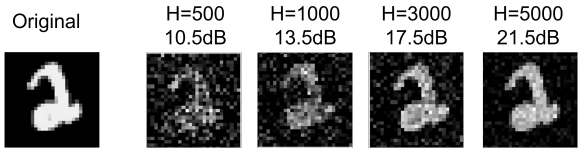


Figure 3: Handwritten '2' from MNIST: original, HDC-retrieved versions at various dimensions, and PSNR - clarity increases and security decreases with dimensionality.

2.2 HDC Encoding - VAE vs. Memory

Recent HDC accelerators have presented techniques based on different entropy storage cells, such as SRAM [8], FeRAM [7], PCM [9], and RRAM [16]. SRAM-based solutions usually require more transistors (e.g., 6T) per entropy cell , leading to increased area use and power leakage. Emerging memories, despite device-level effectiveness, come with significant system-level complexity, such as custom circuits for high programming / supply voltage (FeFET / PCM), static current (PCM / RRAM) and prolonged writing pulses (FeFET). These requirements are exacerbated by data retention drift issues, which are prevalent in nearly all emerging memory technologies. Additionally, any memory-based method for entropy generation or redistribution potentially enlarges the attack surface, heightening security and privacy risks for HDC data and models.

Against these disadvantages, VAE emerges as a promising alternative. Transistor variations are induced by manufacturing imperfections in fabrication processes such as lithography [20], deposition [22], and etching [1]. When compared to memory-based entropy storage for basis vectors, VAE demonstrates almost complete superiority (efficiency, security, robustness, hardware simplicity), except for programmability—a secondary consideration since encoding primarily demands orthogonality enabled by randomness of high dimensional. This is substantiated by the comparison in Fig 2. (c) for any form of distributed symbolic representation.

2.3 HDC Vulnerability

HDC's reversible linear operations introduce security and privacy concerns. Known basis and query vectors simplify the decoding of query feature and retrieving of raw data, as the calculation of $|x_m| = \frac{\mathcal{QV} \cdot \mathcal{BV}_m}{H}$ can reveal original samples, a vulnerability underscored in research by [11]. This risk is further exaggerated with higher HDC dimensions (increasing H) whose data retrieval attains less noise and compromises more information, as shown in Fig. 3. The key HDC vulnerabilities arise from the potential compromise of basis vectors ($\mathcal{BV}$), particularly during generation and redistribution in edge intelligence systems. While current mitigation strategies, such as perturbation-based methods suggested by [6], offer some protection, its degraded performance makes it less preferred. It remains challenging to protect the HDC at the hardware root of trust.

3 VAE CIRCUIT AND ROBUSTNESS

In this section, we discuss the employed VAE cell circuit and demonstrate its simulated entropy robustness.

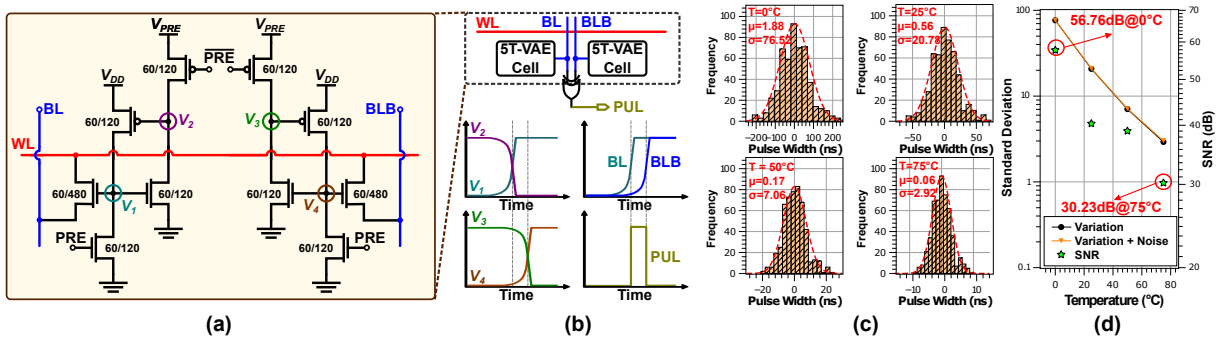


Figure 4: (a) Circuit diagram of 10T time-domain VAE differential pair. (b) Timing diagram of proposed VAE cell and its differential pair output. (c) Distribution of generated pulses of differential pair output under varying temperatures. (d) Signal-to-noise ratio and pulse standard deviation (with/without thermal noise) of VAE across varying temperatures.

