Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 5108331, 21 pages
https://doi.org/10.1155/2022/5108331

Research Article

A Novel Machine Learning Technique for Selecting Suitable Image Encryption Algorithms for IoT Applications

Arslan Shafique,[1] **Abid Mehmood**,[2] **Moatsum Alawida**,[2] **Abdul Nasir Khan**,[3] **and Atta Ur Rehman Khan**[4]

[1]*Riphah International University, Islamabad, Pakistan*
[2]*Department of Computer Sciences, Abu Dhabi University, UAE*
[3]*COMSATS University Islamabad, Abbottabad Campus, Pakistan*
[4]*College of Engineering and Information Technology, Ajman University, UAE*

Correspondence should be addressed to Abdul Nasir Khan; anasir@cuiatd.edu.pk

Received 7 March 2022; Revised 16 May 2022; Accepted 14 June 2022; Published 5 July 2022

Academic Editor: Muhammad Imran

The Internet of Things connects billions of intelligent devices that can interact with one another without human intervention, and during communication, a large amount of data is exchanged between the devices. As a result, it is critical to secure digital data using an encryption technique that provides a suitable degree of security. Numerous existing encryption techniques do not offer sufficient security. Therefore, it is critical to figure out which encryption technique is most appropriate for a particular kind of data. When it comes to manually deciding which encryption technique to use, the process might take a long time. In this research, we present a novel technique for selecting Encryption Algorithms (EAs) based on a particular application using pattern recognition and machine learning techniques. To accomplish this goal, we also prepare a dataset. Several machine learning techniques, such as Support Vector Machines (SVMs), Linear Regression (LR), *K*-Nearest Neighbour (KNN), Naïve Bayes (NB), Decision Trees (DT), and Random Forests (RF), are evaluated. Based on the evaluation, the SVM has been chosen as the best option for the intended technique because its classification accuracy is 98.7%. The experimental results, including accuracy, precision, recall, and F1-score, are used to gauge the performance of the suggested technique. The proposed technique is also compared with the existing techniques to demonstrate its effectiveness.

1. Introduction

Nowadays, the Internet of Things IoTs is extensively used in a variety of industries and applications, including manufacturing, agriculture, e-health, home automation, and smart cities. According to Erickson, by 2022, the world will have around 28 billion linked smart devices. Additionally, about 15 billion devices make use of Machine-to-Machine (M2M) connectivity [1]. Additionally, according to a Cisco research, the internet will be connected to about 500 billion devices by 2030 [2]. In this way, it is easy to see why the IoT has attracted the interest of developers, and researchers have given the revolutionary changes it has brought to human existence. The IoT facilitates the sharing of multimedia data across a broad number of applications, including smart transportation, smart health, smart buildings, and industry [3]. As billions of network devices interact and share potentially sensitive data, the most essential concern in the IoT is data security and privacy [4–6]. Figure 1 shows the data transmission between the several linked devices.

Different types of Encryption Algorithms (EAs) are developed over the past few decades to secure digital images during transmission between multiple connected devices for IoT applications. One advantage of EAs is their efficiency in terms of computation time. However, insufficient

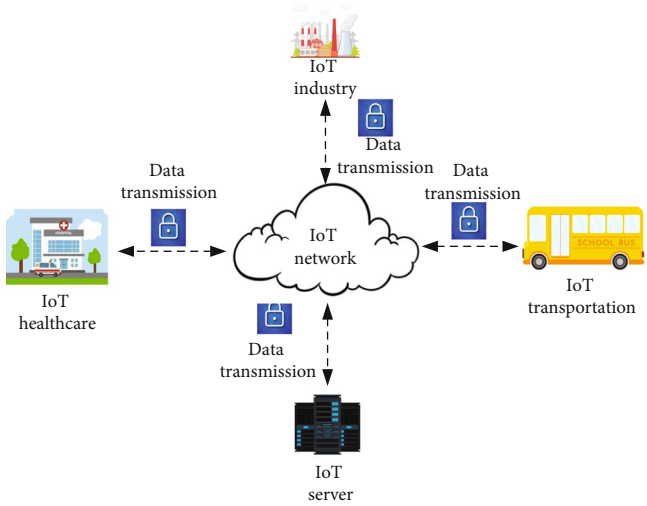


Figure 1: Data transmission between several connected devices.

encryption, as evidenced by patterns visible even after encryption, indicates a flaw in the EA [7, 8]. For proper concealment and a sufficient level of encryption of textual data, conventional Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are well-known techniques [9, 10]. There are multiple rounds of encryption involved, making these classic image encryption techniques unsuitable for real-time applications. In the case of image encryption, traditional EAs are not suitable for real-time applications because they contain several encryption rounds. To overcome such issues, several cryptosystems have been proposed in recent years [11–13]. To break the correlation between the image pixels, permutation and substitution are the most widely used techniques to secure digital images [14, 15]. In [16], Shannon proposed a theory that any EA that contains confusion (referring to permutation) and diffusion (referring to substitution or any other process that can change the pixel value) may be considered a strong cryptosystem.

Generally, two things must be offered by the EA: (a) strong security (b) and computational efficiency. There will always be a trade-off between security and complexity in terms of time. At times, a strong security algorithm may take longer to execute due to the number of mathematical operations it contains [17]. Time-efficient encryption techniques are always required for real-time applications. Various forms of pixel transformations may be employed in image encryption, including permutation, substitution, the Discrete Wavelet Transform (DWT) [18], the Discrete Cosine Transform (DCT) [19], and the Discrete Fourier Transform (DFT) [20]. All of these approaches have been extensively utilised over the last several decades and proposed a variety of algorithms, some of which are resistant to various types of security attacks, including ciphertext-only attacks, brute force attacks, and plaintext-only attacks. A cryptosystem that is vulnerable to security attacks may have two fundamental problems: (a) it is unable to adequately encrypt the plaintext image due to the identical patterns included within it. Similar patterns also correlate to a high degree of correlation between image pixels; (b) it is computationally inefficient, making it unsuitable for low-profile applications such as data transmission from a drone to a base station, which needs high-speed encryption. On the other side, to propose a time-efficient technique, one may reduce the mathematical operations used in encryption schemes, compromising security and allowing the original image's patterns to be visible in the encrypted image. The plaintext images with the smooth patterns are shown in Figures 2(a)–2(h). This indicates that there is a significant degree of correlation between the pixels, whereas Figures 2(i)–2(p) depict the corresponding ciphertext images that have been encrypted using various existing encryption schemes [21–24].

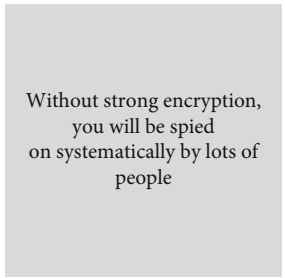
The patterns in Figures 2(i)–2(l) may be visualized, indicating that such images are encrypted using weak encryption techniques. While Figures 2(m)–2(p) are encrypted using secure encryption techniques, the plaintext image's patterns have been properly encrypted and are not visible, and the processing time required to encrypt the plaintext image is quite high.

For instance, if the image pixels have a low correlation, it is unnecessary to employ the majority of the resources available to encrypt the data included in the image. Generally, an encryption technique that employs a large number of mathematical operations is considered inefficient but extremely secure [28, 30]. Similarly, reducing the number of mathematical operations in an EA makes it more time-efficient, but it may compromise its security level [31]. In the proposed technique, EAs are categorized on the basis of computational complexity. For instance, EAs with processing times of [0.001, 1.00], [1.001, 2.000], and [2.001, ∞] are referred to as low-processing-time encryption (ELPT), moderate-processing-time encryption (EMPT), and high-processing-time encryption (EHPT), respectively.

Several metrics such as entropy, correlation, contrast, and energy [32] are evaluated in the suggested study to assess the patterns in the image, whether they are smooth or rough. After evaluating the patterns in the image, the appropriate encryption technique for that specific data may be chosen. The security parameter values may also be determined manually, but it may take a lot of time. As a result, a machine learning-based method is designed to examine the patterns in the plaintext image and suggest a suitable encryption technique, whether the image should be encrypted using a strong EA or concealed using a faster EA. The suggested approach is applicable to images in both colour and grayscale. When a colour image is used, it must be decomposed into three grayscale components, such as red, green, and blue.

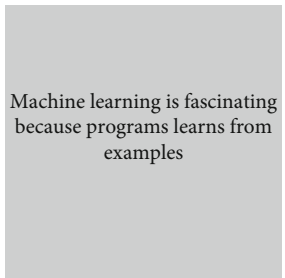
1.1. Contributions. The major contributions of this work are as follows:

(i) A machine learning model is proposed for pattern recognition-based selection of an appropriate encryption technique

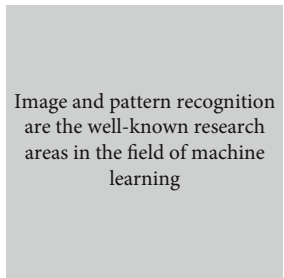


(a) Plaintext image

(b) Plaintext image

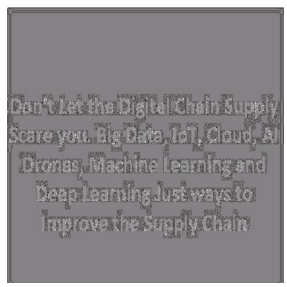


(c) Plaintext image

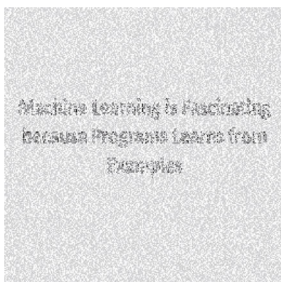


(d) Plaintext image

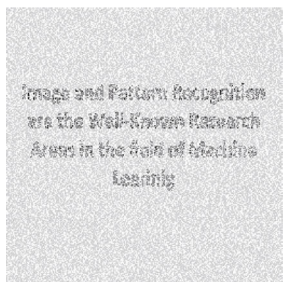
(e) Encryption using the scheme proposed in [21]



(f) Encryption using the scheme proposed in [25]



(g) Encryption using the scheme proposed in [26]



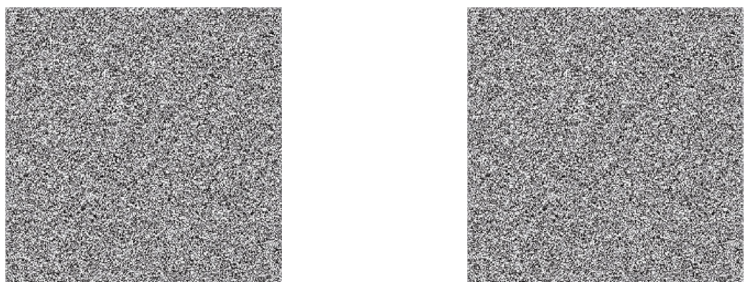
(h) Encryption using the scheme proposed in [27]

(i) Plaintext image

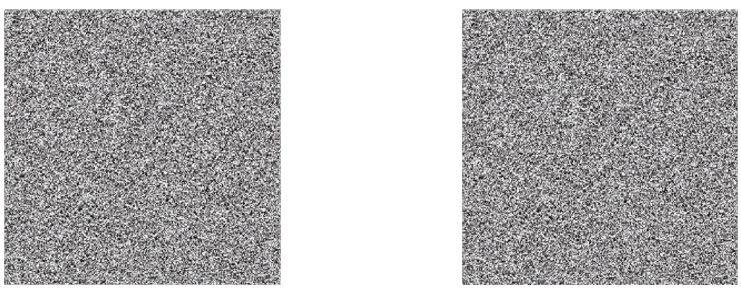
(j) Plaintext image

Figure 2: Continued.

