JIRBDAI

Journal of Institutional Research, Big Data Analytics and Innovation

Design and Analysis of an Image Encryption Scheme Based on Magic Square and HKDF

EZECHI, N. E.*, ADENIJI, A. A., MOGBONJU M. M.
Department of Mathematics, University of Abuja, Nigeria.
*Corresponding Author: Jide4nkiru@gmail.com

ABSTRACT

The increasing demand for secure digital image transmission has motivated the development of encryption schemes that provide strong confusion and diffusion while maintaining efficient key generation. This study proposes an image encryption framework that combines magic-square-based permutation with Elliptic Curve Diffie–Hellman (ECDH) key exchange and the HMAC-based Extract-and-Expand Key Derivation Function (HKDF). In the proposed scheme, the input image is partitioned into blocks, ECDH is used to establish a secret key from which HKDF derives pseudorandom key definition material. The derived HKDF values are associated with the image blocks and arranged in lexicographic order to generate a key dependent block of images. A fixed magic square is employed to further rearrange the image block thereby providing positional confusion. The resulting pixel values are then processed using an HKDF derived key stream through an XOR operation achieving the diffusion stage. The decryption process reverses the encryption operations to recover the original image. Experimental evaluation demonstrates that the encrypted images exhibit approximately uniform histograms, high entropy value of 7.999840 bits, NPCR value of approximately 99.6% and UACI of approximately 33.4%.

KEYWORDS: Magic Square, Image Encryption, Elliptic Curve Diffie-Hellman (ECDH), Hash Based Key Definition Function (HKDF).

I. INTRODUCTION

Cryptography is the art of rendering information exchange between two parties incomprehensive to any unauthorized person. Cryptography is by no means new as it has been very popular among the military, criminal gang and today increasingly becoming very important in our human pursuit beyond its uses in the intelligence domain. Every time a credit card is swiped or a computer is used to send emails, a security method built from a cryptosystem is applied. The digital age has ushered in an unprecedented era of information exchange, where images have become one of the most valuable forms of communication. Image cryptography is a technique of transforming images into unreadable format for and sending it through an insecure channel and preventing unauthorized parties from tampering or modifying the image. The goal of a good image encryption process is to ensure that only authorized users can view the image. A fundamental principle in image encryption is the use of confusion and diffusion introduced by Claude (1949). The confusion aims at changing pixel position while the diffusion aims at changing pixel values.

Elliptic curve Cryptography (ECC) is a powerful tool due to its high security with relatively small key spaces. ECC allows smaller keys to provide equivalent security. The use of elliptic curves in cryptography was suggested independently by (Koblitz 1987) and Miller (1986). Elliptic Curve Diffie-Hellman (ECDH) is a secure key agreement protocol that enables two parties each having an Elliptic curve public and private key pair to establish a shared secret over an insecure channel, allowing them to encrypt subsequent communications. The mathematical representation of an

Volume 2, Issue 2, 2026
https://doi.org/10.5281/zenodo.22165070

elliptic curve over a finite field is expressed as $y^2 = x^3 + ax + b$ where $a, b \in \mathbb{F}_p$ satisfying $4a^3 + 27b^2 \neq 0 \ (mod\ p)$. The shared secret generated by ECDH is generally not suitable for direct use as a cryptographic key. To overcome this limitation, a Key Derivation Function (KDF) is employed to transform the shared secret into one or more cryptographically strong keys. Among the various KDFs available, the Hash-based Message Authentication Code (HMAC)-based Key Derivation Function (HKDF).

Magic squares is a matrix of n rows by n columns. Its values are integers which are arranged such that the sum of the n horizontal, vertical or main diagonal lines is always the same (Hussein and Meholi 2018). In general, magic squares remain magic if the same positive integer is added to each number in the square or each number in the original square is multiplied by the same number. The magic constant or magic sum, M is the sum of any row, or column, or diagonal in the magic square. Every normal magic square has a constant dependent on the order n, calculated by the formula $M = \frac{n(n^2+1)}{2}$.