3.1 Time-domain VAE

The most important design considerations for an entropy cell are high entropy quality (SNR) and low hardware footprint (transistor counts). As such, we employ a 5T time-domain PUF cell [15] as our VAE cell. This VAE cell generates random *latching delays* according to leakage current variations (shown in Fig. 4.(a). Initially, the NMOS gate (V_1) is pre-discharged to GND, and the NMOS gate (V_2) is pre-charged to V_{DD}. As the cell is evaluated, V_1 rises and V_2 falls due to sub-threshold leakage current through the PMOS/NMOS transistors. The voltage at V_1/V_2 establishes positive feedback to expedite the leakage current, causing a rapid voltage transition of V_1 to V_{DD} and V_2 to GND. The latency to this latching event is inversely proportional to the leakage current, exponentially dependent on the inherent threshold voltage variation in the sub-threshold operation region—65× greater than in the super-thershold region [14]. Hence, the latching delay is more susceptible to variation in the sub-V_{th} region, resulting in a broad distribution with a high σ/μ ratio, thus enhancing entropy robustness.

Given that HDC typically requires random variables with symmetric distributions, zero-mean entropy is derived from the 5T VAE cells. A differential VAE pair configuration is constructed, with generated voltage latching bitline (BL) and bitline_bar (BLB) input to an XOR gate when wordline (WL) is activated, as shown by Fig. 4 (b). This yields an output pulse when signal levels differ. The signal from one cell defines the variable polarity, with pulse width representing magnitude. Simultaneously, this differential arrangement minimizes spatial correlations among cells and the common mode noise, ensuring i.i.d entropy generation.

3.2 Entropy Evaluation

The Monte Carlo SPICE simulation, based on 65nm Process Design Kit (PDK), examines the pulse width distribution from the VAE cell outputs considering process variations and thermal noise. At a standard temperature of 25°C, the VAE pair displays a Gaussian distribution with an average pulse width of 0.56 ns and a standard deviation of 20.78 ns. Temperature variation studies indicate a decrease in pulse width variations (76.52-2.92 ns), shown in Fig. 4.(c), at elevated temperatures due to augmented leakage and resulting faster latching. Incorporating thermal noise into the simulation, the SNR, defined as the variance from constant process variance over the variance from thermal noise, is maintained at a high level (shown in shown in Fig. 4.(d)). It achieves 56.76 dB at 0°C. Even at 75°C, a minimum SNR of 30.23 dB or an Effective Number Of Bits (ENOB) of 4.73-bit is attainable. The maintained high SNR is attributed to simultaneously increased signal (leakage due to lowered threshold voltage) that counters the increased noise (thermal noise) at raised temperatures.

4 ARCHITECTURE AND CIRCUITS

This section details the system architecture and the custom circuits of the proposed VAE-HDC encoder. The design of the encoder emphasizes the retention of analog computation within entropy generation arrays throughout the encoding stage, thereby reducing hardware cost associated with data movement, analog-to-digital conversion and digital computation.

4.1 Item Memory with VAE Arrays

In this work, the differential 5T-5T VAE cell is extended to encompass an item memory comprising D basis vectors, each consisting of H i.i.d. random variables. The item memory activates a specific array corresponding to the quantized level of the incoming sample via wordline controller. Leveraging the non-volatile characteristic of the VAE cells, non-active arrays are power-gated to minimize leakage power.

The scope of this paper is confined to the design of the encoder, with is compatible with any standard and state-of-the-art acceleration techniques for similarity computation. We assume standard *digital processing arrays and SRAM-based* class vector storage in this work.

4.2 Analog CDF

An entropy management module transforms an input distribution into a desired output distribution. Typically, this process necessitates the use of computationally or sampling-intensive algorithms to shape the distribution, such as Monte Carlo Markov Chain [5] and acceptance/rejection sampling [2]. To enhance efficiency while preserving entropy in the analog domain, we employ a low-power analog CDF module.