(k) Plaintext image (l) Plaintext image



(m) Encryption using the scheme proposed in [23] (n) Encryption using the scheme proposed in [24]



(o) Encryption using the scheme proposed in [28] (p) Encryption using the scheme proposed in [29]

Figure 2: Plaintext images and their corresponding ciphertext images encrypted with the existing schemes [21, 23–29].

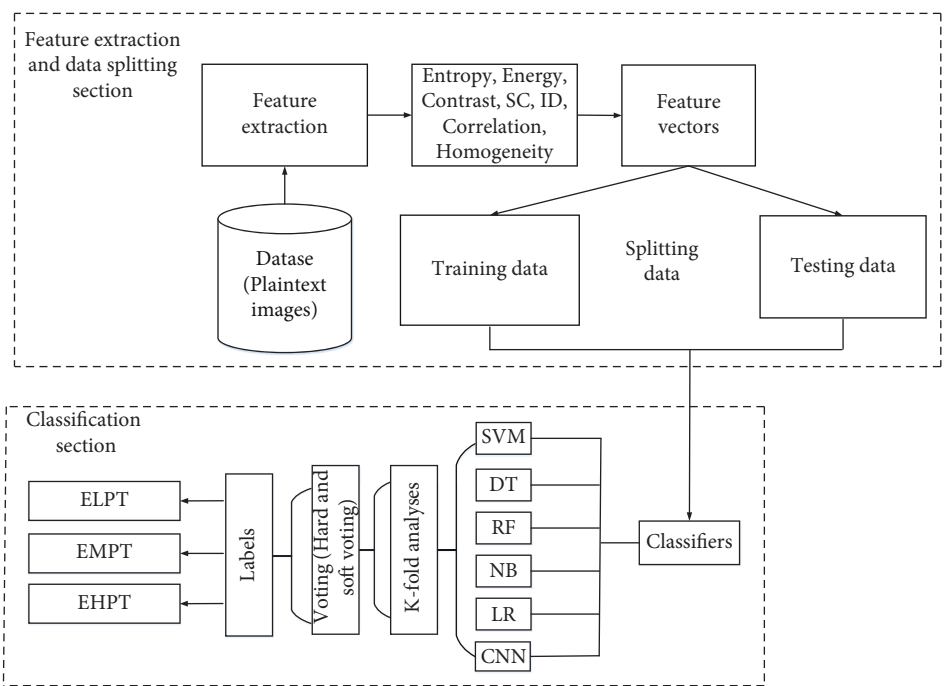


Figure 3: Proposed model for the selection of the suitable EA.

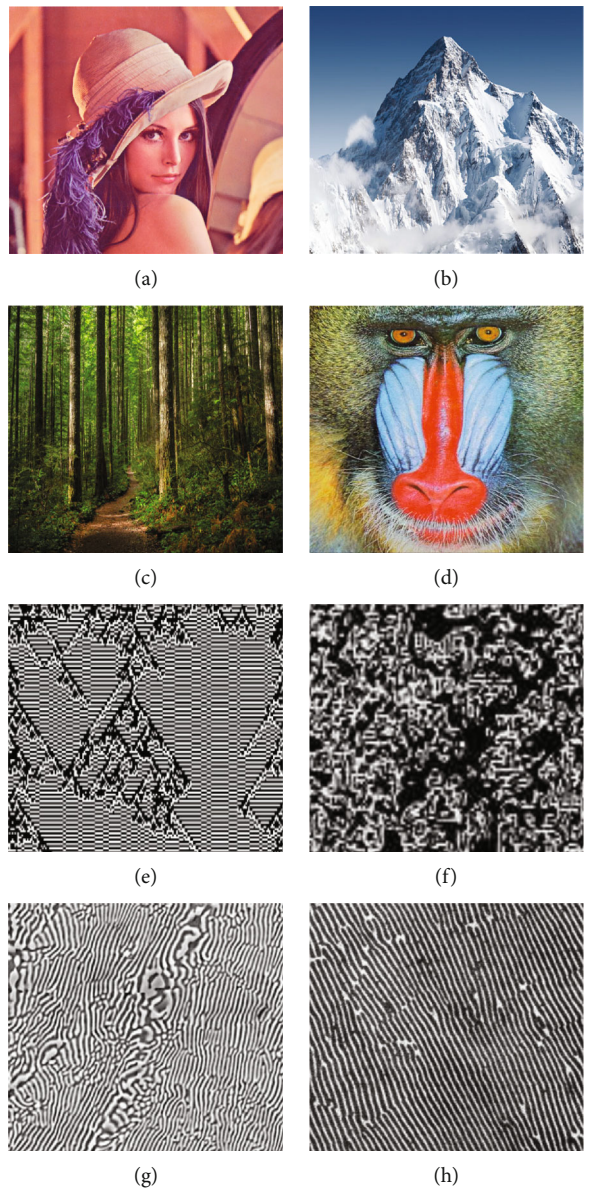


Figure 4: Information in the plaintext images (a–d) is more than the information in the plaintext images (e–h).

Table 1: Values of security parameters corresponding to Figures 4(a)–4(h).

Images	Entropy	Energy	Correlation	I_D	$(\text{Hist})^2$	Contrast	Homogeneity
Figure 4(a)	7.2416	0.7986	0.6798	250365	299.6898	8.9896	0.3367
Figure 4(b)	7.7998	0.6798	0.5710	256970	298.6410	8.6696	0.4697
Figure 4(c)	7.1720	0.6798	0.3367	256971	299.6401	8.9764	0.6798
Figure 4(d)	7.6477	0.5678	0.3665	256300	300.9963	8.6879	0.5556
Figure 4(e)	7.8099	0.0698	0.0167	240120	294.6544	9.8778	0.1352
Figure 4(f)	7.7007	0.0522	0.0331	231687	294.3330	9.9865	0.1001
Figure 4(g)	7.7556	0.0698	0.0130	246120	294.6660	9.7789	0.1336
Figure 4(h)	7.5996	0.0699	0.1978	246987	293.0299	9.7868	0.0157

(ii) The security parameters are used to identify the patterns in the plaintext image and set the appropriate intervals for each security parameter to achieve the desired task

(iii) Various machine learning algorithms are evaluated on the proposed work to find the best one

(iv) To improve the overall accuracy of the proposed model, K-fold analysis is performed to develop several models for the proposed work. The developed models are called K-models

(v) Voting mechanisms such as hard and soft voting are used to choose the final model from the several K-models

(vi) To gauge the performance of the proposed work, several tests and analyses such as accuracy, precision, F1-score, and recall are incorporated

The rest of the paper is as follows: Section 2 is dedicated to a review of the available schemes in the spatial and frequency domains. Section 3 contains preliminaries to the proposed research, including an explanation of SVM and DT. Section 4 discusses the proposed model for selecting an appropriate EA. Section 5 contains an assessment and comparison of the proposed work to previously published work. Finally, Section 6 finishes the proposed work.

2. Related Work

For secure communication, data encryption is necessary before transmission. To overcome the security issues, data can be encrypted either in the spatial domain or in the frequency domain. In the spatial domain, one can directly manipulate the pixel values. While in frequency domain encryption, first, pixels convert into their frequency domain and then further process. For instance, if a DWT is applied to the image pixels, it will convert into four different frequency subbands. Once the pixels are converted into their frequency subbands, the mathematical operations can be applied to them for further encryption. EAs can be used according to the applications and patterns existing in the plaintext image. The patterns having high correlation always required strong security EAs, whereas, in drone applications, a fast encryption speed is also required with strong security. Therefore, it is necessary to observe and analyze the patterns present in the image to select the right EA. There are several EAs that have been proposed in the last few decades which are based on either spatial domain or frequency domain.

2.1. Image Encryption in Spatial Domain. Spatial domain encryption has advanced significantly since incorporating chaos theory to secure digital images [18]. In the past few decades, chaos has been widely used in image encryption due to its several tremendous properties, such as sensitivity to initial conditions, nonperiodicity, and ability to generate pseudorandom numbers.

In [21], Anees et al. proposed an image encryption scheme comprised of two major components. One is a chaotic map, and the second is multiple substitution boxes (S-boxes). Both the components are used to break the high correlation between the image pixels. Moreover, several drawbacks of using a single S-box are addressed. To overcome the vulnerabilities that exist in using a single S-box, multiple S-boxes are used. The S-boxes are selected based on the random sequence generated using the chaotic logistic map. Using statistical analysis, it is proved that the multiple S-box scheme can perform better than the single S-box encryption scheme. However, the patterns of the plaintext image can be visualized. In [33], Ahmad and Hwang made a few improvements to the scheme proposed in [21] by adding noise in the plaintext image prior to the conversion of the noisy image into blocks. To manipulate each block of pixels, a Xor operation is performed that gives the final encrypted image.

In the encryption schemes, nonlinear components such as S-boxes also play a vital role in securing digital images. Therefore, it is crucial to use an S-box that exhibits strong cryptographic properties. In [34], Shafique et al. proposed a new methodology to construct an S-box based on a cubic logistic map, which has been given the name C-logo S-box. The purpose of proposing the S-box is to strengthen the overall EA so that the pixels of the plaintext image can be properly concealed. Several tests and analyses, such as Strict Avalanche Criterion (SAC), Bit Independent Criterion (BIC), and nonlinearity, are carried out to show the strength of the proposed S-box. A comparison reveals that the C-logo S-box performs significantly better than the other S-boxes that are present in the literature [35, 36].

In [37], Li and Yang introduced an image encryption technique based on chaos and discrete Fractional Wavelet Transforms (FWT). Confusion and diffusion operations are implemented independently, which results in a slight increase in the processing time required for encryption. Additionally, numerous cryptographic components, such as

Table 2: Defined intervals for entropy.

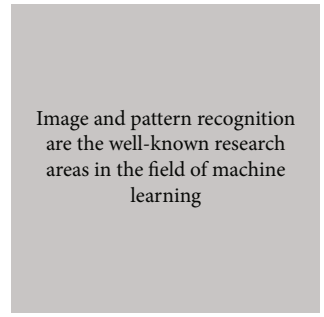
[07.999 07.900] ⟶ encryption with less processing time (ELPT)
[07.293 06.449] ⟶ encryption with moderate processing time (EMPT)
[06.423 06.001] ⟶ encryption with high processing time (EHPT)

Table 3: Defined intervals for contrast.

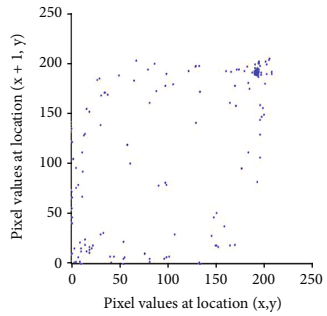
[10.5000 9.5000] ⟶ (ELPT)
[09.2500 8.7500] ⟶ (EMPT)
[08.5000 7.5000] ⟶ (EHPT)

Table 4: Defined intervals for energy.

