Image Encryption Using Dynamic Salt Injection, Hybrid Chaotic Maps, and Dual Operation Substitution

Aizaz Ahmad Khattak[1], Kehinde Babaagba[1], Xiaodong Liu[1], Syed Aziz Shah[2]
[1]*School of Computing, Engineering and the Built Environment*,
Edinburgh Napier University,
Edinburgh, UK.
Emails: 40614576@live.napier.ac.uk, {K.Babaagba, X.Liu}@napier.ac.uk
[2]*Research Centre for Intelligent Healthcare*,
Coventry University,
Coventry, UK.
Email: Syed.Shah@coventry.ac.uk

***Abstract*—In today's digital world, securing the multimedia data, especially images transmitted over unsecure networks, is critically important. In this paper, a novel chaos-based image encryption algorithm is proposed, which utilises dynamic salt injection, hybrid chaotic maps and a dual operation substitution method to protect the image from digital attacks. The dynamic salt injection process creates a unique salt for each encryption instance ensuring that even identical images result in distinct hashes. The dual operation substitution serves as a pixel-level confusion technique which ensures that all identical pixels are replaced by distinct values even if same s-box value is selected. The unique diffusion-confusion components of the proposed scheme make it a secure yet lightweight scheme. Extensive security evaluation shows the effectiveness of the proposed scheme in achieving an entropy of 7.99 and a correlation of 0.005. Moreover, the equally distributed histograms and correlation plots depict the highest level of randomness achieved by the proposed encryption scheme. These results, along with other statistical security parameters, such as homogeneity, energy, and contrast validate the effectiveness of the proposed encryption scheme.**

***Index Terms*—S-Box, chaos, image encryption, confusion, diffusion, hybrid chaotic map, salt.**

I. Introduction

With the widespread use of digital technologies and the extensive exchange of multimedia, especially images over communication networks including social media platforms, it's crucial that digital images are secured effectively [1]. Image encryption, a specialized field in cryptography, protects digital images and the information contained within these images from being attacked and/or tampered with. A secure image encryption algorithm should consist of two important processes, i.e., a confusion process and a diffusion process [2]–[4]. Confusion refers to the transformation or alteration of the pixel values, whereas diffusion or permutation refers to shuffling the pixels of an image [5]. Typically, confusion is achieved through a substitution process, while diffusion, on the other hand, is achieved through permutation [6], [7]. Recently, chaos theory has been extensively utilized to make the confusion and diffusion processes more nonlinear, unpredictable, and dependent on control parameters. Chaos, in conjunction with traditional confusion and diffusion processes, enhances the security of image encryption algorithms against several attacks, such as differential attacks [8], [9].

Traditional chaotic maps, such as the logistic map, sine map, and tent map, despite possessing properties like non-linearity, dependence on initial conditions and control parameters have several drawbacks, such as a small chaotic range and low key space. Recently, utilizing techniques such as modulation and coupling, these maps are combined with others to produce hybrid chaotic maps. Hybrid chaotic maps offer a larger key space and a broader chaotic range, hence, they produce robust pseudo-random sequences [10]–[12]. These sequences, when utilized in image encryption algorithms, add an extra layer of security in the confusion and diffusion processes.

Due to the widespread use of IoT devices, and the popularity of edge and fog computing, image encryption schemes need to be computationally inexpensive, in addition to being highly secure. Most existing image encryption schemes focus on the security aspect of the algorithms but ignore the computational complexity. This paper focuses on designing an image encryption scheme that is robust and secure yet lightweight and computationally inexpensive. The proposed scheme offers a simple confusion-diffusion architecture with components responsible for making the proposed scheme robust and lightweight at the same time.

The major contributions presented in this paper are as follows:

1) A novel, highly secure yet lightweight image encryption scheme consisting of salt generation and integration with hybrid chaotic maps-controlled diffusion and confusion components is proposed and evaluated.