Although magic square can permute image pixel effectively, using it alone to encrypt images will not be secure because the security of an encryption process depends heavily on randomness and unpredictability of the generated keys. To strengthen key generation, the use of HKDF provides a secure key agreement mechanism that enables communicating parties to establish a shared secret. By utilizing the structural properties of magic squares and the use of HKDF key definition algorithm makes encryption of images more secure and decryption easier.

II. RELATED WORK

Different encryption methods have been proposed to protect private information from being accessed by a third party. Some of these methods are:

Chum and Xiaowen (2010) use cryptographic hash function to improve the security and performance of secret sharing schemes based on Latin square or its critical sets. They were able to store a partial Latin square in a hash for a fast retrieval of the shared secret. They set up an ideal perfect $(t + 1, n)$ threshold scheme with different desirable properties. The security of their scheme depends on the number of Latin squares. If the number is too large for the attacker to do the exhaustive search, it will be safe. Sahni & Ojha (2012) utilized the 8×8 magic square to establish a new platform to generate key and encrypt data. They used magic square generalized image and scheme based on random one-time pad. Babayo & Garba (2015) investigated the Loubere Magic Squares and found that the Loubere magic squares are always recognized with center piece C and Magic sum.

Sowmiya *et al.* (2017) proposed the Pan Magic Square (PMS) encryption algorithm for image encryption. This technique provides additional level of security to the image by changing the RGB value of each pixel in an image. Rapeed & Sadiq (2018) presented an image encryption model based on the chaotic technique. Their results show that the technique highly rebuts the statistical attacks such as histogram analysis in which the encrypted image has a completely inform histogram. They also show that the correlation value for the encrypted image is tiny (close to zero), nonetheless, the encrypted image entropy value is selected to be close enough to the theoretical value. Finally, they show that encryption technique has fair sensitivity to the key changing and the time for both image encryption and decryption is very short.

Amounas and El Kinani (2014) introduced an approach for image encryption using Elliptic Curve Cryptography (ECC) where the plain image is divided into blocks called data matrix. The

Volume 2, Issue 2, 2026
https://doi.org/10.5281/zenodo.22165070

cryptosystem used a different key that is generated using ECC for mapping and another key for the encryption process. The mapping method introduced is very fast with low complexity and computation. It converts an image pixel value to a point on a predefined elliptic curve over finite field using transformation algorithm. ParmaNand *et.al* (2014) encrypted image using ECC. First, they converted an image into binary numbers and then map the image into square grid. Then, they transformed each pixel in the square grid into the elliptic curve and encrypt them using ECC. Their technique was implemented for BMP images of different sizes in C language.

Kaliswaran & Mohamed (2022) proposed an ECC dependent image encryption scheme utilizing an enhancement strategy based on the Ant Colony Optimization algorithm (ACO). In the private key generation step of the ECC system, they used an ACO based optimization process to boost the efficiency of the picture encryption. The images output that they got was used as a health attribute in the optimization phase such as the Peak Signal to Noise Ratio (PSNR). Umar *et.al* (2022) proposed a novel image encryption scheme that is based on a ring of integers rather than on a finite field It avoids the traditional way (group law) of generating an Elliptic Curve (EC). Furthermore, it imposes a bound on the y-coordinate of the EC and one does not have to check all the possible values over the underlying structure. Their scheme had three main steps. In the first step, they mask the plain image using points of an EC over a finite ring. In step two, they created diffusion in the masked image with a mapping from the EC over the finite ring to the EC over the finite field. To create high confusion in the plain text, they generated a substitution box (S-box) based on the ordered EC, which is then used to permute the pixels of the diffused image to obtain a cipher image.

Essaid *et al.* (2018) proposed a new image encryption scheme based on confusion and diffusion using an Enhanced Skew Tent Map (ESTM). They conducted simulations for securing color and grayscale images, and performance evaluations including Lyapunov exponent, distribution density and bifurcation diagram showed that the proposed map produced a uniform distribution of the values taken by the new map. They used a key space of 128 bits that protects the algorithm from brute-force attack. Ronal, (2020) introduced a new form of elliptic curve in generalized Huff's model. He also formulated a formula for point addition and doubling on the affine, projective, Jacobian, Lopez-Dahab coordinates and embedded the curve into $P^{|} - P^{|}$ system.