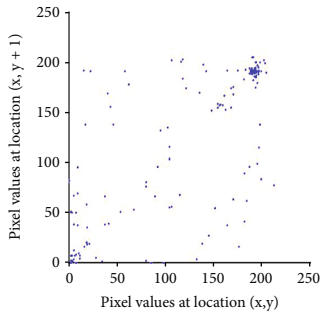
[0.01005 0.01505] ⟶ ELPT
[0.01510 0.02010] ⟶ EMPT
[0.02015 0.03495] ⟶ EHPT



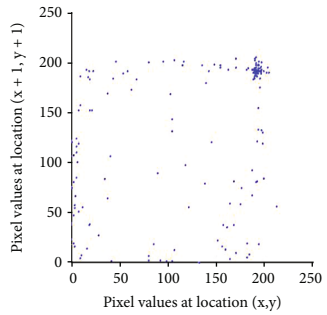
(a) Plain image with high correlation



(b) Horizontal correlation

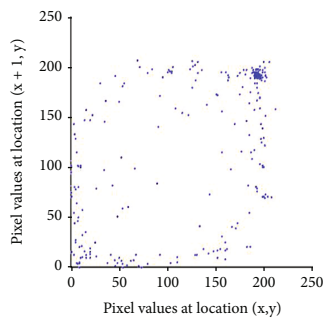


(c) Vertical correlation

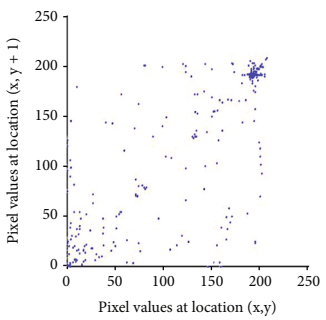


(d) Diagonal correlation

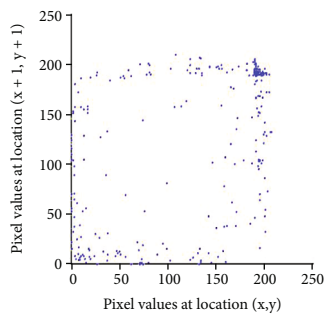
(e) Plain image with high correlation



(f) Horizontal correlation



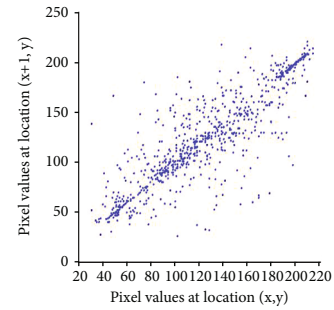
(g) Vertical correlation



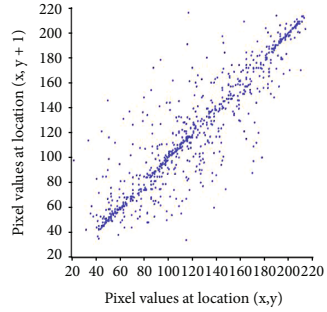
(h) Diagonal correlation

Figure 5: Continued.

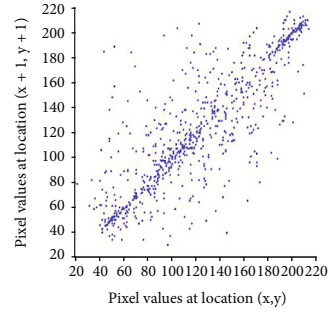
(i) Plain image with comparatively low correlation



(j) Horizontal correlation

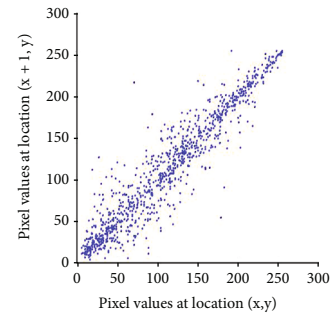


(k) Vertical correlation

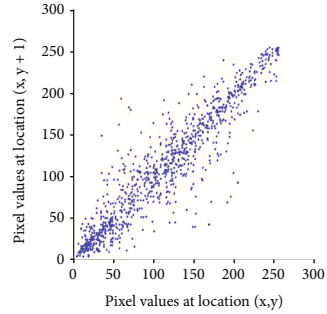


(l) Diagonal correlation

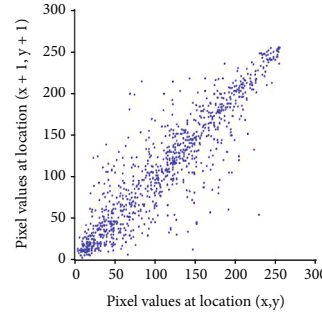
(m) Plain image with comparatively low correlation



(n) Horizontal correlation



(o) Vertical correlation



(p) Diagonal correlation

Figure 5: Plaintext images and their corresponding scattered diagrams to show the correlation between the image pixel in horizontal, vertical, and diagonal directions.

Table 5: Defined intervals for correlation.

$[-0.0012\ 0.0308] \longrightarrow$ ELPT
$[0.0001\ 0.0011] \longrightarrow$ EMPT
$[0.0000\ 0.4500] \longrightarrow$ EHPT

FWT, chaos, and quantum theory, are employed to increase the security of digital images. While using many encryption components sequentially may result in higher security, the processing time required for encryption may increase. Lin et al. [38] proposed a novel method for secure communication based on chaos theory in which mathematical operations to convert the plaintext picture to the ciphertext image are performed sequentially rather than concurrently.

Liu et al. [39] proposed a four-dimensional chaotic map-based encryption system with two encryption rounds and one hashing round. Multiple round encryption techniques often perform much better in terms of security but are not suited for real-time applications due to their increased computing time requirements. The encryption presented in [40] encountered computational complexity concerns because of the method's one-by-one encryption of the HSV components of colour images. Time complexity may be reduced by encrypting the HSV components in parallel. To make the chaos-based encryption scheme more robust, Lidong et al. [41] and Lu et al. [26] used S-box in their proposed cryptosystems. In [41], image compression is also incorporated, followed by encryption to reduce the encryption computational time. Moreover, the scrambling process is applied to the compressed image to break the correlation between the image pixels. To satisfy the criteria of confusion-diffusion proposed by Shannon [16], S-box is applied to create the diffusion in the scrambled image. A single S-box is not enough to secure the image against the deferential attack, specifically, when the image contains smooth patterns. In [26], a new chaotic map called the Logistic-sine System (LSS) is proposed, which has a wider chaotic range. The LSS is then used with the S-box in the proposed encryption scheme, which makes it comparatively more robust than the scheme proposed in [41].

2.2. Image Encryption in Frequency Domain. Apart from spatial domain encryption, frequency domain cryptosystems are also frequently used to secure the images from adversaries. Both of these types of encryption are useful to disturb the patterns of the pixels present in the image. Without a specific pattern in the image, it is difficult to read the information. Therefore, it is necessary to disturb the pixel patterns so that no one can read the information present in the image.

In [42], Rehman et al. proposed a cryptosystem in which both spatial and frequency domain sections are included. For spatial domain encryption, multiple chaotic maps used are known as chaotic logistic amp and chaotic sine map. These chaotic maps are used to generate random sequences for permutation purposes. Moreover, a chaotic sine map is also used to generate random images for diffusion purposes which are achieved using XOR operation performed on the precipher image with the random image. It is not always required to use a forward operation of any frequency transform such as DWT; one can also use its reverse operation Inverse Discrete Wavelet Transform (IDWT) to secure the digital images [43]. In [18], Shafique et al. proposed a DWT-based cryptosystem in which chaos and bit-plane extraction are the major parts. The whole scheme is consisting of three sections; the first and last sections are dependent on the spatial domain encryption while the middle section is devoted to the frequency domain section. The proposed is designed specially for those images that consist of a large number of the same patterns. As a lot of mathematical operations are included in the proposed scheme, it is somehow slower than the other existing schemes [13, 44–46]. Therefore, the scheme proposed in [18] is not suitable for real-time applications. The image encryption schemes presented in this section are based on chaos theory, bit-plane extraction, frequency transformation, and spatial domain transformation. Some of them can be used for specific purposes. For instance, the scheme proposed in [47] is useful to encrypt the image properly that can resist several security attacks, but it is not suitable for low-profile or real-time applications. Therefore, using the encryption scheme proposed in [47] is not the right choice when anyone wants to encrypt the image faster. Here, it can be noted that the orthodox selection of EA is very important for the particular kind of data. Therefore, a machine learning-based model is proposed to learn the image pattern for the selection of suitable EA.

Table 6: Defined intervals for homogeneity.

[0.4122 0.4418] ⟶ ELPT
[0.4521 0.4821] ⟶ EMPT
[0.5367 0.6125] ⟶ HLPT

3. Preliminaries

In the proposed work, several machine learning algorithms such as Decision Tree (DT), Support Vector Machine (SVM), Random Forest, *K*-Nearest Neighbour, and Logistic Regression (LR) are evaluated in which SVM and DT exhibit approximately comparable accuracy and precision. As a result, the preliminary section includes a discussion of SVM and DT. Moreover, among DT and SVM, the final selected ML algorithm is SVM as its accuracy is better than DT and other comparable ML algorithms.

3.1. Support Vector Machine. SVM implementation requires training on training data, since it is a supervised learning algorithm that takes training data as an input and predicts the label of the output based on training [48]. The training and testing datasets may or may not vary in size. The whole dataset's dimension is determined by the number of features employed. For instance, if the dataset has fourteen features, it will be fourteen-dimensional [49]. The general form of the dimension of the dataset is given below:

$$Y = X_1, X_2, X_3, \cdots, \mathrm{X}_n, \tag{1}$$

where Y is the dependent output label and X_i represents the number of independent features. The number of features may vary depending upon the output. A line that is a support vector is necessary to separate the data with maximum margins in the two-dimensional dataset. In the case of a higher-dimensional dataset, on the other hand, a plane is utilised to divide the data points rather than a line.

The proposed work makes use of an eight-dimensional dataset. As a result, it is required to determine the optimal plane for separating the data points in order to properly classify the unseen sample. The categorization function may be defined as follows:

$$\sigma(x) = T \cdot X + K, \tag{2}$$

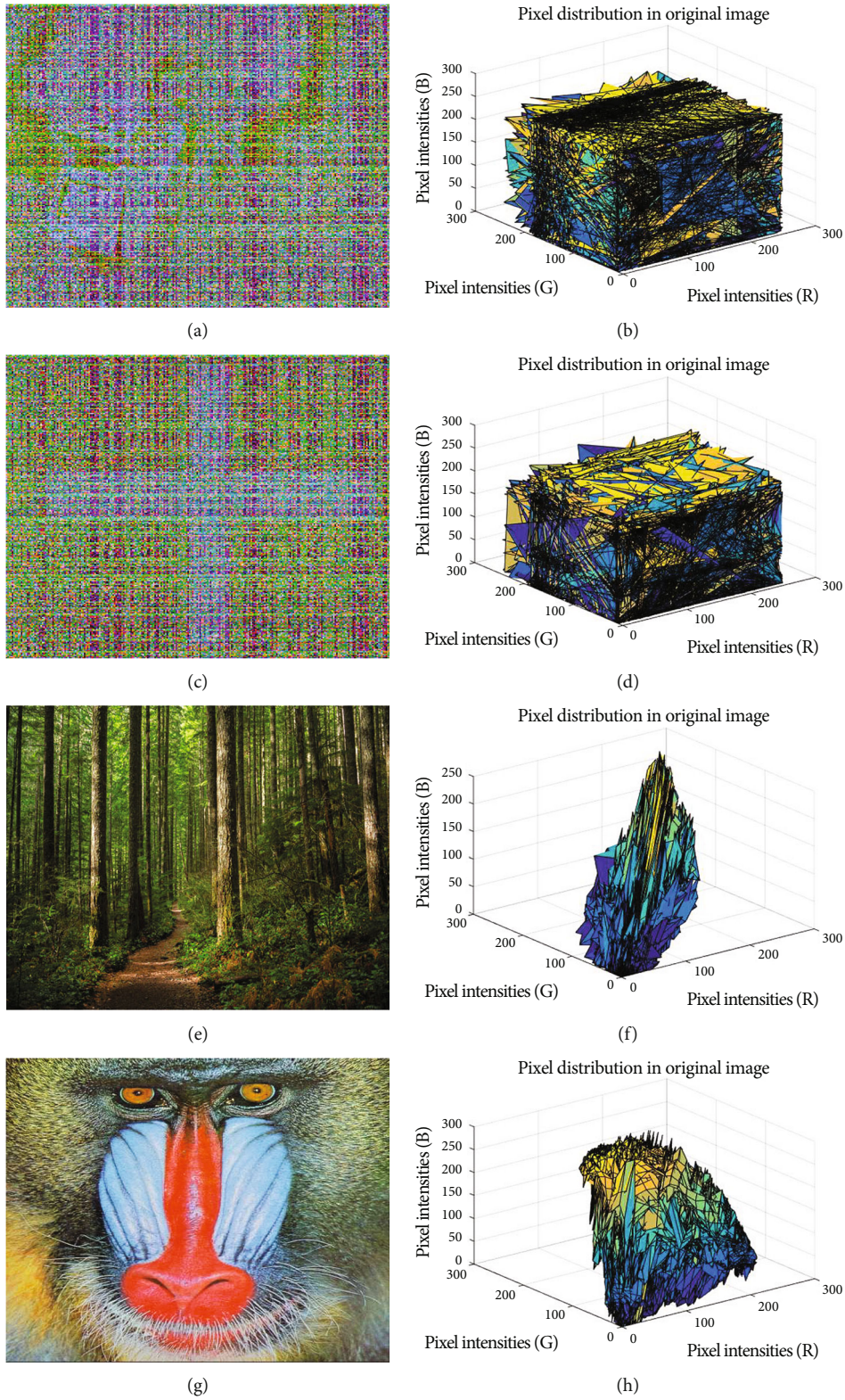


Figure 6: Pixel distribution in original and encrypted images.

where T and K are the weight vector and the intercept, respectively. However, T can be calculated as

$$T = \frac{xn - xm}{yn - ym}. \tag{3}$$

3.2. Decision Tree. DT is also a supervised learning technique to classify the data into specific classes. The growth of the tree may depend on the number of attributes used in the dataset. For determining the computational cost and classification performance, the heuristic plays a vital role in tree-growing [50]. Mostly, decision trees use an impurity-based heuristic which computes the purity of the resulting subset once the splitting attribute is applied to split the training data [51]. To build the tree for the classification purpose, a root node must be selected, which can be determined by calculating the Information Gain (IG), and the one with the highest IG will be selected as the splitting feature [52]. IG can be calculated as

$$\mathrm{IG}(X, Y) = \mathrm{Entropy}(X) - \sum_{y} \frac{|X_y|}{|X|} \mathrm{Entropy}(X_y), \tag{4}$$

where X represents the training events or feature vectors, Y represents the feature and y represents its value, X_y represents the subset of X containing occurrences with $Y = y$, and entropy (X) may be determined as follows:

$$\mathrm{Entropy}(X) - \sum_{j=1}^{|B|} T_X(b_j) \log T_X(b_j), \tag{5}$$

where $T_X(b_j)$ can be evaluated as the probability of the events belonging to b_j in X and $|B|$ is the number of labels present in the dataset.

4. Proposed Model

Numerous encryption techniques have been proposed in recent years, including chaos and transformation-based algorithms. Analyzing the statistical results of EAs indicates that some of them are insecure and do not provide enough protection [53–56].

In this article, a machine learning model that incorporates SVM is developed to determine the optimal encryption technique for the data in the form of images. The proposed work is shown schematically in Figure 3. The process for constructing the proposed model is as follows:

(i) Take a large collection of plaintext images (I) having size $M \times N$ ($[I_{ij}]_{MXN} \longrightarrow M$ and $N \in \mathbb{Z}$) in which a different amount of information is present. For instance, a few images from the dataset are shown in Figure 4 in which a significant amount of information lies in Figures 4(a)–4(d) as compared to the information present in Figures 4(e)–4(h)

Table 7: Defined intervals for histogram analysis.

[3000 4000] ⟶ ELPT
[4500 6000] ⟶ MLPT
[6500 7000] ⟶ HLPT

Table 8: Defined intervals for I_D.

[248800 247000] ⟶ EHPT
[250700 248900] ⟶ EMPT
[252600 250800] ⟶ ELPT

4.1. Features Used in the Proposed Work. Security parameters such as entropy, energy, contrast, correlation, homogeneity, histogram uniformity, and irregular deviation are considered features to select which plaintext image contains the highest, lowest, and moderate amount of information. On the other hand, peak signal to noise ratio and mean square error, both of which are security metrics, need at least two images, such as plaintext and ciphertext, in order to quantify the difference between the two. In our case, only plaintext images are considered in the proposed work.

4.1.1. Entropy. Entropy is used to find the randomness in an image. Furthermore, the entropy value corresponds to the high randomness [57]. The relation between entropy and randomness is given below:

$$\text{Entropy} \propto \text{randomness}. \tag{6}$$

The maximum entropy value for every image is determined by its bit count. For example, the maximum entropy values for an eight-bit and binary image are 8 and 2, respectively. Entropy may be stated mathematically as

$$\text{Entropy} = \sum_{x=1}^{A \times B} p(s_w) \log_2(p(s_w)), \tag{7}$$

where $p(\mathrm{s}_w)$ is the probability of occurrence of message s_w and $A \times B$ represent the number of pixels present in plaintext image.

The entropy value of an image increases in proportion to the complexity of the patterns contained inside. As seen in Figures 4(a)–4(d), the patterns are visible, indicating that the entropy value for such images is low. Similarly, the entropy values for the images shown in Figures 4(e)–4(h) will be rather high, as indicated in Table 1.

To classify the plaintext images to be encrypted either with fast, moderate, or slow processing EA, three intervals are defined in Table 2.

4.1.2. Contrast. Contrast analysis of an image allows the observer to identify the objects in the image [57]. Mathematically, it can be calculated as

$$\text{Contrast} = \sum_{c,d} |c - d|^2 p(c, d), \tag{8}$$

Table 9: Feature summary.

Features	Mathematical equations	Relationship with strong security (S.S)	Variable explanation
Energy	$\text{En} = \sum_{T=1}^{M} P(c,d)$	$\text{Energy} \propto \frac{1}{\text{S.S}}$	$P(a,b)$ is an original image
Histogram	$(\text{Hist})^2 = \sum_{k=0}^{255} \frac{g_i - t}{t}$		$t = M \times N/256$ g_i: number of gray levels
Entropy	$\text{Ent} = \sum_{x=1}^{A\times B} p(s_w)\log_2(p(s_w))$	$\text{Ent} \propto \text{S.S}$	$p(s_w)$: probability occurrence $A \times B$: no. of pixels
Contrast	$\text{Cont} = \sum_{c,d} \lvert c-d\rvert^2 p(c,d)$	$\text{Con} \propto \text{S.S}$	$p(c,d)$ is gray-level cooccurrence matrix
Homogeneity	$\text{Hom} = \sum_x \sum_y \frac{I(x,y)}{1+\lvert x+y\rvert}$	$\text{Hom} \propto \frac{1}{\text{S.S}}$	—
Correlation	$\text{Corr}_{qp} = \text{cov}\,(q,p)/\sqrt{T(q)}\sqrt{T(p)}$ $\text{Cov}(q,p) = 1/M\sum_{r=1}^{M}(q_r - G(q))(p_r - G(p))$ $T(q) = 1/M\sum_{r=1}^{M}(q_r - G(q))^2$ $T(p) = 1/M\sum_{r=1}^{M}(p_r - G(p))^2$ $G(q) = 1/M\sum_{r=1}^{M} q_r$ $G(p) = 1/M\sum_{r=1}^{M} p_r$	$\text{Correlation} \propto \frac{1}{\text{S.S}}$	Corr_{qp}: pixel correlation
Irregular deviation	$I_D = \sum_{j=0}^{255} \lvert X_i - X_h\rvert$	$I_D \propto \frac{1}{\text{S.S}}$	X_i, X_h: histogram deviations

where c and d represent the number of rows and columns of the image. $P(c,d)$ represents the number of gray levels in the occurrence matrices. The value of contrast reflects that the image contains less information. The relationship between the image pattern and contrast values is given in

$$\text{Image patterns} \propto \text{Less contrast value}. \tag{9}$$

As demonstrated in Table 1, the contrast values for the images in Figures 4(a)–4(d) are smaller than those in Figures 4(e)–4(h). This implies that the images (Figures 4(a)–4(d)) must use a robust encryption scheme to preserve the image's patterns. Using additional resources to encrypt the images (Figures 4(e)–4(h)) is not a viable option. It may be encrypted using a faster-processing encryption technique with a moderate level of security. The following intervals are given in Table 3 for the categorization of images that may be encrypted using either category of encryption methods.

4.1.3. Energy. Energy values reflect the amount of information present in the image. The higher the values of energy, the greater amount of information is present in the image [58]. Energy can be calculated using Equation (10), whereas the relationship between the amount of information and energy is given in Equation (11).

$$\text{Energy} = \sum_{T=1}^{M} P(c,d), \tag{10}$$

where M shows the total number of pixels in an image ($P(c,d)$):

$$\text{Information} \propto \text{Energy}. \tag{11}$$

Table 1 contains several energy values for various images, and it can be seen that the energy values for the images (Figures 4(a)–4(d)) are higher than the images shown in Figures 4(e)–4(h), implying that the images (Figures 4(a)–4(d)) require strong security algorithms to secure the patterns of the plaintext images. Table 4 shows the intervals for the classification of different EAs.

4.1.4. Correlation. Correlation indicates the similarity of two or more objects, i.e., correlation between the whole image or a subset of its pixels. Correlation coefficients increase as the object's similarity increases [59]. In digital images, a gradient pattern has a higher degree of correlation between the pixels than texture patterns, which indicates that images with more gradient patterns will have a higher correlation value, necessitating the use of a powerful encryption technique to break the correlation. In comparison, texture patterns in digital images have less correlation between pixels, which is very simple to eliminate even with a moderate or poor security level encryption techniques. Correlations between image pixels may be calculated using

$$\text{Corr}_{qp} = \frac{\text{cov}\,(q,p)}{\sqrt{T(q)}\sqrt{T(p)}}, \tag{12}$$

Table 10: Some portion of the dataset.