It consists of three parts, namely a pre-pulse voltage converter, an operational transconductance amplifier (OTA), and a post-pulse voltage converter, as shown by Fig. 5. The pre-pulse voltage converter is a gated current source. The upstream signal will control

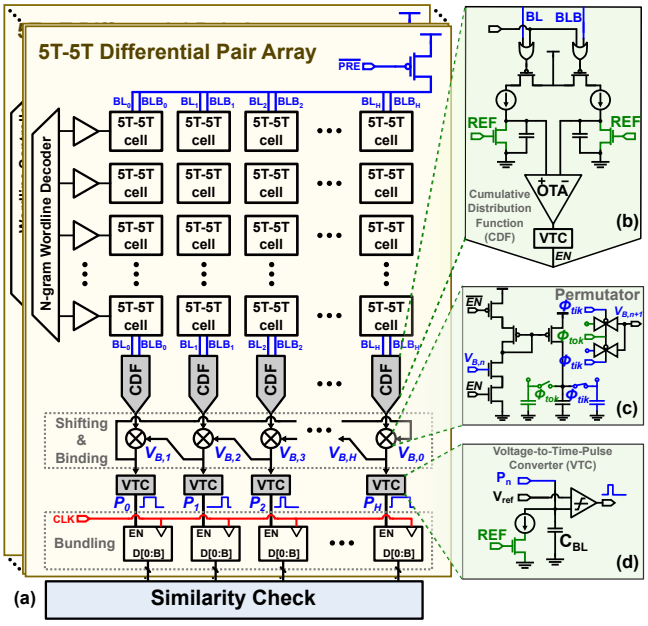


Figure 5: (a) Differential VAE pairs array for normally distributed time pulses generation. (b) Cumulative distribution function (CDF). (c) Charge-domain permutator (d) Voltage-to-time-pulse converter (VTC).

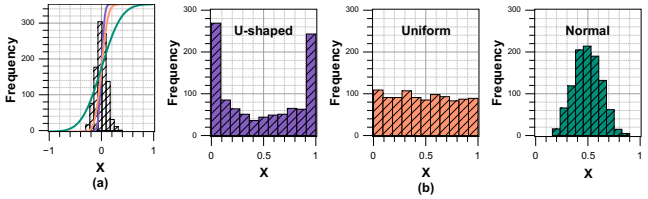


Figure 6: (a) Standard normal distribution before reshaping, and CDF curves with different parameters. (b) Reshaping the same normal distribution to U-shaped, uniform, and Gaussian distribution.

the charging time of the current source, thereby converting it into a corresponding voltage signal on the capacitor. The post-voltage pulse converter is a reverse process. The capacitor is discharged through a current source and the voltage on the capacitor is compared to a reference voltage to convert the voltage into pulse. We use an adjustable-gain OTA to fit the CDF curve. By adjusting the bias voltage of the OTA, we can change the shape of the CDF, as shown in the Fig .6 (a). In this way, when a standard normal distribution passes through the CDF, the parameters according to the CDF will become U-shaped, uniform, and normal distribution to adapt to the different needs of different algorithms for probability distribution, thereby improving accuracy, as shown in the Fig .6 (b).

4.3 Charge-domain N-gram Permutator

To perform permutation, Hypervector (HV) of prior samples needs to be shifted and multiplied with the new BV. We introduce a charge-domain permutator, which seamlessly aggregates N base HVs directly within the analog domain, eliminating the need for immediate data conversion at each base HV generation.

It consists of two parts. The first part is a voltage-controlled gated current source, which is gated by a pair of time pulse signals EN and $\overline{EN}$ generated by the upstream VAE entropy array, and the size of the output current is controlled by a bias voltage V_B. This bias voltage is derived from the voltage stored in the analog buffer on adjacent column, as shown by Fig. 5. The other part is that an analog buffer composed of three capacitors. Among them, the capacitor in the middle is the primary capacitor, which is charged by the voltage-controlled current source, and charge domain multiplication occurs, while the capacitors on both sides are secondary capacitors, which are used to latch the temporary product and output it as the bias voltage of the adjacent column. The secondary capacitors are controlled by a pair of tik-tok signals Φ_{tik} and Φ_{tok}. In tik phase, the secondary capacitor on the right follows the primary capacitor, and the secondary capacitor on the left latches the last calculation result and outputs it as biasing voltage. In tok phase, contrary to tik phase, the secondary capacitor on the left follows the primary capacitor, while the secondary capacitor on the right stores the last calculation result and outputs it. Through this permutator, charge domain permutation can be completed efficiently and without loss of precision.