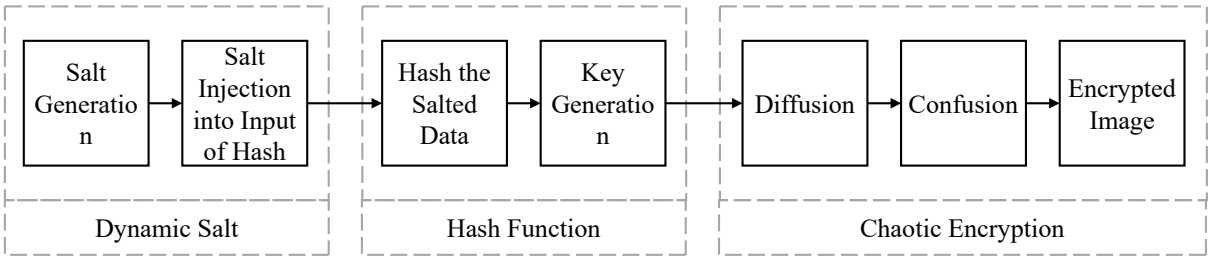


Fig. 1: Overview of the proposed encryption scheme

2) The proposed scheme introduces the use of dynamic salting process, i.e., the generation and integration of a 'Unique Salt' before applying the hash function, to ensure that the same input images will not result in the same hash. It improves the security of stored keys generated by the hash function against the dictionary and rainbow table attacks by ensuring precomputed hashes are not useful.
3) The proposed scheme utilises a dual-operation substitution technique. This technique utilizes two cryptographic operations, i.e., $\alpha = (x_{i,j} + s_{l\times m}) \mod 2^8$, and $\beta = (s_{l\times m} \gg n) \oplus (x_{i,j} \ll (8-n))$. These operations are performed on the selected s-box value prior to the substitution process. This ensures each s-box is transformed into a new outcome even if the pixel value was the same.

II. The Proposed Encryption Scheme

The proposed encryption scheme consists of three main components: (1) The dynamic salt generation and intergration, (2) Hashing of the salted data, and (3) The chaotic confusion-diffusion encryption architecture. These components are depicted in Fig. 1. The proposed scheme utilises hybrid chaotic maps to control the diffusion and confusion processes. The confusion process has two confusion phases, i.e., pixel-level confusion and bit-level confusion. For the pixel level confusion, the chaotic dual operation substitution is utilised, which is the main highlight of this scheme and makes the proposed scheme secure yet efficient. Whereas, for the bit-level confusion, a chaotic seed is generated by a hybrid chaotic map. This seed is bit-xored with the input image to transform the pixel values of the image. The important components of the proposed scheme are explained in the following subsections.

A. Dynamic Salt Injection

Salting is a concept primarily used with hashing functions to improve the security of stored passwords against dictionary and rainbow table attacks. A salt is random data added to the input of a hash function (like a password) before hashing occurs. The presence of a unique salt means that common passwords will not result in the same hash across different accounts, making precomputed attack vectors far less effective. In image encryption, salting helps in a way that even if two images are identical, using a unique salt for each hash operation ensures their hashes will be different. This can be useful for ensuring unique hash values in a system where duplicates could cause issues.

In the proposed scheme, a random salt or unique set of bytes are created using the Logistic-Sine map. It is ensured that the salt is unique for each input image or use case to ensure that the same image doesn't always result in the same hash. The next step involves combining the salt with the image Data. Before hashing, the Salt is integrated in the input image data by using bit x-or operation. SHA-256 is then used to hash the salted image data and a salted hash is obtained. This process of salt injection ensures that for duplicate images, the hash is always unique and hence, enhances the security of the encryption scheme.

B. Utilised Hybrid Chaotic Maps

The proposed scheme utilises three hybrid chaotic maps, i.e., the Logistic Sine Map, the Logistic Tent Map, and the Tent Sine Map. These hybrid maps offer a broad chaotic range and hence, a larger key space. The utilised maps control the diffusion and the confusion processes.