F.V no.	Images	Entropy	Energy	Contrast	Correlation	Homogeneity	I_D	Hist^2	EA
1	Plaintext-1	8	0.01	10.75	-0.5	0.392	247000	292.697	ELPT
2	Plaintext-2	7.9999	0.01005	10.745	-0.495	0.3921	247100	292.687	ELPT
3	Plaintext-3	7.9998	0.0101	10.74	-0.49	0.3922	247200 0	292.996	ELPT
4	Plaintext-4	7.9997	0.01015	10.735	-0.485	0.3923	247300	292.666	ELPT
5	Plaintext-5	7.9996	0.0102	10.73	-0.48	0.3924	247400	292.697	ELPT
6	Plaintext-6	7.9995	0.01025	10.725	-0.475	0.3925	247500	292.698	ELPT
7	Plaintext-7	7.9994	0.0103	10.72	-0.47	0.3926	247600	292.341	ELPT
8	Plaintext-38	7.9993	0.01035	10.715	-0.465	0.3927	247700	292.101	ELPT
9	Plaintext-9	7.9992	0.0104	10.71	-0.46	0.3928	247800	292.198	ELPT
10	Plaintext-10	7.9991	0.01045	10.705	-0.455	0.3929	247900	292.699	ELPT
11	Plaintext-11	7.999	0.0105	10.7	-0.45	0.393	248000	292.987	ELPT
12	Plaintext-12	7.9989	0.01055	10.695	-0.445	0.3931	248100	292.310	ELPT
13	Plaintext-13	7.9988	0.0106	10.69	-0.44	0.3932	248200	292.112	ELPT
14	Plaintext-14	7.9987	0.01065	10.685	-0.435	0.3933	248300	292.874	ELPT
15	Plaintext-15	7.9986	0.0107	10.68	-0.43	0.3934	248400	292.311	ELPT
16	Plaintext-16	7.9985	0.01075	10.675	-0.425	0.3935	248500	292.336	ELPT
17	Plaintext-17	7.9984	0.0108	10.67	-0.42	0.3936	248600	292.156	ELPT
18	Plaintext-18	7.9983	0.01085	10.665	-0.415	0.3937	248700	292.667	ELPT
19	Plaintext-19	7.9982	0.0109	10.66	-0.41	0.3938	248800	292.122	ELPT
20	Plaintext-20	7.9981	0.01095	10.655	-0.405	0.3939	248800	292.966	ELPT
21	Plaintext-21	7.293	0.01505	10.245	0.0001	0.4021	248900	294.334	EMPT
22	Plaintext-22	7.292	0.0151	10.24	0.00011	0.4022	249000	294.669	EMPT
23	Plaintext-23	7.291	0.01515	10.235	0.00012	0.4023	249100	294.110	EMPT
24	Plaintext-24	7.290	0.0152	10.23	0.00013	0.4024	249200	294.987	EMPT
25	Plaintext-25	7.289	0.01525	10.225	0.00014	0.4025	249300	294.001	EMPT
26	Plaintext-26	7.288	0.0153	10.22	0.00015	0.4026	249400	294.312	EMPT
27	Plaintext-27	7.287	0.01535	10.215	0.00016	0.4027	249500	294.900	EMPT
28	Plaintext-28	7.286	0.0154	10.21	0.00017	0.4028	249600	294.001	EMPT
29	Plaintext-28	7.285	0.01545	10.205	0.00018	0.4029	249700	294.361	EMPT
30	Plaintext-29	7.284	0.0155	10.2	0.00019	0.403	249800	294.936	EMPT
31	Plaintext-30	7.283	0.01555	10.195	0.0002	0.4031	249900	294.887	EMPT
32	Plaintext-31	7.282	0.0156	10.19	0.00021	0.4032	250000	294.474	EMPT
33	Plaintext-32	7.281	0.01565	10.185	0.00022	0.4033	250100	294.101	EMPT
34	Plaintext-33	7.280	0.0157	10.18	0.00023	0.4034	250200	294.031	EMPT
35	Plaintext-34	7.279	0.01575	10.175	0.00024	0.4035	250300	294.351	EMPT
36	Plaintext-35	7.278	0.0158	10.17	0.00025	0.4036	250400	294.333	EMPT
37	Plaintext-36	7.277	0.01585	10.165	0.00026	0.4037	250500	294.110	EMPT
38	Plaintext-37	7.276	0.0159	10.16	0.00027	0.4038	250600	294.669	EMPT
39	Plaintext-38	7.275	0.01595	10.155	0.00028	0.4039	250600	294.110	EMPT
40	Plaintext-40	7.274	0.016	10.15	0.00029	0.404	250700	294.311	EMPT
41	Plaintext-31	6.389	0.0201	9.74	0.0012	0.4122	250800	296.003	EHPT
42	Plaintext-42	6.388	0.02015	9.735	0.0013	0.4123	250900	297.963	EHPT
43	Plaintext-43	6.387	0.0202	9.73	0.0014	0.4124	251000	295.221	EHPT
44	Plaintext-44	6.386	0.02025	9.725	0.0015	0.4125	251100	298.733	EHPT
45	Plaintext-45	6.385	0.0203	9.72	0.0016	0.4126	251200	296.331	EHPT
46	Plaintext-46	6.384	0.02035	9.715	0.0017	0.4127	251200	297.301	EHPT
47	Plaintext-47	6.383	0.0204	9.71	0.0018	0.4128	251300	297.332	EHPT
48	Plaintext-48	6.382	0.02045	9.705	0.0019	0.4129	251400	297.301	EHPT

Table 10: Continued.

F.V no.	Images	Entropy	Energy	Contrast	Correlation	Homogeneity	I_D	Hist^2	EA
49	Plaintext-49	6.381	0.0205	9.7	0.002	0.413	251500	296.36	EHPT
50	Plaintext-50	6.380	0.02055	9.695	0.0021	0.4131	251600	298.36	EHPT
51	Plaintext-51	6.379	0.0206	9.69	0.0022	0.4132	251700	297.651	EHPT
52	Plaintext-52	6.378	0.02065	9.685	0.0023	0.4133	251800	297.660	EHPT
53	Plaintext-53	6.377	0.0207	9.68	0.0024	0.4134	251900	297.633	EHPT
54	Plaintext-54	6.376	0.02075	9.675	0.0025	0.4135	252000	297.336	EHPT
55	Plaintext-55	6.375	0.0208	9.67	0.0026	0.4136	252100	297.631	EHPT
56	Plaintext-56	6.374	0.02085	9.665	0.0027	0.4137	252200	297.310	EHPT
57	Plaintext-57	6.373	0.0209	9.66	0.0028	0.4138	252300	296.120	EHPT
58	Plaintext-58	6.372	0.02095	9.655	0.0029	0.4139	252400	296.999	EHPT
59	Plaintext-59	6.371	0.021	9.65	0.003	0.414	252500	297.613	EHPT
60	Plaintext-60	6.370	0.02105	9.645	0.0031	0.4141	252600	297.643	EHPT

Table 11: EA classification based on the information present in the plaintext images.

Plain images	Contrast	Entropy	Energy	Correlation	Homogeneity	I_D	$(\text{Hist})^2$	EA
Plain image$_1$	9.9971	7.97608	0.0183	0.00059	0.4092	24763	294.664	EMPT
Plain image$_2$	8.9651	7.9283	0.02334	0.0061	0.4192	24770	294.210	EMPT
Plain image$_3$	8.4131	7.8633	0.02452	0.0066	0.4027	248706	296.331	ELPT
Plain image$_4$	10.3574	7.9937	0.0159	-0.1351	0.3932	24993	292.665	EHPT
Plain image$_5$	11.3585	7.9982	0.0151	-0.0951	0.3984	247830	291.336	EHPT
Plain image$_6$	10.9875	7.99313	0.1682	-0.0651	0.3994	246378	292.346	EHPT
Plain image$_7$	9.6381	7.9832	0.0175	0.00063	0.4071	249763	291.032	EHPT
Plain image$_8$	10.8934	6 7.9931	0.0145	-0.044	0.3931	248610	291.336	EHPT

$$\text{Cov}(q,p) = \frac{1}{M}\sum_{r=1}^{M}(q_r - G(q))(p_r - G(p)), \tag{13}$$

$$T(q) = \frac{1}{M}\sum_{r=1}^{M}(q_r - G(q))^2, \tag{14}$$

$$T(p) = \frac{1}{M}\sum_{r=1}^{M}(p_r - G(p))^2, \tag{15}$$

$$G(q) = \frac{1}{M}\sum_{r=1}^{M} q_r, \tag{16}$$

$$G(p) = \frac{1}{M}\sum_{r=1}^{M} p_r, \tag{17}$$

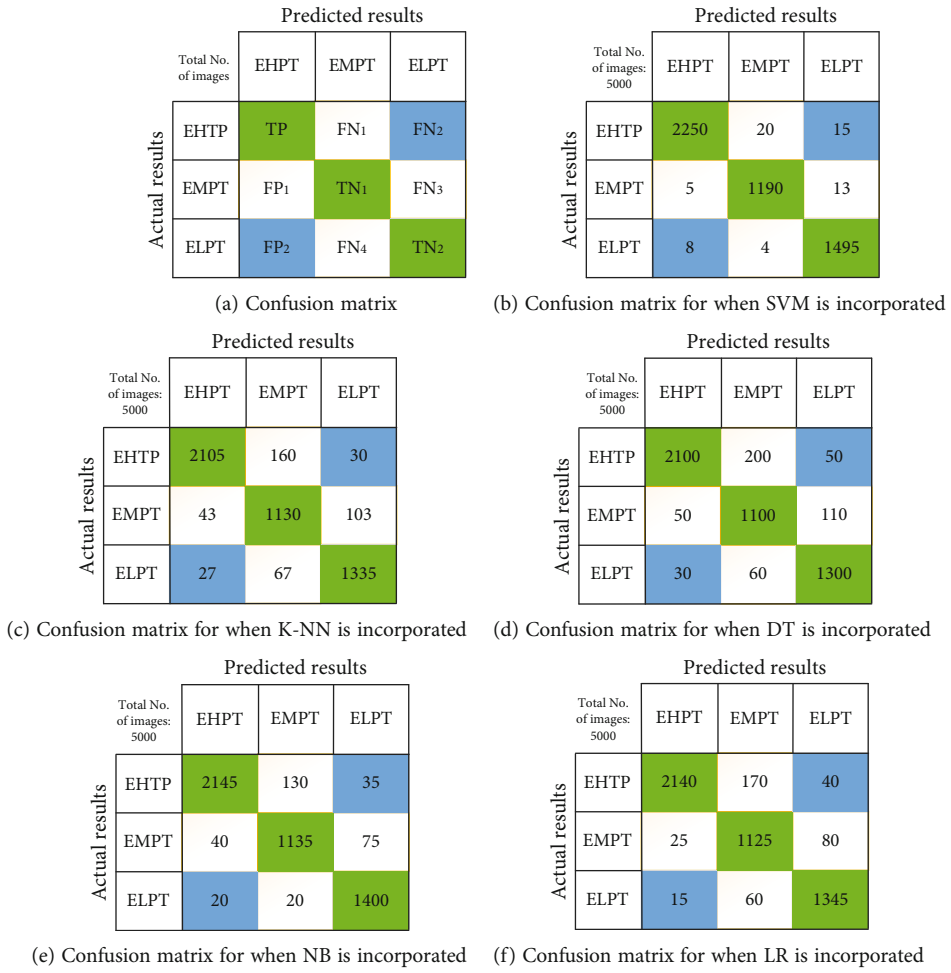
where q and p denote neighbouring pixel values, respectively, and Corr_{qp} denotes pixel correlation. Correlation coefficients are in the range of $[-1\ 1]$. $\text{Corr}_{qp} \longrightarrow -1$ and $\text{Corr}_{qp} \longrightarrow +1$ denoted the correlation between neighbouring pixels' lowest and maximum values, respectively. The 2500 pixel pairs are taken from the plaintext image in three distinct directions: horizontal, vertical, and diagonal. Figures 5(b)–5(d) and 5(f)–5(h) illustrate the horizontal, vertical, and diagonal correlations of image pixels, respectively. As can be observed, the pixels are closer together, indicating a significant correlation. In comparison, the distribution of pixels in Figures 5(j)–5(l) and 5(n)–5(p) is relatively random, indicating a weaker correlation. Thus, images with a low correlation may be easily secured using a simple, mathematically structured encryption approach. Digital image encryption is classified according to the intervals specified in Table 5.

