IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 4, 2020, accepted December 18, 2020, date of publication December 22, 2020,
date of current version January 15, 2021.

Digital Object Identifier 10.1109/ACCESS.2020.3046528

Detecting the Security Level of Various Cryptosystems Using Machine Learning Models

ARSLAN SHAFIQUE[1], JAMEEL AHMED[1], (Member, IEEE), WADII BOULILA[2,3], (Senior Member, IEEE), HAMZAH GHANDORH[3], JAWAD AHMAD[4], (Senior Member, IEEE), AND MUJEEB UR REHMAN[1]

[1]Department of Electrical Engineering, Riphah International University, Islamabad 44000, Pakistan
[2]RIADI Laboratory, University of Manouba, Manouba 2010, Tunisia
[3]College of Computer Science and Engineering, Taibah University, Medina 42353, Saudi Arabia
[4]School of Computing, Edinburgh Napier University, Edinburgh EH10 5DT, U.K.

Corresponding author: Arslan Shafique (arslan.shafique@riphah.edu.pk)

ABSTRACT With recent advancements in multimedia technologies, the security of digital data has become a critical issue. To overcome the vulnerabilities of current security protocols, researchers tend to focus their efforts on modifying existing protocols. Over the last few decades, though, several proposed encryption algorithms have been proven insecure, leading to major threats against important data. Using the most appropriate encryption algorithm is a very important means of protection against such attacks, but which algorithm is most appropriate in any particular situation will also be dependent on what sort of data is being secured. However, testing potential cryptosystems one by one to find the best option can take up an important processing time. For a fast and accurate selection of appropriate encryption algorithms, we propose a security level detection approach for image encryption algorithms by incorporating a support vector machine (SVM). In this work, we also create a dataset using standard encryption security parameters, such as entropy, contrast, homogeneity, peak signal to noise ratio, mean square error, energy, and correlation. These parameters are taken as features extracted from different cipher images. Dataset labels are divided into three categories based on their security level: strong, acceptable, and weak. To evaluate the performance of our proposed model, we have performed different analyses (f1-score, recall, precision, and accuracy), and our results demonstrate the effectiveness of this SVM-supported system.

INDEX TERMS Support vector machine (SVM), security analysis, image encryption, cryptosystem.

I. INTRODUCTION

Due to the exponential increase in transmissions of multimedia data over insecure channels (mostly the Internet), security has become a much-in-demand area of research. To protect data from eavesdroppers and unauthorized users, many researchers have turned to developing new encryption algorithms [1]–[5].

When encrypting digital images, two factors are crucial: diffusion and confusion (also known as scrambling). In [6], Claud Shannon proposed a theory that cryptosystem contains confusion and diffusion mechanisms, may be considered a secure cryptosystem. With digital images, the scrambling process can be performed directly either on pixels or else on rows and columns, whereas diffusion changes the original pixel values. In other words, with the substitution process, every unique pixel value replaces with the unique value of the S-box.

However, the transmission of data in an encrypted form is not enough to ensure its privacy. For instance, if anyone encrypts an image with a single substitution box (S-box), the information in the substituted or enciphered image may still be visible. This means that the encryption with a single S-box is not enough to conceal the original image properly. Although the information which is to be transmitted is in encrypted form, it can still be visualized by unauthorized users due to the weak security of the encryption algorithm, as seen in Figure 1(b). Thus. it is also necessary to use a strong encryption algorithm to boost encryption security.

The robustness of the encrypted image is highly dependent on the security level of the encryption algorithm that has encrypted it. A highly secure encryption algorithm will

The associate editor coordinating the review of this manuscript and approving it for publication was Yan Huo.

(a) Plain Cameraman image (b) Encrypted image with single S-box

FIGURE 1. Single S-box encryption.

encrypt the plain image completely, enabling it to resist attacks against its integrity, confidentiality, and availability.