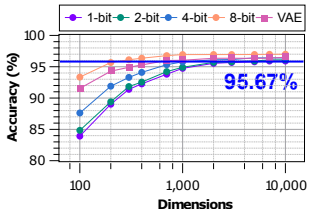
5 EVALUATION

In this section, we will discuss the evaluation results of VAE-HDC system performance, hardware efficiency and attack resilience.

5.1 Experiment Setup

The circuits are realized using a 65nm PDK and standard cell library. Analog modules such as the VAE arrays, the analog CDF, the permutator, VTC and asynchronous counters, are implemented in Cadence Virtuoso at both the schematic and layout levels to provide an accurate estimation of footprint. Simulations are conducted in Cadence Spectre. Digital modules and SRAMs are synthesized using Synopsys Design Compiler and SRAM Compiler, respectively, with area, leakage, and energy metrics derived from the synthesis results. The nominal operating conditions are set at V_{DD}=1.2V and a temperature of 25°C. For PUF evaluations, the temperature range is extended to 0 – 75°C. Throughout the experiments, Monte Carlo simulation is employed, accounting for static process variations in threshold voltage and thermal noise for each transistor.

For the baseline digital HDC encoder, we assume that each random variable is explicitly generated and stored in a 6T SRAM cell with a precision of 1, 2, 4, or 8 bits. In this baseline configuration, the processes of binding, permutation, and bundling are implemented in the digital domain quantized to same precision levels. For the VAE-based HDC, while the basis vector entropy are continuous-valued,



	Accuracy	Dims	# of T (x10^6)
1-bit	95.67%	10,000	7.68
2-bit		3,000	4.61
4-bit		1,000	3.07
8-bit		300	1.84
VAE		700	0.89

Figure 7: The plot illustrates the accuracy of human activity detection via HDC-based inference, varying by dimension and basis vector entropy representations. The table specifies the necessary dimensions and transistor counts for HDC basis vectors to maintain a certain target accuracy.

Table 1: Comparison across state-of-the-art HDC encoders.

	Proposed	Baseline	[12]	[4]	[9]	[16]	[7]
Cell type	VAE	SRAM	SRAM	SRAM	PCM	ReRAM	FeFET
Technology (nm)	65	65	28	22	90	-	-
Supply (V)	1.2	1.2	0.8	1.1	2.7	±1.5	4
Bit precision (bit)	4.73 (ENOB)	8	1	1	1	1	1
Dataset	UCIHAR / LANG	UCIHAR / LANG	LANG	UCIHAR	LANG	LANG	LANG
Accuracy (%)	**96.03 / 95.92**	**96.94 / 95.77**	**91.0****	**95.50**	**94.94**	**90.4**	**97.14**
encoder area (mm^2)	**0.83**	**2.02**	1.27 (**6.8***)	0.50 (**4.4***)	**1.39**	**0.38**	-
energy per query (nJ)	**48.5**	**1491.8**	1500 (**7835***)	160 (**562***)	**420.8**	**318000**	**85.39**
runtime power (mW)	1.56@100MHz	48.5@100MHz	267@420MHz (332@100MHz)	9.6@400MHz (8.4@100MHz)	-	-	-
array static power (μW)	**0.11**	**37.4**	-	**1600**	-	-	-

* Projected to 65nm ** Result for area size: 32 × 2048

(b)

Dataset	Acc	Precision	Dims	Area (mm^2)	Runtime Power (uW)	Static Power (uW)
LANG	93%	1-bit	10,000	2.53	12,158	46.96
		2-bit	4,000	2.02	9,707	37.49
		4-bit	1,000	1.01	4,854	18.75
		8-bit	700	1.41	6,776	26.17
		VAE	700	0.58	218	0.08
UCIHAR	96%	1-bit	10,000	2.53	12,158	46.96
		2-bit	3,000	1.91	8,621	29.43
		4-bit	1,000	1.01	4,854	18.75
		8-bit	300	0.73	4,680	17.71
		VAE	700	0.58	218	0.08

Figure 8: (a) Accuracy comparison of proposed VAE on multiple baseline configurations across different datasets. (b) Hardware overhead of different baseline configurations when achieving the same accuracy on LANG and UCIHAR datasets.