4.1.5. Homogeneity. The Grey-level Co-occurrence Matrix (GLCM) illustrates the brightness of pixels. Those images that contain high information have higher homogeneity values. This means that encrypting images with high homogeneity values is difficult and requires a strong encryption scheme. Homogeneity can be calculated as

$$\sum_x \sum_y \frac{I(x,y)}{1+|x+y|}, \tag{18}$$

where $I(x,y)$ is plaintext image and x,y shows the pixel position. Table 6 contains the intervals used to classify encryption schemes. If the plaintext image's homogeneity values fall within the range $[0.4122\ 0.4418]$, it may be encrypted using a strategy that requires less mathematical operations and requires less processing time.

4.1.6. Histogram Analysis. Histogram analysis is often used in image encryption to determine the security of ciphertext



(a) Confusion matrix

(b) Confusion matrix for when SVM is incorporated

(c) Confusion matrix for when K-NN is incorporated

(d) Confusion matrix for when DT is incorporated

(e) Confusion matrix for when NB is incorporated

(f) Confusion matrix for when LR is incorporated

Figure 7: Confusion matrices for CNN, transfer learning, and fine tuning based on the proposed model.

Table 12: Performance measuring parameters and their statistical values.

Parameters	Mathematical equations
Accuracy (Acc_y)	$\frac{\Gamma P + \Gamma N_1 + \Gamma N_2}{\Gamma P + \Gamma N_1 + \Gamma N_2 + \sqsubseteq N_1 + \sqsubseteq N_2 + \sqsubseteq P_1 + \sqsubseteq N_3 + + \sqsubseteq P_2 + \sqsubseteq N_4} \times 100 = 98.7\%$ $\frac{2250 + 1190 + 1495}{2250 + 20 + 15 + 5 + 1190 + 13 + 8 + 4 + 1495} \times 100 = 98.7\%$
Specificity (Spec_y)/precision (Prec_y)	$\frac{\Gamma P}{\Gamma P + \sqsubseteq N_1 + \sqsubseteq N_2 + \sqsubseteq N_3 + \sqsubseteq N_4}$ $\frac{2250}{2250 + 20 + 15 + 13 + 4} = 0.97$
Sensitivity (Sen_y)/recall	$\frac{\Gamma N_1 + \Gamma N_2}{\Gamma N_1 + \Gamma N_2 + \sqsubseteq P_1 + \sqsubseteq P_2}$ $\frac{1190 + 1495}{1190 + 1495 + 5 + 8} = 0.99$
F1-score	$2 \times \left[\frac{\text{Sen}_y \times \text{Spec}_y}{\text{Sen}_y + \text{Spec}_y}\right] = 0.97$

images. To offer effective encryption, the encrypting images' pixel distribution must be constant, which means that the histogram must be flat, which corresponds to the image pixels being properly concealed. Plaintext images contain more information than encrypted images, indicating a less uniform pixel distribution. The histograms of multiple plaintext images are provided in Figure 6, along with the pixel distribution.

The relationship between the information present in the plaintext image and uniformity of the histogram is given as

$$\text{Plaintext information} \propto \frac{1}{\text{Histogram uniformity}}. \quad (19)$$

According to Equation (19), less uniformity in the histogram indicates that the corresponding image has a greater

quantity of information. This implies that images with flat histograms are simple to encrypt and can be made secure by using an encryption strategy with less mathematical operations and processing time. Equation (20) may be used to compute the statistical value of the histogram analysis:

$$(\text{Hist})^2 = \sum_{k=0}^{255} \frac{g_i - t}{t}, \tag{20}$$

where g_i represents the number of gray levels and $t = M \times N/256$. According to the existing work [60], $(\text{Hist})^2$ must be less than 293.24783 to achieve the uniformity in the histogram. $\text{Hist}^2 > 293.24783$ represents the variation in the peaks of the pixels. Based on the Hist^2 values, plaintext images are categorized into three intervals as shown in Table 7 for encryption purposes.

4.1.7. Irregular Deviation. The uniformity of the histogram also relates to the irregular deviation (I_D) in the image pixels. I_D may be used to determine image quality. The more information is present in the plaintext images, the higher the I_D value. It may be defined as the degree to which the histogram deviation distribution and the uniform distribution are similar. I_D can be calculated as

$$I_D = \sum_{j=0}^{255} |X_i - X_h|, \tag{21}$$

where X_i and X_h are the histogram deviations at the i^{th} and h positions, respectively, and the mean value. The less consistent the histograms, the lower the I_D value. The I_D interval is specified in Table 8 to classify encryption techniques for plaintext images. The summary of the features used in the proposed work is given in Table 9.

(i) A dataset is created using the security parameters as a feature and the intervals defined in Section 4.1. The collection is vast and includes the bulk of textual image categories that we see in everyday life, such as medical images and war images. As a consequence, this dataset is often referred to as the source domain for the proposed model training, validation, and construction. Table 10 includes a subset of the detailed data. The dataset is split into the training and test sets at a ratio of 0.8 : 0.2, as specified in

$$\begin{cases} \text{if} & \\ \text{Test dataset} & \text{Test} = N - \text{samples} \\ \text{Training dataset} & (\text{Total no.of samples}) - (N - \text{samples}) \end{cases} \tag{22}$$

(ii) After extracting statistical features from plaintext images, save feature values in an array to create unique vector streams (V.S), also referred to as feature vectors. Vector streams may be expressed as follows in terms of their features as given:

$$\text{Dataset} = \begin{pmatrix} \text{V.S}_1 = f.v_1, f.v_2, f.v_1, \cdots, f_7 \\ \text{V.S}_2 = f.v_1, f.v_2, f.v_1, \cdots, f_7 \\ \text{V.S}_3 = f.v_1, f.v_2, f.v_1, \cdots, f_7 \\ \text{V.S}_4 = f.v_1, f.v_2, f.v_1, \cdots, f_7 \\ \vdots \\ \text{V.S}_n = f.v_1, f.v_2, f.v_1, \cdots, f_7 \end{pmatrix}. \tag{23}$$

The feature values for each feature are $f.v_1, f.v_2, f.v_3, \cdots, f.v_7$. The provided dataset (22) is separated into two sections for the purpose of training the proposed model (training and testing). Each part is further separated into categories, such as X-train and Y-train for training purposes and X-test and Y-test for testing purposes. Train various machine learning algorithms on the training dataset to identify plaintext images based on the information contained in them. The purpose of comparing various machine learning algorithms is to determine which method outperforms the others

Table 13: K-fold analysis for accuracy.

Classifiers	SVM	NB	LR	K-NN	DT
$K = 5(M_1)$	98.5	91.6	93.9	93.8	93.8
$K = 10(M_2)$	98.6	90.5	92.2	94.2	92.3
$K = 20(M_3)$	98.8	92.3	92.7	93.9	92.9
$K = 25(M_4)$	98.7	91.6	93.3	93.4	93.8
$K = 50(M_5)$	98.4	92.8	93.1	94.7	93.6

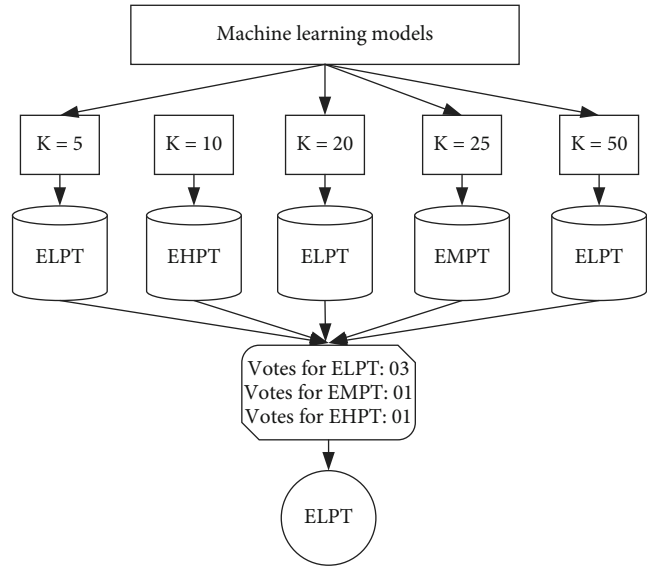


Figure 8: Hard voting-based classification

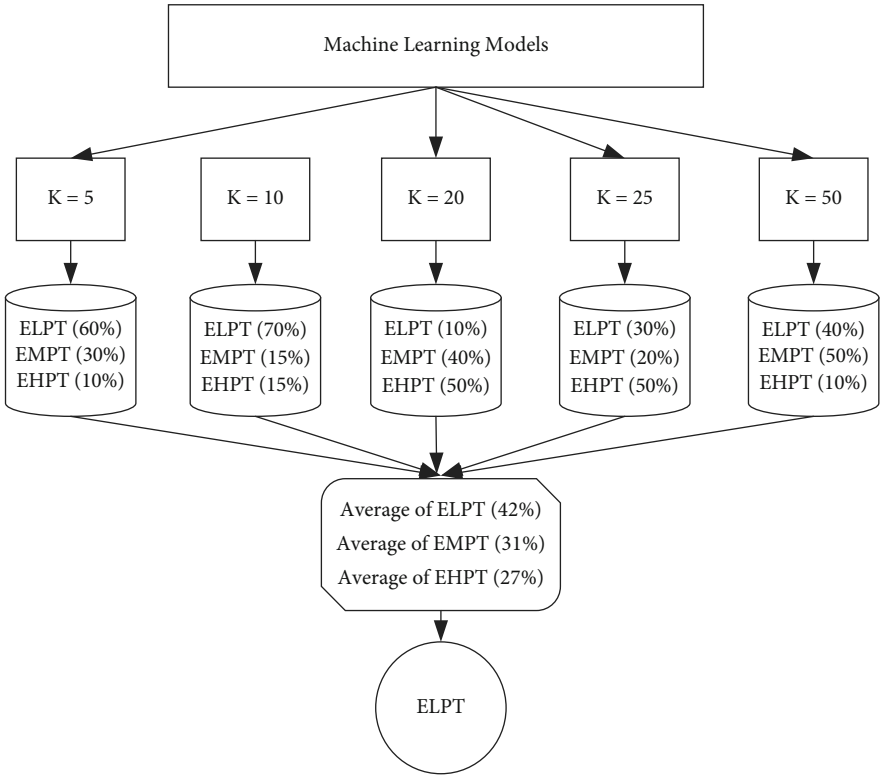


Figure 9: Hard voting-based classification

on the provided dataset. A few instances of categorization for numerous plaintext images are shown in Table 11.

5. Results and Discussion

Two distinct tools such as MATLAB 2014a and a Jupyter notebook (for Python, version 3.7) are used to construct the proposed model. Several characteristics including accuracy, precision, recall, and F-score are examined while evaluating the proposed model, and their values may be simply computed using the confusion matrix. This is a two-dimensional array that contains True Positive (TP), True Negative (TN), False Positive (FP), and False Negatives (FN). Figure 7 shows the generalised confusion matrix and the confusion matrices for the proposed work when DT, K-NN, RF, NB, and SVM are used.

The terms TP, TN, FP, and FN are defined below according to the proposed model.

(i) True positives (TP)

The proposed technique predicts that a strong EA (EHPT) is required to encrypt such a plaintext image that contains a bulk of information.