Along with security, time complexity is another important factor to count up in the selection of an appropriate encryption system. The selection of any cryptosystem depends on the nature of the application to be encrypted, as different types of data will have different security priorities. For example, the Advanced Encryption Standard (AES) [7] is currently the most secure encryption algorithm available. However, it is not suitable for applications where fast encryption is required, since AES required several rounds, which takes more time to encrypt the original information. Moreover, the time complexity is also dependent on the total number of pixels present in the original image. The greater number of pixels in the plain image, the more processing time will be required to encrypt it [8]. By contrast, if the main requirement is only to encrypt a plain image with strong security, then the processing time may not need to such a strong consideration. Although strong encryption provides better security results, it is not necessarily a feature of fast encryption, which may be preferred sometimes [9].

To evaluate the security level of an encryption algorithm, a statistical analysis such as entropy, correlation, energy, or homogeneity must be performed upon it. Such tasks can be achieved by testing each encryption algorithm and calculating the statistics of its security parameters. After performing such security analyses on different encryption algorithms one by one, we can choose the best and strongest option from those tested. However, this process often takes too much time away from achieving the actual task. Instead, we propose, this manual testing can be replaced by a machine learning model, which will be able to select the strongest encryption algorithm quickly, easily, and accurately.

We have categorized the security of encryption algorithms into three different levels (strong, moderate and weak) based on standard security parameters of the encryption algorithms. Below is the detail of how we divided the encryption algorithms into three said security levels based on the security parameters such as entropy, homogeneity, contrast, correlation, energy, PSNR and MSE.

As we are targeting those encryption algorithms, which are used to encrypt the 8–bit images. For the 8–bit images, the maximum entropy cannot be exceeded by 8. Likewise, for the binary images, the maximum entropy that can be obtained is 2. So, in the case of 8-bit images, we have divided the whole entropy interval for 8-bit images into three intervals. The range of the whole interval is 0 to 8.

The average entropy value of any plain image may vary from 7.600 to 7.700. Whereas, an enciphered image encrypted generated using a weak encryption algorithm such as a single Substitution-box (S-box) algorithm may produce the average entropy value between 7.9503 to 7.9799. While for an acceptable and strong encryption algorithm, the average entropy value may vary from 7.9800 to 7.9900 and 7.9901 to 8.000 respectively. Similarly, the values for other security parameters may vary accordingly.

To justify the above statement, we obtain the security parameter values for different enciphered images which are generated from different encryption algorithms. Weak and moderate encryption algorithms are not able to encrypt the images properly. The enciphered images encrypted with weak and moderate encryption algorithms are shown in Figure 3.

The statistical values for different images encrypted with weak, moderate and strong encryption algorithms and their corresponding average entropy values are listed in Table 1.

For the security level detection, we have considered all types of image encryption algorithms whether it is based on the frequency domain, transform-based or chaotic maps based schemes The main objective of the proposed work is to find the security level of the encryption algorithms. To generate a dataset, we considered a bunch of enciphered images and extract the feature values of those images. The size of the dataset is not restricted, it can be of any size. Feature values for strong and acceptable security level must be properly mentioned in the dataset. Take entropy values as an example; for the entropy values, we have taken the step size of 0.0001. we have divided the entropy values into three said intervals. For strong security, there are one hundred values ranges from 7.9901 to 8.000. Likewise, for the acceptable security level, there are one hundred and two values ranges from 7.9900 to 7.9800. All the other values which are below 7.9800 will be for weak security status. Similarly, we have divided the other parameter values into three intervals by selecting an appropriate step size accordingly. For the visualization of the dataset, some portion of the proposed dataset is shown in Table 2 in which the first twenty feature vectors of each category of security level are displayed.

Rules for classification: To classify the encryption algorithms into three different categories (strong, acceptable and weak), the following are the rules must follow by the proposed model.

For the classification of each category, the decision will be based on the values of the security parameter.

- We have divided the range of each of the parameters into three intervals defined for weak, acceptable and strong security. Fo the weak security level, below 50 percent feature values must lie in the acceptable interval values.
- For acceptable security, atleast 65 percent feature values must lie in the acceptable interval values.

TABLE 1. Statistical values for different enciphered images.