Hiba & Ammar, (2023) introduced an efficient approach based on block matrices integrated with elliptic curves. They proposed two protocols for key generation using Elliptic curve Diffie-Hellman algorithm on block matrices. He *et al.,* (2025) introduced a robust non-linear RN chaotic system, combining two chaotic maps to enhance unpredictability and expand the chaotic interval. They then proposed an encryption process scheme developed by integrating this system with Elliptic Curve Diffie-Hellman key exchange, Hierarchical Key Derivation Function (HKDF) and dynamic chaotic S-box generation. The scheme achieved near-ideal entropy levels (~7.999), high NPCR (>99.6%) and UACI above 32%, and was resistant to security attacks. They were also able to authenticate the image using ECDSA.

Bagus *et al.,* (2025) proposed a hybrid cryptographic framework for secure digital image encryption, integrating HKDF-SHA256 with DNA-inspired encryption. Their scheme used a multi-layered encryption approach that employs DNA-based transformation and chaotic pixel permutation for encrypting medical images in digital forensics. Existing approaches have investigated image encryption on magic square based on chaotic maps, ECC/ECDH based key establishment and HKDF based key derivation separately or in other hybrid encryption systems. This work uses an ECDH- based key generation mechanism together with HKDF for key definition combined with

Volume 2, Issue 2, 2026
https://doi.org/10.5281/zenodo.22165070

magic square permutation and XOR diffusion to improve security and resistance against Brute force attack.

Theoretical Background

(a). Elliptic Curve Diffie-Hellman Key Exchange (ECDH)

The elliptic curve Diffie -Hellman is a public key exchange algorithm that allows two parties to securely establish a shared secret over an insecure communication channel. If Alice and bob want to communicate a secrete message using ECDH key exchange protocol, then they have to agree to a particular elliptic curve $E(\mathbb{F}_p)$ and a specific point P on $E(\mathbb{F}_p)$. Alice then picks a secret integer $n_A$and does not reveal it to anyone. Likewise, Bob also chooses a secret integer n_B and also keeps it secret. They both use their secret key to compute their public key Q_A and Q_B.

$Q_A = n_A P$ and $\quad Q_B = n_B P$

Alice computes Bob computes

After computing Q_A and Q_B, Alice and Bob exchange this on an unsecured communication channel. Alice and Bob then use their secret integer to compute $n_A Q_B = (n_A n_B)P = n_B Q_A$, which they can use as a key to communicate privately.

Key Derivation Function

Among the various KDFs available, the Hash-based Message Authentication Code (HMAC)-based Key Derivation Function (HKDF) has become the preferred choice for this paper due to its strong theoretical foundation, efficiency, and security. When integrated with ECDH, HKDF enhances the security of the overall cryptographic system by converting the raw ECDH shared secret into keys that possess high entropy and are suitable for cryptographic applications. HKDF consists of two stages:

The Extraction Stage

The extract phase converts the input keying material into a fixed-length pseudorandom key (PRK).

$$PRK = HMAC(salt, IKM)$$

Where PRK connote pseudo-random key, salt is a random salt and IKM is the shared secret. It is worthy to note that PRK has the same length as the hash output.

The Expansion Stage

After obtaining PRK, we generate the final key. The first block of keys is:

$$T_1 = HMAC(PRK, T_0 \,||\, info \,||\, 1)$$

where $T_0 = \emptyset$ and || connote concatenation

The second:

$$T_2 = HMAC(PRK, T_1 \,||\, info \,||\, 2)$$

$$T_n = HMAC(PRK, T_{n-1} \,||\, info \,||\, n)$$

Finally, output keying material OKM:

$$OKM = T_1 \,||\, T_2 \,||\, T_3 \,||\, \ldots$$

Fixed Magic Square

Definition: (Fixed Magic Square): Let $n \geq 3$. A fixed magic square of order n, denoted by M_n, is the unique magic square gotten from a predetermined construction algorithm.