(ii) True negatives (TN)

The proposed technique predicts that such an EA is required that offers moderate security (EMPT) to encrypt a plaintext image that contains moderate amount of information, or the proposed technique predicts that such an EA is required that offers weak security (ELPT) to encrypt a plaintext image which contains less amount of information.

(iii) False positives (FP)

The proposed technique predicts that a strong EA (EHPT) is required to encrypt such a plaintext image that contains moderate or less amount of information.

(iv) False negatives (FN)

The proposed technique predicts that such an EA is required that offers moderate security (EMPT) to encrypt a plaintext image that contains a bulk of information, or the proposed technique predicts that such an EA is required that offers weak security (ELPT) to encrypt a plaintext image that contains a moderate amount of information.

The mathematical equations and corresponding values calculated using the proposed mode are shown in Table 12.

To enhance the overall accuracy of the proposed model, K-fold analysis is performed in which five different values of K ($K = 5, K = 10, K = 20, K = 25$, and $K = 50$) are selected to build five models (M_1, M_2, M_3, M_4, and M_5). For instance, if $K = 20$, a total of twenty iterations will be performed and take the average accuracy for M_1. The mathematical representation for calculating the average accuracy for M_3 (Avg_{acc}) is shown in Equations (24) and (25), whereas Av

Table 14: Performance comparison with existing models.

Schemes	SVM (sigmoid kernel)	SVM (linear kernel)	SVM (rbf kernel)	SVM (polynomial kernel)	NB	LR	DT	RF	K-NN
				Accuracy (Acc_y)					
Proposed	98.7	95.4	96.3	95.8	90.2	78.3	80.6	95.2	96.9
Reference [62]	91	81	89	90	90	92	91	84	86
Reference [63]	86	93	92	92	91	92	92	91	92
Reference [61]	95	75	77	79	73	74	82	84	86
Reference [64]	85	83	82	89	92	93	91	92	97
Reference [65]	92	86	82	92	92	94	91	92	93
				Precision ($Prec_y$)					
Proposed	0.97	0.98	0.98	0.89	0.99	0.32	0.35	0.99	0.97
Reference [62]	0.84	0.92	0.90	0.85	0.86	0.87	0.89	0.92	0.89
Reference [63]	0.92	0.95	0.93	0.96	0.93	0.93	0.95	0.98	0.99
Reference [61]	0.89	0.88	0.87	0.84	0.92	.97	0.98	0.97	0.98
Reference [64]	0.97	0.95	0.96	0.98	0.96	099	0.98	0.99	0.98
Reference [65]	0.89	0.88	0.87	0.84	0.92	.97	0.98	0.97	0.98
				Sensitivity (Sen_y)					
Proposed	0.97	0.98	0.99	0.96	0.80	0.15	0.87	0.92	0.85
Reference [62]	0.89	0.92	0.93	0.95	0.91	0.94	0.95	0.94	0.92
Reference [63]	0.92	0.94	0.91	0.90	0.98	0.94	0.95	0.92	0.91
Reference [61]	0.97	0.91	0.92	0.91	0.92	0.96	0.95	0.92	0.96
Reference [64]	0.91	0.92	0.90	0.89	0.96	0.92	0.93	0.91	0.92
Reference [65]	0.91	0.92	0.94	0.96	0.96	0.92	0.92	0.91	0.91
				F1-score					
Proposed	0.98	0.99	0.98	0.96	0.89	0.22	0.45	0.94	91
Reference [62]	0.86	0.92	0.81	0.88	0.85	0.97	0.93	0.94	0.92
Reference [63]	0.92	0.92	0.83	0.92	0.93	0.91	0.98	0.96	0.94
Reference [61]	0.91	0.90	0.92	0.93	0.92	0.91	0.95	0.96	0.99
Reference [64]	0.96	0.97	0.92	0.91	0.91	0.96	0.95	0.92	0.91
Reference [65]	0.91	0.90	0.92	0.93	0.92	0.91	0.95	0.96	0.99

g_{acc} for other classifiers at different values of K are displayed in Table 13:

$$\text{Avg}_{\text{acc}}(M_3) = \frac{\text{Acc}_{(K_1)} + \text{Acc}_{(K_2)} + \text{Acc}_{(K_3)} + \text{Acc}_{(K_4)} + \text{Acc}_{(K_5)}}{5} \times 100, \tag{24}$$

$$\text{Accuracy}(M_1) = \frac{98.8 + 98.7 + 98.9 + 98.9 + 98.8}{5} = 98.8\%. \tag{25}$$

Finally, voting techniques such as soft and hard voting are applied on the proposed M-models to classify the labels in a more sophisticated way.

5.1. Hard Voting. This technique works on the majority of votes. For instance, there are five models for the proposed work $(M_1, M-2, \cdots, M_5)$. Three of them classify the upcoming event as ELPT, one each is for classes EMPT and EHPT. Therefore, according to the hard voting technique, the new event will belong to class ELPT as shown in Figure 8.

5.2. Soft Voting. The probability-based classification can be performed using soft voting. In this technique, the probability of each class occurring is calculated separately, and then, the decision will be in favour of the class which has the highest probability value, as shown in Figure 9.

The probability of occurring in each class (ELPT, EMPT, and EHPT) using the generated M-models is calculated individually according to

$$\text{For class ELPT} = \frac{Po(\text{ELPT})_1 + Po(\text{ELPT})_2 + Po(\text{ELPT})_3 + \cdots + Po(\text{ELPT})_N}{N}, \tag{26}$$

$$\text{For class EMPT} = \frac{Po(\text{EMPT})_1 + Po(\text{EMPT})_2 + Po(\text{EMPT})_3 + \cdots + Po(\text{EMPT})_N}{N}, \tag{27}$$

$$\text{For class EHPT} = \frac{Po(\text{EHPT})_1 + Po(\text{EHPT})_2 + Po(\text{EHPT})_3 + \cdots + Po(\text{EHPT})_N}{N}, \tag{28}$$

where $Po(\text{ELPT})$, $Po(\text{EMPT})$, and $Po(\text{EHPT})$ is the probability of occurring in the events ELPT, EMPT, and EHPT, respectively. According to the calculated probabilities, Equations (29), (30), and (31) become

$$\text{For class ELPT} = \frac{60 + 70 + 10 + 30 + 40}{5} \times 100 = 42\%, \tag{29}$$

$$\text{For class EMPT} = \frac{30 + 15 + 40 + 20 + 50}{5} \times 100 = 31\%, \tag{30}$$

$$\text{For class EHPT} = \frac{10 + 15 + 50 + 50 + 10}{5} \times 100 = 27\%. \tag{31}$$

According to Equations (29), (30), and (31), the upcoming event will belong to class ELPT.

The statistical values of the performance metrics for the proposed and existing work are displayed in Table 14. Several machine learning algorithms, including SVM, NB, LR, DT, RF, and K-NN, are evaluated when comparing the proposed work to current models. Based on the comparative study, it is evident that, among the machine learning algorithms used in the proposed work, SVM offers the highest accuracy. Moreover, comparable schemes are significantly less accurate than the proposed approach. However, the technique suggested in [61] has a 95% accuracy rate, which is comparable to the accuracy offered by the proposed work.

6. Conclusions and Future Research Directions

The proposed research presents a pattern recognition-based machine learning technique for selecting the most appropriate encryption technique for a specific kind of data contained in digital images. Digital images are classified into three categories based on the amount of data present in them. Images containing highly correlated data which are transferred between the IoT devices should be encrypted through EHPT, while images containing textures should be encrypted through ELPT. Several machine learning algorithms are evaluated in the proposed study in order to determine the optimal ML algorithm to achieve the desired task. SVM outperforms all other machine learning methods in terms of accuracy, and it classifies the images with an accuracy of 98.7%. As a result, it is selected for the proposed technique. Moreover, a detailed comparison reveals that the proposed technique performs better than the existing ones.

In the future, we may use the proposed technique to secure digital images. Moreover, the dataset utilised in this research may be improved by incorporating more number of features.

Data Availability

The dataset generated and analyzed during this research study are available from the corresponding author on reasonable request.

Conflicts of Interest

The authors declare no conflict of interest.

References

[1] M. Condoluci, G. Araniti, T. Mahmoodi, and M. Dohler, "Enabling the iot machine age with 5g: machine-type multicast services for innovative real-time applications," *IEEE Access*, vol. 4, pp. 5555–5569, 2016.

[2] F. Ariani, R. Y. Endra, E. Erlangga, Y. Aprilinda, and A. R. Bahan, "Sistem monitoring suhu dan pencahayaan berbasis internet of thing (iot) untuk penetasan telur ayam," *EXPERT: Jurnal Manajemen Sistem Informasi dan Teknologi*, vol. 10, no. 2, pp. 36–41, 2020.

[3] Y. Harbi, Z. Aliouat, S. Harous, A. Bentaleb, and A. Refou, "A review of security in internet of things," *Wireless Personal Communications*, vol. 108, no. 1, pp. 325–344, 2019.

[4] A. Rashid, A. Masood, and A. R. Khan, "Zone of trust: blockchain assisted iot authentication to support cross-communication between bubbles of trusted IoTs," *Cluster Computing*, pp. 1–18, 2022.

[5] M. U. Rehman, A. Shafique, K. H. Khan et al., "Novel privacy preserving non-invasive sensing-based diagnoses of pneumonia disease leveraging deep network model," *Sensors*, vol. 22, no. 2, p. 461, 2022.

[6] S. Abbas, Q. Nasir, D. Nouichi et al., "Improving security of the internet of things via rf fingerprinting based device identification system," *Neural Computing and Applications*, vol. 33, no. 21, pp. 14753–14769, 2021.

[7] I. Hussain, F. Ahmed, U. M. Khokhar, and A. Anees, "Applied cryptography and noise resistant data security," *Security and Communication Networks*, vol. 2018, 2 pages, 2018.

[8] A. Shafique, A. Mehmood, and M. Elhadef, "Survey of security protocols and vulnerabilities in unmanned aerial vehicles," *IEEE Access*, vol. 9, pp. 46927–46948, 2021.

[9] A. M. Sagheer, S. S. Al-Rawi, and O. A. Dawood, "Proposing of developed advance encryption standard," in *2011 Developments in E-systems Engineering*, p. 197202, Dubai, United Arab Emirates, December 2011.

[10] D. Coppersmith, "The data encryption standard (des) and its strength against attacks," *IBM Journal of Research and Development*, vol. 38, no. 3, pp. 243–250, 1994.

[11] I. Hussain, A. Anees, T. A. Al-Maadeed, and M. Mustafa, "A novel encryption algorithm using multiple semield s-boxes based on permutation of symmetric group," 2020, http://arxiv.org/abs/2004.12264.

[12] A. Shafique, J. Ahmed, W. Boulila, H. Ghandorh, J. Ahmad, and M. U. Rehman, "Detecting the security level of various cryptosystems using machine learning models," *IEEE Access*, vol. 9, pp. 9383–9393, 2020.

[13] I. Hussain, A. Anees, M. Aslam, R. Ahmed, and N. Siddiqui, "A noise resistant symmetric key cryptosystem based on S8 S-boxes and chaotic maps," *The European Physical Journal Plus*, vol. 133, no. 4, pp. 1–23, 2018.

[14] T. S. Ali and R. Ali, "A new chaos based color image encryption algorithm using permutation substitution and Boolean operation," *Multimedia Tools and Applications*, vol. 79, no. 27, pp. 19853–19873, 2020.