1) The Logistic-Sine Map: The Logistic-Sine map combines the Logistic map, i.e., $\mathcal{L}(r, x_n)$, and the Sine map, i.e., $\mathcal{S}((4-r), x_n)$. The resulting hybrid map, as presented in (1) and (2) presents a broad chaotic range and larger keyspace. Figure 2(d) shows the bifurcations diagram of the logistic sine map, showing its broad chaotic behaviour.

$$x_{n+1} = (\mathcal{L}(r, x_n) + \mathcal{S}((4-r), x_n)) \mod 1 \quad (1)$$

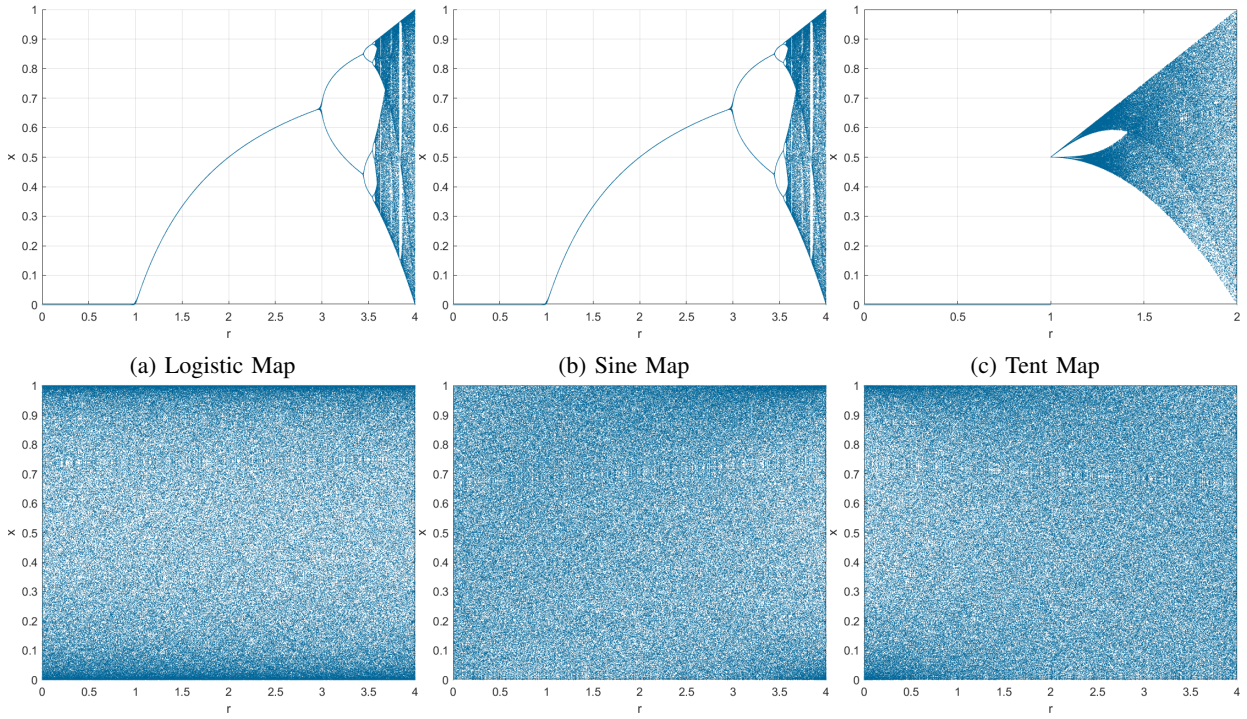
$$x_{n+1} = \left(r x_n (1 - x_n) + \frac{(4-r)}{4} \sin(\pi x_n) \right) \mod 1 \quad (2)$$

Here, $\mathcal{L}(r, x_n)$ is the Logistic function, and $\mathcal{S}((4-r), x_n)$ is the Sine function, with the parameter r lying in the range $[0, 4]$. If $x_n < 0.5$.