Volume 2, Issue 2, 2026
https://doi.org/10.5281/zenodo.22165070

This will the magic square that will be used as our reference magic square throughout this work. The construction method depends on the value of n. For
i) Odd order ($n = 2k + 1$): M_n is constructed using the Siamese (de la Loubère) method.
ii) Doubly even order ($n = 4k$): M_n is constructed using the standard complementation method.
iii) Singly even order ($n = 4k + 2$): M_n is constructed using the Strachey or LUX method, where k is a natural number.

How they are constructed

Odd order: we construct the magic square using the Siamese method, which is also known as the De la Loubère method, and it follows the following steps

i. Place the number 1 in the center of the first row.
ii. Repeat by moving one row up, one column right (wrapping around the edges).
iii. If the next cell is occupied, move one row down instead.

Typically, the movement is NE-W-S or NW-E-S.

For a 3×3 Siamese magic square

8	1	6
3	5	7
4	9	2

For a 5×5 Siamese magic square

17	24	1	8	15
23	5	7	14	16
4	6	13	20	22
10	12	19	21	3
11	18	25	2	9

Doubly even order magic square

Here $n = 4, 8, 12, \ldots$ $(n \equiv 0\ (mod\ 4))$: It is constructed by drawing $X's$ through the main diagonals of each 4×4 sub square. Fill the diagonal of each 4×4 block with the corresponding cell value of C_{ij}.

Examples

4 × 4

1	15	14	4
12	6	7	9
8	10	11	5
13	3	2	16

Volume 2, Issue 2, 2026
https://doi.org/10.5281/zenodo.22165070

8 × 8

1	63	62	4	5	59	58	8
56	10	11	53	52	14	15	49
48	18	19	45	44	22	23	41
25	39	38	28	29	35	34	32
33	31	30	36	37	27	26	40
24	42	43	21	20	46	47	17
16	50	51	13	12	54	55	9
57	7	6	60	61	3	2	64

3) Singly even magic square

Here $n = 6, 10, 14, \ldots \; (n \equiv 2 \, mod \, (4))$

i. Divide the square into four equal odd-order sub-squares.
ii. Construct each sub-square using the Siamese method.
iii. Add suitable constants to the entries of each sub square.
iv. Swap selected columns (and sometimes rows) between the sub-squares, according to the Strachey or LUX algorithm.

Example 6 × 6

35	1	6	26	19	24
3	32	7	21	23	25
31	9	2	22	27	20
8	28	33	17	10	15
30	5	34	12	14	16
4	36	29	13	18	11

III. METHODOLOGY

The proposed image encryption framework integrates the Elliptic Curve Diffie-Hellman (ECDH) key exchange and a key derivation function (HKDF-SHA 256) to securely encrypt images. A grayscale image is selected and the image is divided into $n \times n$ blocks. A key is then generated using ECDH. HKDF is introduced to derive pseudorandom key material suitable for the proposed encryption process. Next, associate the bytes gotten from HKDF with the blocks of the image, then the HKDF values are sorted in ascending order using the Lexicographic order. When this is done, a new block arrangement is formed. This new block position is then ordered using the fixed Magic Square permutation. This forms the confusion stage of the encryption.

Volume 2, Issue 2, 2026
https://doi.org/10.5281/zenodo.22165070

Lastly the diffusion stage comprises of XORing the pixel of the image to the value of the key gotten from HKDF. The decryption process takes place by reversing all the steps in the encryption process.

The Algorithm for the proposed Encryption Process

Start

↓

Original image

↓

Phase 1: Key generation

↓

Compute the shared secret Z from ECDH

↓

HKDF-Extract: $PRK = HMAC\ (salt, Z)$

↓

HKDF-Expand: $K = HKDF - expand\ (PRK, info, L)$

↓

Sort HKDF using Lexicographic order

Let $K = \{k_1, k_2, \dots, k_m\}$ be the sequence of the bytes derived from HKDF. Define a permutation π on the set $\{1,2, \dots, n\}$ such that $\pi(i) = rank\ k_i$. Then the new permuted block image order H is $H = h_{\pi(1)}, h_{\pi(2).} \dots, h_{\pi(m)}$.