[15] A. Shafique and F. Ahmed, "Image encryption using dynamic s-box substitution in the wavelet domain," *Wireless Personal Communications*, vol. 115, no. 3, pp. 2243–2268, 2020.

[16] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[17] S. S. Jamal, A. Anees, M. Ahmad, M. F. Khan, and I. Hussain, "Construction of cryptographic s-boxes based on mobius transformation and chaotic tent-sine system," *IEEE Access*, vol. 7, pp. 173273–173285, 2019.

[18] A. Shafique, J. Ahmed, M. U. Rehman, and M. M. Hazzazi, "Noise-resistant image encryption scheme for medical images in the chaos and wavelet domain," *IEEE Access*, vol. 9, pp. 59108–59130, 2021.

[19] A. Anees and Y.-P. P. Chen, "Discriminative binary feature learning and quantization in biometric key generation," *Pattern Recognition*, vol. 77, pp. 289–305, 2018.

[20] E. Salah, K. Amine, K. Redouane, and K. Fares, "A Fourier transform based audio watermarking algorithm," *Applied Acoustics*, vol. 172, p. 107652, 2021.

[21] A. Anees, A. M. Siddiqui, and F. Ahmed, "Chaotic substitution for highly autocorrelated data in encryption algorithm," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 9, pp. 3106–3118, 2014.

[22] A. Shafique, A. Mehmood, and M. Elhadef, "Detecting signal spoofing attack in uavs using machine learning models," *IEEE Access*, vol. 9, pp. 93803–93815, 2021.

[23] I. Hussain, A. Anees, A. H. AlKhaldi, A. Algarni, and M. Aslam, "Construction of chaotic quantum magnets and matrix Lorenz systems S-boxes and their applications," *Chinese Journal of Physics*, vol. 56, no. 4, pp. 1609–1621, 2018.

[24] A. Anees and I. Hussain, "A novel method to identify initial values of chaotic maps in cybersecurity," *Symmetry*, vol. 11, no. 2, p. 140, 2019.

[25] J. Ahmad and F. Ahmed, "Efficiency analysis and security evaluation of image encryption schemes," *Computing*, vol. 23, p. 25, 2010.

[26] Q. Lu, C. Zhu, and X. Deng, "An efficient image encryption scheme based on the lss chaotic map and single s-box," *IEEE Access*, vol. 8, pp. 25664–25678, 2020.

[27] K. A. K. Patro, A. Soni, P. K. Netam, and B. Acharya, "Multiple grayscale image encryption using cross-coupled chaotic maps," *Journal of Information Security and Applications*, vol. 52, p. 102470, 2020.

[28] I. Hussain, A. Anees, A. H. Alkhaldi, M. Aslam, N. Siddiqui, and R. Ahmed, "Image encryption based on chebyshev chaotic map and s8 s-boxes," *Optica Applicata*, vol. 49, no. 2, 2019.

[29] A. Belazi, A. A. Abd El-Latif, R. Rhouma, and S. Belghith, "Selective image encryption scheme based on dwt, aes s-box and chaotic permutation," in *2015 International wireless communications and mobile computing conference (IWCMC)*, pp. 606–610, Dubrovnik, Croatia, August 2015.

[30] F. Masood, J. Ahmad, S. A. Shah, S. S. Jamal, and I. Hussain, "A novel hybrid secure image encryption based on julia set of fractals and 3d lorenz chaotic map," *Entropy*, vol. 22, no. 3, p. 274, 2020.

[31] M. Khan, A. S. Alanazi, L. S. Khan, and I. Hussain, "An efficient image encryption scheme based on fractal Tromino and Chebyshev polynomial," *Complex & Intelligent Systems*, vol. 7, no. 5, pp. 2751–2764, 2021.

[32] H. R. Alsanad, O. N. Ucan, M. Ilyas, A. U. R. Khan, and O. Bayat, "Real-time fuel truck detection algorithm based on deep convolutional neural network," *IEEE Access*, vol. 8, pp. 118808–118817, 2020.

[33] J. Ahmad and S. O. Hwang, "Chaos-based diffusion for highly autocorrelated data in encryption algorithms," *Nonlinear Dynamics*, vol. 82, no. 4, pp. 1839–1850, 2015.

[34] A. Shafique, "A new algorithm for the construction of substitution box by using chaotic map," *The European Physical Journal Plus*, vol. 135, no. 2, pp. 1–13, 2020.

[35] M. Khan and Z. Asghar, "A novel construction of substitution box for image encryption applications with gingerbreadman chaotic map and S8 permutation," *Neural Computing and Applications*, vol. 29, no. 4, pp. 993–999, 2018.

[36] A. Razaq, A. Yousaf, U. Shuaib, N. Siddiqui, A. Ullah, and A. Waheed, "A novel construction of substitution box involving coset diagram and a bijective map," *Security and Communication Networks, vol.*, vol. 2017, pp. 1–16, 2017.

[37] C. Li and X. Yang, "An image encryption algorithm based on discrete fractional wavelet transform and quantum chaos," *Optik*, vol. 260, p. 169042, 2022.

[38] C.-M. Lin, D.-H. Pham, and T.-T. Huynh, "Encryption and decryption of audio signal and image secure communications using chaotic system synchronization control by tsk fuzzy brain emotional learning controllers," *IEEE Transactions on Cybernetics*, pp. 1–15, 2021.

[39] J. Liu, Y. Wang, Q. Han, and J. Gao, "A sensitive image encryption algorithm based on a higher-dimensional chaotic map and steganography," *International Journal of Bifurcation and Chaos*, vol. 32, no. 1, p. 2250004, 2022.

[40] A. Shrivastava, J. B. Sharma, and S. D. Purohit, "Image encryption based on fractional wavelet transform, arnold transform with double random phases in the hsv color domain," *Recent Advances in Computer Science and Communications (Formerly: Recent Patents on Computer Science)*, vol. 15, no. 1, pp. 5–13, 2022.

[41] L. Lidong, D. Jiang, X. Wang, L. Zhang, and X. Rong, "A dynamic triple-image encryption scheme based on chaos, S-Box and image compressing," *IEEE Access*, vol. 8, pp. 210382–210399, 2020.

[42] M. U. Rehman, A. Shafique, S. Khalid, and I. Hussain, "Dynamic substitution and confusion-diffusion-based noise-resistive image encryption using multiple chaotic maps," *IEEE Access*, vol. 9, pp. 52277–52291, 2021.

[43] H. R. Shakir, "An image encryption method based on selective aes coding of wavelet transform and chaotic pixel shuffling," *Multimedia Tools and Applications*, vol. 78, no. 18, pp. 26073–26087, 2019.

[44] A. Shafique and J. Shahid, "Novel image encryption cryptosystem based on binary bit planes extraction and multiple chaotic maps," *The European Physical Journal Plus*, vol. 133, no. 8, pp. 1–16, 2018.

[45] A. Shafique and J. Ahmed, "Dynamic substitution based encryption algorithm for highly correlated data," *Multidimensional Systems and Signal Processing*, vol. 32, no. 1, pp. 91–114, 2021.

[46] A. Anees, I. Hussain, A. Algarni, and M. Aslam, "A robust watermarking scheme for online multimedia copyright protection using new chaotic map," *Security and Communication Networks, vol.*, vol. 2018, article 1840207, pp. 1–20, 2018.

[47] A. Shafique, M. M. Hazzazi, A. R. Alharbi, and I. Hussain, "Integration of spatial and frequency domain encryption for digital images," *IEEE Access*, vol. 9, pp. 149943–149954, 2021.

[48] S. K. Mishra and V. H. Deepthi, "Retracted article: brain image classification by the combination of different wavelet transforms and support vector machine classification," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 6, pp. 6741–6749, 2021.

[49] J. Cervantes, F. Garcia-Lamont, L. Rodrguez-Mazahua, and A. Lopez, "A comprehensive survey on support vector machine classification: applications, challenges and trends," *Neurocomputing*, vol. 408, pp. 189–215, 2020.

[50] T. Brázdil, K. Chatterjee, J. Křetínský, and V. Toman, "Strategy representation by decision trees in reactive synthesis," in *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*, Lecture Notes in Computer Science, pp. 385–407, Springer, 2018.

[51] F. Avellaneda, "Efficient inference of optimal decision trees," *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 34, no. 4, pp. 3195–3202, 2020.

[52] M. U. Rehman, A. Shafique, S. Khalid, M. Driss, and S. Rubaiee, "Future forecasting of covid-19: a supervised learning approach," *Sensors*, vol. 21, no. 10, p. 3322, 2021.

[53] A. Anees and Y.-P. P. Chen, "Designing secure substitution boxes based on permutation of symmetric group," *Neural Computing and Applications*, vol. 32, no. 11, pp. 7045–7056, 2020.

[54] A. Khurshid, A. N. Khan, F. G. Khan, M. Ali, J. Shuja, and A. U. R. Khan, "Secure-CamFlow: a device-oriented security model to assist information flow control systems in cloud environments for IoTs," *Concurrency and Computation: Practice and Experience*, vol. 31, no. 8, p. e4729, 2019.

[55] F. Ahmed and A. Anees, "Hash-based authentication of digital images in noisy channels," in *Robust Image Authentication in the Presence of Noise*, pp. 1–42, Springer, Cham, 2015.

[56] M. F. Aziz, A. N. Khan, J. Shuja, I. A. Khan, F. G. Khan, and A. U. R. Khan, "A lightweight and compromise-resilient authentication scheme for IoTs," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 3, p. e3813, 2022.

[57] I. Hussain, A. Anees, and A. Algarni, "A novel algorithm for thermal image encryption," *Journal of Integrative Neuroscience*, vol. 17, no. 3-4, pp. 447–461, 2018.

[58] A. Anees, W. A. Khan, M. A. Gondal, and I. Hussain, "Application of mean of absolute deviation method for the selection of best nonlinear component based on video encryption," *Zeitschrift für Naturforschung A*, vol. 68, no. 6-7, pp. 479–482, 2013.

[59] Y. Sang, J. Sang, and M. S. Alam, "Image encryption based on logistic chaotic systems and deep autoencoder," *Pattern Recognition Letters*, vol. 153, pp. 59–66, 2022.

[60] M. Guan, X. Yang, and W. Hu, "Chaotic image encryption algorithm using frequency-domain DNA encoding," *IET Image Processing*, vol. 13, no. 9, pp. 1535–1539, 2019.

[61] S. S. Vanjire and M. Lakshmi, "MDTA: a new approach of supervised machine learning for android malware detection and threat attribution using behavioral reports," in *Mobile Computing and Sustainable Informatics*, pp. 147–159, Springer, Singapore, 2022.

[62] S. Mishra and A. K. Tyagi, "The role of machine learning techniques in internet of things-based cloud applications," in *Artificial Intelligence-based Internet of Things Systems*, pp. 105–135, Springer, Cham, 2022.

[63] S. Sengan, O. I. Khalaf, D. K. Sharma, and A. A. Hamad, "Secured and privacy-based ids for healthcare systems on e-medical data using machine learning approach," *International Journal of Reliable and Quality E-Healthcare (IJRQEH)*, vol. 11, no. 3, pp. 1–11, 2022.

[64] M. U. Ilyas and S. A. Alharbi, "Machine learning approaches to network intrusion detection for contemporary internet traffic," *Computing*, vol. 104, no. 5, pp. 1061–1076, 2022.

[65] H. Li, C. Li, and Y. Liu, "Machine learning-based frequency security early warning considering uncertainty of renewable generation," *International Journal of Electrical Power & Energy Systems*, vol. 134, p. 107403, 2022.