2) The Logistic-Tent Map: The Logistic-Tent Map combines the Logistic Map and the Tent Map. This map along with exhibiting chaotic behaviour over a large range, generates highly random pseudo-random sequences. The Logistic Map, $\mathcal{L}(r, x_n)$, is expressed as (3).

$$\mathcal{L}(r, x_n) = x_{n+1} = r \cdot x_n \cdot (1 - x_n) \quad (3)$$

Where:



(a) Logistic Map (b) Sine Map (c) Tent Map

(d) Hybrid Logistic Sine Map (e) Hybrid Logistic Tent Map (f) Hybrid Tent Sine Map

Fig. 2: Bifurcation diagrams of traditional maps vs. hybrid chaotic maps.

- x_n represents the initial condition, within the range $[0, 1]$.
- r is the control parameter, spanning the range $[0, 4]$.

The Tent map, $\mathcal{T}((4-r), x_n)$, is given as:

$$\mathcal{T}((4-r), x_n) = \begin{cases} r \cdot x_n, & \text{if } x_n < \frac{1}{2} \\ r \cdot (1 - x_n), & \text{if } x_n \geq \frac{1}{2} \end{cases} \quad (4)$$

The hybrid Logistic-Tent map, $A_{LT}(r, x_n)$, is given in (5) and (6) as:

$$A_{LT}(r, x_n) = x_{n+1} = (\mathcal{L}(r, x_n) + \mathcal{T}((4-r), x_n)) \mod 1 \quad (5)$$

$$x_{n+1} = \begin{cases} \left(r \cdot x_n \cdot (1 - x_n) + \frac{(4-r) \cdot x_n}{2}\right) \mod 1, & \text{if } x_n < \frac{1}{2} \\ \left(r \cdot x_n \cdot (1 - x_n) + \frac{(4-r) \cdot (1-x_n)}{2}\right) \mod 1, & \text{if } x_n \geq \frac{1}{2} \end{cases} \quad (6)$$

The wide chaotic range of this hybrid map is given in Fig. 2(e).

3) The Tent-Sine Map: The Tent-Sine Map combines the Tent Map and the Sine Map. As seen in Fig. 2 (f), this map exhibits a wider chaotic range. The Tent map $\mathcal{T}(r, x_n)$, is given as:

$$\mathcal{T}(r, x_n) = \begin{cases} r \cdot x_n, & \text{if } x_n < 0.5 \\ r \cdot (1 - x_n), & \text{if } x_n \geq 0.5 \end{cases} \quad (7)$$

The Sine map component, on the other hand, is given as:

$$\mathcal{S}((4-r), x_n) = \frac{(4-r) \cdot \sin(\pi \cdot x_n)}{4} \quad (8)$$

By combining these, the Tent-Sine Map, $A_{TS}(r, x_n)$, is expressed as follows:

$$A_{TS}(r, x_n) = (\mathcal{T}(r, x_n) + \mathcal{S}((4-r), x_n)) \mod 1 \quad (9)$$

$$x_{n+1} = \begin{cases} \left(\frac{r \cdot x_n}{2} + \frac{(4-r) \cdot \sin(\pi \cdot x_n)}{4}\right) \mod 1, & \text{if } x_n < 0.5 \\ \left(\frac{r \cdot (1-x_n)}{2} + \frac{(4-r) \cdot \sin(\pi \cdot x_n)}{4}\right) \mod 1, & \text{if } x_n \geq 0.5 \end{cases} \quad (10)$$

The chaotic range of the hybrid Tent Sine map is given in Fig 2(f).

C. Dual Operation Substitution– Pixel Level Confusion

The proposed encryption scheme utilises a dual operation substitution technique inspired by the substitution technique presented in [2]. The algorithm of this technique is presented in Algorithm 1. This technique utilizes two cryptographic operations, i.e., $\alpha = (x_{i,j} + s_{l \times m}) \mod 2^8$, and $\beta = (s_{l \times m} \gg n) \oplus (x_{i,j} \ll (8 - n))$. When a s-box value is selected for substitution, these operations are performed on the selected s-box value prior to substituting the pixel in the image. This ensures each s-box value is transformed into a distinct outcome even if the pixel value was the same.

D. Chaotic Seed-based Bit Level Confusion

To perform bit-level transformation on the pixels, a chaotic seed is generated by the hybrid Tent Sine map. This seed has a dimension of 256×256 and it is embedded in the substituted image by using bit x-or operation.