↓

Phase 2: Image blocking

↓

Read grayscale image I of size $W \times W$

↓

Split blocks $I = \{B_1, B_2, \dots B_n\}$

↓

Determine fixed magic square order

↓

Phase 3: Confusion Phase

↓

Compute the confusion matrix $P = H \circ M$ where ○ is function composition

↓

Phase 4: Diffusion phase

↓

Generate key stream $S = HKDF - Expand\ (PRK, info)$

↓

Apply XOR: cipher image $C = P \oplus S$

↓

Output: C = encrypted image

↓

Stop

Volume 2, Issue 2, 2026
https://doi.org/10.5281/zenodo.22165070

IV. RESULTS AND DISCUSSION

The proposed algorithm in this paper has been applied to a number of pictures. The algorithm was implemented using Phyton. Figure 1 shows an implementation of the proposed algorithm using two separate pictures of 256 x 256 pixels and 512 x 512 pixels.

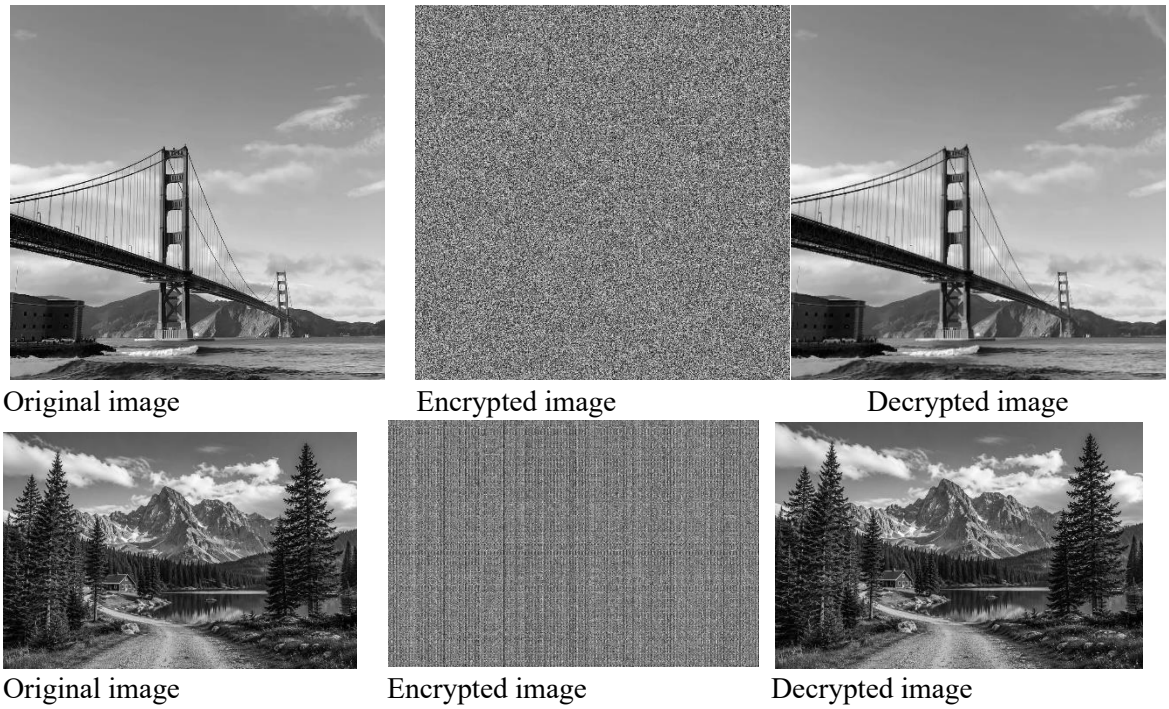

Figure 1: Implementation of the Proposed Image Encryption Framework

Histogram Analysis

In order to prevent the attacker from revealing any information from the original image, any statistical similarities between the original image and the ciphered image must be avoided. We used the histogram analysis of the image to deduce the statistical properties of the image. The histogram of an image shows the frequency distribution of pixel intensity values. An 8-bit grayscale image has intensity values ranging from 0 to 255. Figure 