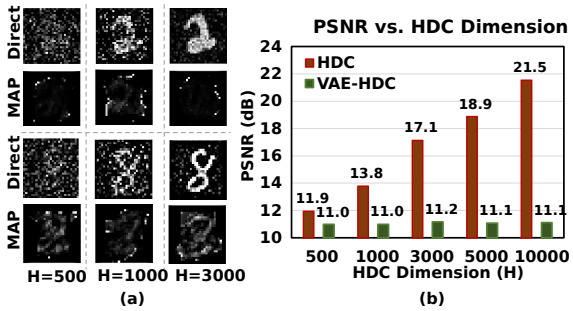


Figure 9: (a) Image retrieval with known basis-vectors (direct) and with statistical MAP attack of increasing HDC dimension; (b) PSNR with direct (HDC) and MAP (VAE-HDC) attacks of increasing HDC dimension.

we quantize the encoded feature to 4 bits for further similarity check in digital domain. The SRAM cells and digital modules, along with their hardware metrics, are also generated using an SRAM compiler and the Synopsys Design Compiler. We have constructed a classification module that incorporates synthesized digital processing elements for cosine similarity computation, as well as SRAM for storing class vectors. This module has the potential for further enhancement through the adoption of a compute-in-memory architectures, which is beyond the scope of this work.

5.2 Case Study: VAE-HDC Human Activity Detection

Prior to custom circuit integration, the feasibility and potential advantages of VAE-based HDC are evaluated through algorithmic modeling. We illustrate its application in human activity detection on open-source data-set UCIHAR [19], modeling the VAE entropy as an i.i.d. static Gaussian analog variable with zero mean. This variable exhibits dynamic noise that is 30.23 dB (as worst case SNR at $75^{\circ}C$) below the entropy strength. We benchmark this against HDC implementations using digital entropy of 1, 2, 4, and 8 bits. The corresponding accuracy improvements with increasing dimensions are depicted in Fig. 7. We observe improved accuracy for larger dimension for all entropy representations, a result of improved orthogonality at higher dimension, as well as improved accuracy-dimension trade-off for higher bit-precision due to denser information per cell, aligning with the findings of [10].

Moreover, VAE-based HDC demonstrates a more favorable accuracy-dimension trade-off compared to 1/2/4-bit HDC (consistent with 4.73 ENOB). For instance, to achieve 95.67% accuracy—the peak for 1-bit HDC—the VAE HDC requires 700 dimensions, in contrast to 10,000, 3,000, and 1,000 dimensions needed for 1, 2, and 4-bit HDC, respectively. Although VAE requires a larger dimension than 8-bit HDC (300), each VAE cell utilizes only 10 transistors (vs. 48 for 8-bit SRAM). This reduced transistor count at equivalent accuracy underscores the potential for area, leakage, and power savings with VAE compared to traditional digital SRAM baselines for HDC. These findings demonstrate the viability of VAE for HDC encoding, particularly due to high SNR and minimized transistor count per entropy unit.

5.3 System Accuracy and Hardware Efficiency

We have bench-marked the performance of VAE-HDC circuit systems vs. digital counterparts across diverse applications and open-source data-sets, including human activity detection (UCIHAR) [19], voice detection (ISOLET) [3], gesture detection (GESTURE) [17], language classification (LANG) [18], and handwritten digit classification (MNIST) [13]. Throughout these experiments, we assume

same dimension for different entropy representations where VAE-HDC accuracy saturates. We found that, for the same dimension, the VAE-HDC outperforms 1-4bits HDC, while slightly less accurate than 8-bit HDC, as shown in Fig. 8.

When we set the accuracy the same, which is set to be the maximally-achievable accuracy for binary-HDC for very large dimension, we found that VAE-HDC achieves 1.3-4.4× area efficiency gains, 21-55× energy efficiency gains compared with digital counter parts. Since unused VAE cells are power gated, it leakage power is reduced by at least 327×. Table. 1 is a comparison with the most advanced work. It can be seen that under the same accuracy, our proposed VAE-HDC has great advantages in area, runtime power and static power.

5.4 Attack Resilience

The evaluation used the 28x28 pixel MNIST dataset, where images were expanded from 784 to H dimensions using direct HDC binding. Without access to the basis vectors, an input-output attack was simulated using statistical data retrieval based on maximum a posterior probability (MAP), assuming the adversary has knowledge of 20 pairs of raw data and corresponding query vectors.