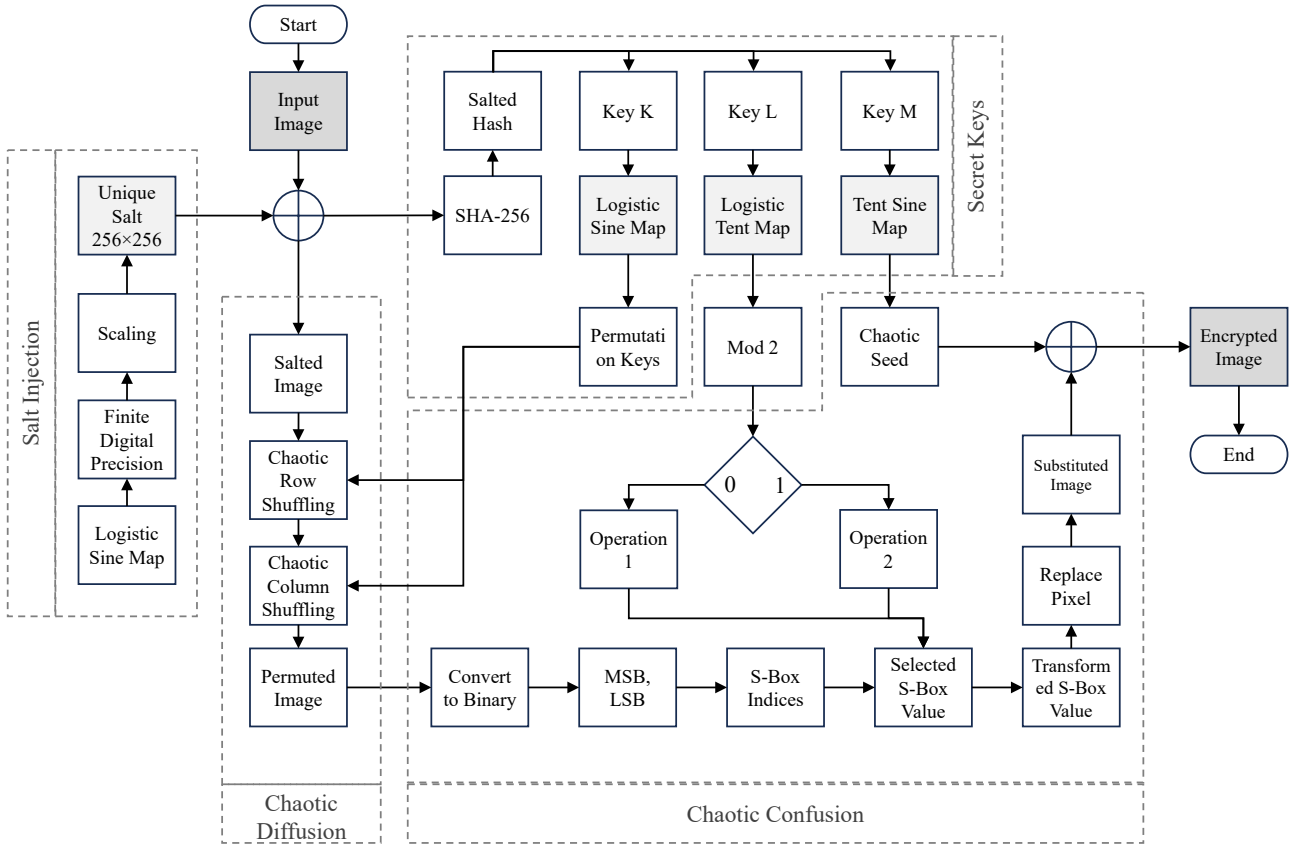


Fig. 3: The proposed encryption scheme

E. Image Encryption Process

The detailed flowchart of the proposed image encryption algorithm, entailing the steps involved in the three main modules, i.e., the salt generation and injection module, the chaotic diffusion module and the chaotic confusion module, is given in 3. The step-wise explanation is as follows:

Step 1: Image Preparation

A grayscale input image I of 256×256 is read and initialised. If the input image is of any arbitrary dimensions, it is ensured that the image is resized to 256×256 dimension.