4.2 presents the histograms of an original, encrypted and decrypted images of the first picture in figure 1. The histogram of the original image shows significant variations with distinct peaks and valleys. This non-uniform distribution provides statistical information that an attacker could potentially exploit. The histogram of the encrypted image is rectangular or flat. This indicates that every intensity value from 0 to 255 appears with approximately equal frequency. The decrypted image histogram is the same as the original image. This confirms that the scheme is 100% lossless and that the encryption process is reversible.

The fact that the histogram of the encrypted image is flat, confirms that the XOR diffusion stage has successfully eliminated statistical redundancy present in the original plaintext.

Volume 2, Issue 2, 2026
https://doi.org/10.5281/zenodo.22165070

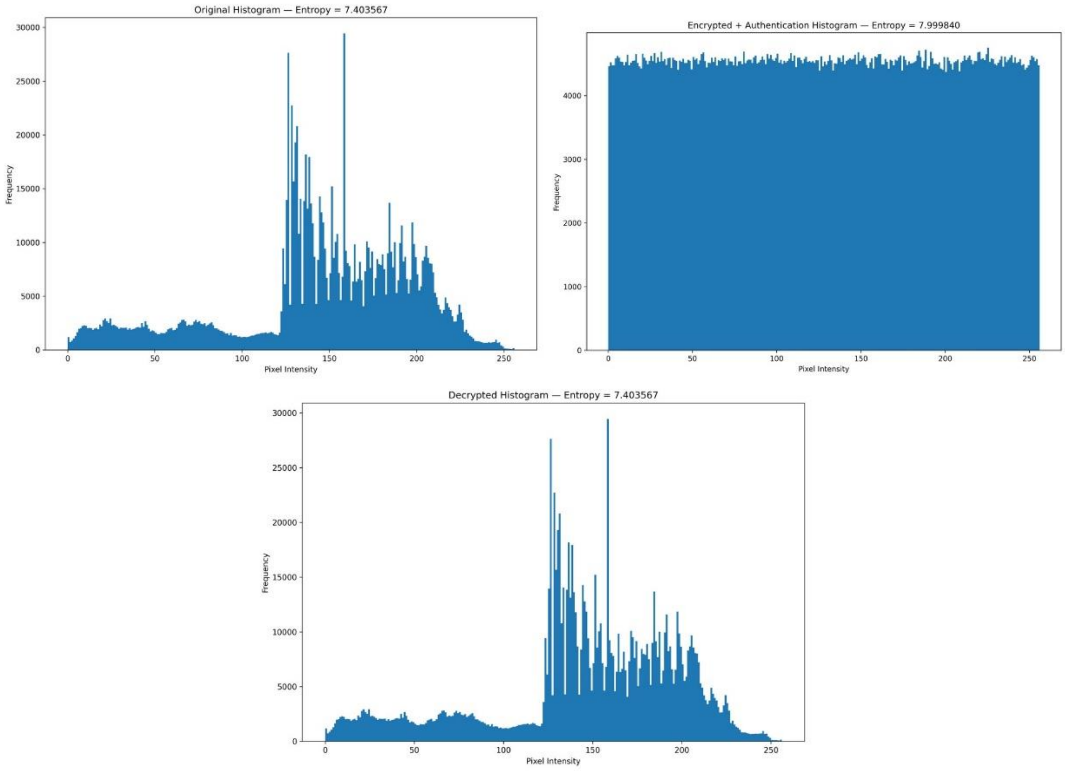

Figure 2: Histogram Analysis of the Proposed Image Encryption Framework

Entropy Analysis

Shannon entropy provides a quantitative measure of the randomness or information content in an image. For an 8-bit grayscale image with pixel values $x \in \{0, 1, \ldots, 255\}$, the entropy H is defined as:

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

where $p(i)$ is the probability of occurrence of intensity value i.