Figure 9 (a) illustrates the variance in image retrieval for two digits ('2' and '8') when employing direct encoding and statistical (MAP) decoding methods. It was noted that as the feature dimension H increases, the images retrieved through direct methods increasingly resemble the original images, yet statistical retrieval remains challenging. This trend is corroborated by the Peak Signal-to-Noise Ratio (PSNR) metrics presented in Figure 9 (b), which show a consistent rise in PSNR for direct decoding, while the PSNR for MAP decoding does not exhibit significant improvement.

6 CONCLUSION

This paper presents a novel HDC encoding strategy that utilizes the analog entropy from transistor process variations to substantially improve the efficiency and security of hyperdimensional computing. The technique is validated through simulations and system-level verifications, showing marked improvements in hardware efficiency and accuracy. It also introduces an unclonable HDC scheme to prevent data and model compromise, effectively enhancing data privacy and model security. Additionally, custom-designed analog circuits compatible with VAE are detailed, which demonstrate superior performance in terms of area and power consumption reductions. These advancements position the proposed VAE-HDC encoding approach as a powerful solution for the next generation of secure and efficient HDC implementations.

REFERENCES

[1] C. T. Black, K. W. Guarini, K. R. Milkove, S. M. Baker, T. P. Russell, and M. T. Tuominen. 2001. Integration of self-assembled diblock copolymers for semiconductor capacitor fabrication. *Applied Physics Letters* 79, 3 (July 2001), 409–411. https://doi.org/10.1063/1.1383805

[2] George Casella, Christian P. Robert, and Martin T. Wells. 2004. Generalized Accept-Reject sampling schemes. In *A Festschrift for Herman Rubin*. Vol. 45. Institute of Mathematical Statistics, 342–348. https://doi.org/10.1214/lnms/1196285403

[3] Ron Cole and Mark Fanty. 1994. ISOLET. UCI Machine Learning Repository. DOI: https://doi.org/10.24432/C51G69.

[4] Sohum Datta, Ryan A. G. Antonio, Aldrin R. S. Ison, and Jan M. Rabaey. 2019. A Programmable Hyper-Dimensional Processor Architecture for Human-Centric IoT. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems* 9, 3 (Sept. 2019), 439–452. https://doi.org/10.1109/JETCAS.2019.2935464 Conference Name: IEEE Journal on Emerging and Selected Topics in Circuits and Systems.

[5] Charles J. Geyer. 1992. Practical Markov Chain Monte Carlo. *Statist. Sci.* 7, 4 (1992), 473–483. https://www.jstor.org/stable/2246094 Publisher: Institute of Mathematical Statistics.

[6] Alejandro Hernández-Cano, Rosario Cammarota, and Mohsen Imani. 2021. PRID: Model Inversion Privacy Attacks in Hyperdimensional Learning Systems. In *2021 58th ACM/IEEE Design Automation Conference (DAC)*. 553–558. https://doi.org/10.1109/DAC18074.2021.9586217

[7] Qingrong Huang, Zeyu Yang, Kai Ni, Mohsen Imani, Cheng Zhuo, and Xunzhao Yin. 2023. FeFET-Based In-Memory Hyperdimensional Encoding Design. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 42, 11 (Nov. 2023), 3829–3839. https://doi.org/10.1109/TCAD.2023.3253766 Conference Name: IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems.

[8] Mohsen Imani, John Hwang, Tajana Rosing, Abbas Rahimi, and Jan M. Rabaey. 2017. Low-Power Sparse Hyperdimensional Encoder for Language Recognition. *IEEE Design & Test* 34, 6 (Dec. 2017), 94–101. https://doi.org/10.1109/MDAT.2017.2740839

[9] Geethan Karunaratne, Manuel Le Gallo, Giovanni Cherubini, Luca Benini, Abbas Rahimi, and Abu Sebastian. 2020. In-memory hyperdimensional computing. *Nature Electronics* 3, 6 (June 2020), 327–337. https://doi.org/10.1038/s41928-020-0410-3

[10] Arman Kazemi, Mohammad Mehdi Sharifi, Zhuowen Zou, Michael Niemier, X. Sharon Hu, and Mohsen Imani. 2021. MIMHD: Accurate and Efficient Hyperdimensional Inference Using Multi-Bit In-Memory Computing. In *2021 IEEE/ACM International Symposium on Low Power Electronics and Design (ISLPED)*. 1–6. https://doi.org/10.1109/ISLPED52811.2021.9502498

[11] Behnam Khaleghi, Mohsen Imani, and Tajana Rosing. 2020. Prive-HD: Privacy-Preserved Hyperdimensional Computing. https://doi.org/10.48550/arXiv.2005.06716

[12] Behnam Khaleghi, Hanyang Xu, Justin Morris, and Tajana Šimunić Rosing. 2021. tiny-HD: Ultra-Efficient Hyperdimensional Computing Engine for IoT Applications. In *2021 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. 408–413. https://doi.org/10.23919/DATE51398.2021.9473920 ISSN: 1558-1101.