Step 2: Generation of Salt

The salt is generated by using Logistic Sine map. The chaotic sequence generated by the Logistic Sine map is scaled and modulated to produce a salt matrix S of size 256×256, with values in the range $[0, 255]$.

Step 3: Salt injection

The salt S is then injected into the input image I_{256} using Bit x-or oepration that results in a salted image I_{salted}:

$$I_{\text{salted}} = I_{256} \oplus S \tag{11}$$

Step 4: Hashing the Salted Data using SHA-256 Hash

The salted image I_{salted} is then hashed using SHA-256 resulting in a digest. This digest is used to create control paramteres and initial conditions of the three chaotic maps.

Step 5: Diffusion via Logistic Sine Map

Two permutation keys are generated by the logistic sine map, i.e., $\{x_n\}$ and $\{y_n\}$, which are used to shuffle the rows and columns of I_{salted}, resulting in a permuted image I_{permuted}. The diffusion (permutation) process breaks the correlation between the pixels of the image.

Step 6: Pixel-level Confusion using Dual Operation Substitution

Each pixel p of the permuted image I_{permuted} is replaced by a transformed S_{box} value using one of the two operations described below. The selection of operation is controlled by the selection sequence generated by the Logistic Tent map. This process yields a substituted image $I_{\text{substituted}}$:

$$\alpha = (x_{i,j} + s_{l \times m}) \mod 2^8 \tag{12}$$

$$\beta = (s_{l \times m} \gg n) \oplus (x_{i,j} \ll (8 - n)) \tag{13}$$

where n is number of bits to be shifted, and $\gg$, $\ll$, and $\oplus$ denote right shift, left shift, and bitwise XOR operations, respectively.

Step 7: Bit-level Confusion using Chaotic Seed

A chaotic seed matrix M_{seed} is generated using the Tent Sine map, which is bit XOR-ed with $I_{\text{substituted}}$ to produce the final encrypted image $I_{\text{encrypted}}$. This step transforms the pixel

Algorithm 1 Dual Operation Substitution

Input: *permutedImage*, *S_box*
Output: *substitutedImage*
Initialize constants: $K_2 \leftarrow 5$, $n \leftarrow 3$, $C \leftarrow 100$
Initialize x_0 **for L-T map:** $x_0 \leftarrow 0.7$
Compute *sizeImg* as the total number of pixels in *permutedImage*
Initialize *operationSelection*[1..*sizeImg*] and *substitutedImage* with the size of *permutedImage*
operationSelection[1] $\leftarrow x_0$
for $k \leftarrow 2$ **to** *sizeImg* **do**
    operationSelection[k] $\leftarrow \sin(\pi \times$ *operationSelection*[$k-1$])
end for
Normalize *operationSelection* to binary values (0 or 1)
for each pixel in *permutedImage* **do**
    Convert pixel to 8-bit binary and split into MSB, LSB
    Fetch s from *S_box* using MSB and LSB as indices
    if *operationSelection*[idx] $== 0$ **then**
        new_pixel_value $\leftarrow (p + s) \mod 256$
    else
        new_pixel_value $\leftarrow$ *bitxor*(*bitshift*$(s, -n)$, *bitshift*$(p, 8-n)$)
    end if
    substitutedImage[i, j] $\leftarrow$ *new_pixel_value*
    $idx \leftarrow idx + 1$
end for
Convert *substitutedImage* to uint8 type

value at bit level and ensures that without the chaotic seed, it is impossible to reverse the encryption process.

III. Results

The novel chaos-based image encryption scheme presented in this paper has been extensively evaluated for key security evaluation parameters, such as entropy, contrast, correlation, homogeneity, energy, and histogram analysis. The results are demonstrated in the following sections.