The theoretical maximum entropy for an 8-bit image is:

$$H_{max} = \log_2(256) = 8.0000$$

The entropy of the original image is 7.403567 bits and the entropy of the encrypted image is 7.999840 bits. The proposed cryptosystem increased the information entropy by 0.596273 bits/pixel, moving from 7.403567 to 7.999840 bits as seen in figure 4.3. This represents 99.99805% of the theoretical maximum randomness.

Volume 2, Issue 2, 2026
https://doi.org/10.5281/zenodo.22165070

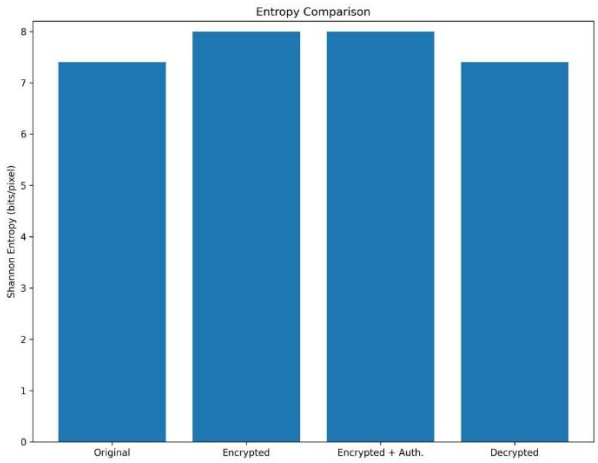

Figure 3: Entropy Comparison

The Number of Pixel Change Rate (NPCR)

The Number of Pixels Change Rate (NPCR) evaluates the confusion property of an encryption scheme. It measures the percentage of pixels that change in the ciphertext when a single pixel in the plaintext is modified. A high NPCR value indicates that the encryption scheme is highly sensitive to small changes in the plaintext, making it resistant to differential cryptanalysis. The NPCR test was conducted by modifying a single pixel in the original image (changing pixel (0,0) from its original value to + 1) and encrypting both the original and modified images using the same key. The NPCR was then calculated between the two resulting ciphertext images. The results are presented in Table 1.

Table 1: Number of Pixels Change Rate of the Proposed Image Encryption Framework

Test image size	NPCR %
Image 1 256 × 256	99.62%
Image 2 512 × 512	99.64%

The NPCR value of 99.62% exceeds the ideal threshold of 99.6%, confirming that over 99.6% of the pixels in the ciphertext change when only one pixel in the plaintext is modified.

The Unified Average Changing Intensity (UACI)

The Unified Average Changing Intensity (UACI) is a critical security metric that evaluates the diffusion property of an encryption scheme. While NPCR measures how many pixels change, UACI measures how much they change on average. The ideal UACI value for a secure encryption scheme is approximately 33.46%. The UACI test was conducted simultaneously with the NPCR test: a single pixel in the original image was modified (changing pixel (0,0) from its original value to + 1), and both the original and modified images were encrypted using the same key. The UACI was then calculated between the two resulting ciphertext images. The results are presented in the table 2:

Table 2: Unified Average Changing Intensity of the Proposed Image Encryption Framework

Test Image	Image Size	UACI (%)
Image 1	256 x 256	33.45%
Image 2	512 x 512	33.46 %

Volume 2, Issue 2, 2026
https://doi.org/10.5281/zenodo.22165070

The UACI value of 33.45% is within the ideal range of 33.30% to 33.60%, confirming that the intensity changes are uniformly distributed across the entire spectrum.