[13] Yann LeCun and Corinna Cortes. 2010. MNIST handwritten digit database. http://yann.lecun.com/exdb/mnist/. (2010).

[14] Jongmin Lee, Donghyeon Lee, Yongmin Lee, and Yoonmyung Lee. 2018. A 445F2 leakage-based physically unclonable Function with Lossless Stabilization Through Remapping for IoT Security. In *2018 IEEE International Solid - State Circuits Conference - (ISSCC)*. 132–134. https://doi.org/10.1109/ISSCC.2018.8310219

[15] Jongmin Lee, Donghyeon Lee, Yongmin Lee, and Yoonmyung Lee. 2018. A 445F2 leakage-based physically unclonable Function with Lossless Stabilization Through Remapping for IoT Security. In *2018 IEEE International Solid - State Circuits Conference - (ISSCC)*. 132–134. https://doi.org/10.1109/ISSCC.2018.8310219 ISSN: 2376-8606.

[16] Haitong Li, Tony F. Wu, Abbas Rahimi, Kai-Shin Li, Miles Rusch, Chang-Hsien Lin, Juo-Luen Hsu, Mohamed M. Sabry, S. Burc Eryilmaz, Joon Sohn, Wen-Cheng Chiu, Min-Cheng Chen, Tsung-Ta Wu, Jia-Min Shieh, Wen-Kuan Yeh, Jan M. Rabaey, Subhasish Mitra, and H.-S. Philip Wong. 2016. Hyperdimensional computing with 3D VRRAM in-memory kernels: Device-architecture co-design for energy-efficient, error-resilient language recognition. In *2016 IEEE International Electron Devices Meeting (IEDM)*. 16.1.1–16.1.4. https://doi.org/10.1109/IEDM.2016.7838428 ISSN: 2156-017X.

[17] Giulio Marin, Fabio Dominio, and Pietro Zanuttigh. 2016. Hand gesture recognition with jointly calibrated Leap Motion and depth sensor. *Multimedia Tools and Applications* 75, 22 (Nov. 2016), 14991–15015. https://doi.org/10.1007/s11042-015-2451-6

[18] Abbas Rahimi, Pentti Kanerva, and Jan M. Rabaey. 2016. A Robust and Energy-Efficient Classifier Using Brain-Inspired Hyperdimensional Computing. In *Proceedings of the 2016 International Symposium on Low Power Electronics and Design* (San Francisco Airport, CA, USA) *(ISLPED '16)*. Association for Computing Machinery, New York, NY, USA, 64–69. https://doi.org/10.1145/2934583.2934624

[19] Anguita Davide Ghio Alessandro Oneto Luca Reyes-Ortiz, Jorge and Xavier Parra. 2012. Human Activity Recognition Using Smartphones. UCI Machine Learning Repository. DOI: https://doi.org/10.24432/C54S4K.

[20] Brian Stine, Duane S. Boning, James E. Chung, David A. Bell, and Edward Equi. 1996. Inter- and intra-die polysilicon critical dimension variation. In *Microelectronic Manufacturing Yield, Reliability, and Failure Analysis II*, Vol. 2874. SPIE, 27–35. https://doi.org/10.1117/12.250826

[21] Fangfang Yang and Shaolei Ren. 2020. Adversarial Attacks on Brain-Inspired Hyperdimensional Computing-Based Classifiers. https://doi.org/10.48550/arXiv.2006.05594

[22] Jie Zhang, Xin Zhou Wang, Wang Wang Yu, and Yu He Deng. 2017. Numerical investigation of the influence of process conditions on the temperature variation in fused deposition modeling. *Materials & Design* 130 (Sept. 2017), 59–68. https://doi.org/10.1016/j.matdes.2017.05.040