A. Entropy Analysis

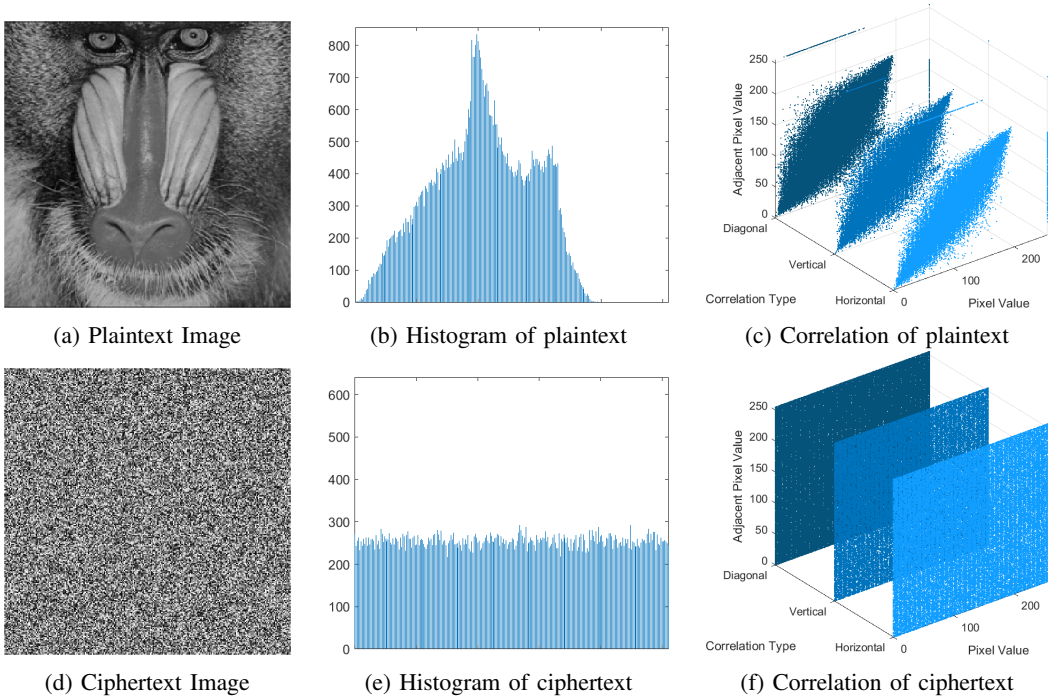
Entropy is the measure of randomness of the pixels in an image. For a 256×256 grayscale image, the ideal entropy should be 8. The entropy of the ciphertext image produced by the proposed encryption scheme is given in Table 1. It can be seen that the entropy comes out to be 7.99 showing close to ideal results.

B. Histogram Analysis

A histogram of a grayscale image shows the frequency of occurrence of each pixel in an image. The histogram of a perfectly encrypted image should be equally distributed. This means that all pixel intensities or grayscale levels in an image occur equally, making it difficult for the attacker to find the intensity information of the original image. It can seen in Fig. 4(e) that the histogram of the encrypted image is equally distributed.

C. Correlation Analysis

The correlation measures the relationship between the neighbouring pixels of an image. High correlation values depict presence of some pattern or shape in the image, whereas the low correlation values depict that the neighbouring pixels are totally different from each other. Table 1 shows the close



(a) Plaintext Image (b) Histogram of plaintext (c) Correlation of plaintext

(d) Ciphertext Image (e) Histogram of ciphertext (f) Correlation of ciphertext

Fig. 4: Results of the proposed encyption scheme

TABLE I: Resutls of evaluation parameters

Sr.	Security Parameters	Plaintext Image	Ciphertext Image
1	Entropy	7.298	7.998
2	Correlation (Plaintext/ Ciphertext)	1	0.005
3	Autocorrelation	0.8283	-0.002738
4	Energy	0.0014	0.000023
5	Contrast	553.8452	10957.1458
6	Homogeneity	0.1653	0.036238

to zero values of the correlation for the proposed encryption scheme validating its efficacy and robustness. The correlation plots givein in Fig 4 also show that the correlation coefficients are dispersed in an effective manner.