V. CONCLUSION

This work integrates HKDF with a magic-square permutation for image encryption. HKDF provides the cryptographic key material whereas the magic square provides the structural mechanism for rearranging the image blocks. The derived values from HKDF are then used to determine the ordering of the image blocks, after which the magic-square permutation is applied to achieve the required rearrangement. This rearrangement serves as the confusion phase. After confusion the pixel of each block in the confusion phase is XORed with the pixel of the HKDF key produced. This serves as the diffusion phase and hence the encrypted image. The results of this algorithm show that the technique is resistant to statistical attacks such as histogram analysis in which the encrypted image has a completely uniform histogram. Also, the entropy value of 7.999840 is very close to the theoretical values. Finally, NPCR value of approximately 99.6% and UACI of approximately 33.4%. are obtained. Future work may consider comparative study with NIST post quantum algorithms.

VI. REFERENCES

Amounas, F. & EL Kinani, E.H (2014): *Security Enhancement of Image Encryption Based on Matrix Approach using Elliptic Curve*. International Journal of Engineering Inventions, 3, II:8-16

Babayo, A.M & Garba, G.U. (2015): *Loubere magic squares semigroups and groups*: Global journal of science frontier Reasearch for mathematics and decision sciences, 15, 1.

Bagus, S., Waluyo, P., Kusworo, A. & Aris, P.W. (2025) *"Autonomous Key Generation and Management Using HKDF-SHA256 for Secure DNA-Based Image Cryptography." 3rd International Conference on Computer System, Information Technology and Electrical Engineering (COSITE).*

Chum, C.S. & Xiaowen, Z. (2010): *The Latin square and the secret sharing schemes*. Group complex cryptol. 2, Pages 175-102.

Claude, S. (1949): *Communication Theory of Secrecy Systems*. Bell System Technical Journal 28,4,656-715

Essaid M., Akharraz I., Saaidi A. & Mouhib A. *(2018) A New Image Encryption Scheme Based on Confusion-Diffusion Using an Enhanced Skew Tent Map.* The First International Conference on Intelligent Computing in Data Sciences.

He Z., Abdul R., Arif, N. & Fairouz, T. (2025). *Design and Analysis of a Secure Image Encryption Algorithm Using a Non-Linear RN Chaotic System and ECC/HKDF Key Derivation with Authentication.* Scientific Reports. DOI: 10.1038/s41598-025-23592.

Hiba, H. & Ammar A. N. (2023): *Diffie-Hellman key exchange based on block matrices combined with elliptic curve:* international Journal of Intelligent Systems and applications in Engineering. 2147-6799

Hussein & Meholi (2018): *A New Method for constructing Magic Squares Using Latin Square.* International Journal of Computer Applications 179,6.

Kaliswaran S. & Mohamed P. (2022): *Image Encryption the use of Elliptic curve Cryptography with Act colony Optimization Algorithm*. NeuroQuantology: 20,10,10782-10787

Koblitz, N. (1987): *Elliptic Curve Cryptosystem:* Mathematics of computation .48(177): 203-209

Miller V. (1987): *Use of Elliptic Curves in cryptography*: Advances in Cryptology -CRYPTO '85 proceedings. Lecture Notes in Computer Science. 85.417-426

https://doi.org/10.5281/zenodo.22165070

ParmaNand, A., Bhairvee S.& Divyanshu Chauhan (2014): *Image Encryption and Decryption us ing Elliptic Curve cryptography*: International journal of advanced Research in science and Engineering. 3, 10.

Rageed, H. A. & Sadiq A.M. (2018). *A new Algorithm based on magic square and a novel chaotic system for image encryption*. J.intell.syst.2029; 129(1), 1202-1215

Ronal, P. C. (2020): *Mathematical Aspects of Elliptic curve Cryptography*. Google search

Sahni, M. & Ojha, D.B. (2012): *Magic square and cryptography.* Journal of global research in computer science 3, 12,2229-371X

Sowmiya S., Tresa M.I & Chakkaravarthy A.P. (2017): *Pixel based image encryption using magic square*. https://WWW.researchgate.net/publication / 321814424

Umar, H., Ikram, U., Naveed, A. A. & Sumaira, A. (2022): *A Novel Image Encryption Scheme Based on Elliptic Curves Over Finite Rings*. Entropy, 24, 571. https:// doi.org/10.3390/e24050571