Encryption schemes	Lenna	Baboon	Pepper	Boat	Camera-man	House
			Entropy			
Weak encryption algorithm	7.9700	7.9615	7.9701	7.9525	7.9530	7.9740
Acceptable encryption algorithm [10]	7.9850	7.9848	7.8961	7.9900	7.9890	7.9876
Strong encryption algorithm [11]	7.9961	7.9940	7.9920	7.9933	7.9993	7.9999
			Homoge-neity			
Weak encryption algorithm	0.4235	0.4359	0.4401	0.4169	0.4139	0.4399
Acceptable encryption algorithm [10]	0.4095	0.4063	0.4115	0.4099	0.4056	0.4089
Strong encryption algorithm [11]	39.5063	39.8901	39.7320	40.1583	39.9930	39.8012
			Contrast			
Weak encryption algorithm	8.8900	9.6810	9.6834	9.641	8.9640	9.1360
Acceptable encryption algorithm [10]	9.8690	9.8701	9.9931	9.9610	10.3871	10.6980
Strong encryption algorithm [11]	10.6431	10.7410	10.4065	10.6741	10.9641	10.4680
			Energy			
Weak encryption algorithm	0.0110	0.01240	0.0143	0.0148	0.01491	0.01500
Acceptable encryption algorithm [10]	0.0164	0.0186	0.0173	0.0173	0.0200	0.0189
Strong encryption algorithm [11]	0.0249	0.0289	0.0299	0.0346	0.0349	0.0315
			Correla-tion			
Weak encryption algorithm	0.0100	0.0239	0.0290	0.0018	0.0080	0.0119
Acceptable encryption algorithm [10]	0.0005	0.0007	0.0006	0.0005	0.0011	0.0003
Strong encryption algorithm [11]	-0.4631	-0.1383	-0.2621 -	0.0367	-0.03736	7.7840
			PSNR			
Weak encryption algorithm	7.6520	7.6941	9.6781	10.000	8.6971	6.1678
Acceptable encryption algorithm [10]	12.3687	16.9871	18.3614	19.3769	14.6771	16.6630
Strong encryption algorithm [11]	25.3480	28.397	39.6480	40.3972	45.6871	50.3974
			PSNR			
Weak encryption algorithm	18.0023	45.6874	89.3571	99.6712	79.3150	88.3666
Acceptable encryption algorithm [10]	150.6782	159.6470	189.3102	197.3160	179.3671	185.0345
Strong encryption algorithm [11]	250.6713	300.1573	305.9871	369.3478	350.1579	376.6547

- For strong security, more than 80 percent features values must lie in the acceptable interval values.

A. CONTRIBUTIONS OF THIS WORK

- We have proposed a new dataset to determine the security level of different encryption algorithms. In the proposed dataset, security parameters of the evaluation for encryption algorithms are taken as features, while three different levels of security – "strong," "acceptable," and "weak" are taken as labels.
- We have developed a new model using a support vector machine (SVM) to identify the security level of various cryptosystems.
- We conduct experiments and analyses for factors such as accuracy, F1 score, precision and recall, using our findings to calculate and evaluate the effectiveness of the work we propose.

II. LITERATURE REVIEW

A number of encryption algorithms have been proposed as means of securing images before transmission. Encryption algorithms may develop based on chaos or transformation methods, such as discrete wavelet transformation, discrete cosine transformation and discrete Fourier transformation [12]–[17]. These are just some of the many image encryption schemes that have been proposed in recent years, though. Further details of each type are provided below:

In [18], a cosine transformation and chaos-based image encryption algorithm was proposed. Here, three different chaotic maps were used instead of a single chaotic system. The proposition of using more than one chaotic map was to create more complexity in the overall algorithm, thus enabling it to exhibit more complicated and dynamic behavior. To enhance the security of the encryption algorithm, Kaur et. al proposed a new optical image encryption scheme based on a chaotic in [19] which proved capable of generating the vectors of multiple orders using a piece-wise linear chaotic map (PWLCM) [20]. For a fast image encryption, Khan *et al.* proposed a chaos-based selective image encryption scheme in [21]. Although selective encryption schemes work well for real-time applications where fast encryption is required, they are not suitable for text encryption, where every individual single bit must be encrypted in order for the data to be properly concealed. These algorithms achieved efficient encryption, as demonstrated by the statistical analysis; however, these results were not enough to show the security level of the proposed work. More analysis would be needed to show a better assessment of that particular encryption algorithm. Although the chaos has an ability to generate random number, Nardo *et al.* explained the limitations of chaos-based encryption schemes in [22], claiming that these types of encryption algorithms are implemented on a finite precision computer, causing dynamic degradation that makes the chaos-based encryption insecure. To encrypt plain images, the authors used a finite precision error, which was generated by the implementation of chaos-based systems using different interval delays. Explaining few moew limitations of chaos, the authors in [23] claimed that chaos-based communication systems are not secure enough because they depend on initial values, meaning that their security can be broken by identifying those initial values. To enhanced the security of the chaos-based crptosystem, in our previous work, a bit-plane extraction method is incorporated to

TABLE 2. Some portion of the proposed dataset.