D. Statistical Security Parameters

The statistical security parameters utilised in this paper to evaluate the proposed encryption algorithm are contrast, homogeneity, and energy. For an effectively encrypted image, the contrast should be as high as possible, and energy and homogeneity should be as low as possible. The results shown in Table 1 show that the contrast of the ciphertext image is high and the energy and homogeneity results are low.

IV. Conclusion

This paper presented a lightweight yet highly secure image encryption scheme that utilised salt injection, hybrid chaotic maps and a dual operation substitution method. The presented scheme has a diffusion-confusion architecture where the confusion module contains two-level confusion components, i.e., pixel-level and bit-level. The utilised salt injection ensure that all duplicate input images result in unique hash and the dual operation substitution method ensured unique substitution values for identical pixels. These components resulted in close to ideal security results while evaluating the proposed scheme for entropy, correlation, energy, contrast, homogeneity, and histograms. The superior results validated the efficacy of the proposed encryption scheme. Furthermore, potential future work could be the inclusion of adaptive salt injection for diverse environments and integrating quantum cryptography to further enhance the security and efficiency of the proposed scheme.

Acknowledgment

This work is supported in parts by Engineering and Physical Research Council (EPSRC) Grant EP/W037076/1.

References

[1] W. Alexan, M. Elkandoz, M. Mashaly, E. Azab, and A. Aboshousha, "Color image encryption through chaos and kaa map," *IEEE Access*, vol. 11, pp. 11 541–11 554, 2023.

[2] M. S. Khan, J. Ahmad, H. Ali, N. Pitropakis, A. Al-Dubai, B. Ghaleb, and W. J. Buchanan, "Srss: A new chaos-based single-round single s-box image encryption scheme for highly auto-correlated data," *arXiv preprint arXiv:2308.10834*, 2023.

[3] E. Winarno, K. Nugroho, P. W. Adi *et al.*, "Combined interleaved pattern to improve confusion-diffusion image encryption based on hyperchaotic system," *IEEE Access*, 2023.

[4] X. Liu, K. Sun, and H. Wang, "A novel image encryption scheme based on 2d silm and improved permutation-confusion-diffusion operations," *Multimedia Tools and Applications*, vol. 82, no. 15, pp. 23 179–23 205, 2023.

[5] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, pp. 656–715, 10 1949.

[6] M. S. Khan, J. Ahmad, A. Al-Dubai, Z. Jaroucheh, N. Pitropakis, and W. J. Buchanan, "Permutex: Feature-extraction-based permutation – a new diffusion scheme for image encryption algorithms," 2023.

[7] M. S. Khan, J. Ahmad, A. Al-Dubai, B. Ghaleb, N. Pitropakis, and W. J. Buchanan, "Rna-transcrypt: Image encryption using chaotic rna encoding, novel transformative substitution, and tailored cryptographic operations," 2024.

[8] H. Ali, M. S. Khan, M. Driss, J. Ahmad, W. J. Buchanan, and N. Pitropakis, "Cellsecure: Securing image data in industrial internet-of-things via cellular automata and chaos-based encryption," in *2023 IEEE 98th Vehicular Technology Conference (VTC2023-Fall)*. IEEE, 2023, pp. 1–6.

[9] L. Asghar, F. Ahmed, M. S. Khan, A. Arshad, and J. Ahmad, "Noise-crypt: Image encryption with non-linear noise, hybrid chaotic maps, and hashing," 2023.

[10] M. T. Elkandoz, W. Alexan, and H. H. Hussein, "Logistic sine map based image encryption," in *2019 Signal Processing: Algorithms, Architectures, Arrangements, and Applications (SPA)*. IEEE, 2019, pp. 290–295.

[11] P. Ramasamy, V. Ranganathan, S. Kadry, R. Damaševičius, and T. Blažauskas, "An image encryption scheme based on block scrambling, modified zigzag transformation and key generation using enhanced logistic—tent map," *Entropy*, vol. 21, no. 7, p. 656, 2019.

[12] G. Zhang, W. Ding, and L. Li, "Image encryption algorithm based on tent delay-sine cascade with logistic map," *Symmetry*, vol. 12, no. 3, p. 355, 2020.