Feature vector No.	Entropy	Energy	Contrast	Correlation	Homogeneity	MSE	PSNR in dB	Security-Level
cipher image-1	8	0.01	10.75	-0.5	0.392	222	0.1	Strong
cipher image-2	7.9999	0.01005	10.745	-0.495	0.3921	221	0.2	Strong
cipher image-3	7.9998	0.0101	10.74	-0.49	0.3922	220 0	0.3	Strong
cipher image-4	7.9997	0.01015	10.735	-0.485	0.3923	219	0.4	Strong
cipher image-5	7.9996	0.0102	10.73	-0.48	0.3924	218	0.5	Strong
cipher image-6	7.9995	0.01025	10.725	-0.475	0.3925	217	0.6	Strong
cipher image-7	7.9994	0.0103	10.72	-0.47	0.3926	216	0.7	Strong
cipher image-8	7.9993	0.01035	10.715	-0.465	0.3927	215	0.8	Strong
cipher image-9	7.9992	0.0104	10.71	-0.46	0.3928	214	0.9	Strong
cipher image-10	7.9991	0.01045	10.705	-0.455	0.3929	213	1	Strong
cipher image-11	7.999	0.0105	10.7	-0.45	0.393	212	1.1	Strong
cipher image-12	7.9989	0.01055	10.695	-0.445	0.3931	211	1.2	Strong
cipher image-13	7.9988	0.0106	10.69	-0.44	0.3932	210	1.3	Strong
cipher image-14	7.9987	0.01065	10.685	-0.435	0.3933	209	1.4	Strong
cipher image-15	7.9986	0.0107	10.68	-0.43	0.3934	208	1.5	Strong
cipher image-16	7.9985	0.01075	10.675	-0.425	0.3935	207	1.6	Strong
cipher image-17	7.9984	0.0108	10.67	-0.42	0.3936	206	1.7	Strong
cipher image-18	7.9983	0.01085	10.665	-0.415	0.3937	205	1.8	Strong
cipher image-19	7.9982	0.0109	10.66	-0.41	0.3938	204	1.9	Strong
cipher image-20	7.9981	0.01095	10.655	-0.405	0.3939	203	2.0	Strong
cipher image-21	7.99	0.01505	10.245	0.0001	0.4021	121	10.2	Acceptable
cipher image-22	7.9899	0.0151	10.24	0.00011	0.4022	120	10.3	Acceptable
cipher image-23	7.9898	0.01515	10.235	0.00012	0.4023	119	10.4	Acceptable
cipher image-24	7.9897	0.0152	10.23	0.00013	0.4024	118	10.5	Acceptable
cipher image-25	7.9896	0.01525	10.225	0.00014	0.4025	117	10.6	Acceptable
cipher image-26	7.9895	0.0153	10.22	0.00015	0.4026	116	10.7	Acceptable
cipher image-27	7.9894	0.01535	10.215	0.00016	0.4027	115	10.8	Acceptable
cipher image-28	7.9893	0.0154	10.21	0.00017	0.4028	114	10.9	Acceptable
cipher image-29	7.9892	0.01545	10.205	0.00018	0.4029	113	11	Acceptable
cipher image-30	7.9891	0.0155	10.2	0.00019	0.403	112	11.1	Acceptable
cipher image-31	7.989	0.01555	10.195	0.0002	0.4031	111	11.2	Acceptable
cipher image-32	7.9889	0.0156	10.19	0.00021	0.4032	110	11.3	Acceptable
cipher image-33	7.9888	0.01565	10.185	0.00022	0.4033	109	11.4	Acceptable
cipher image-34	7.9887	0.0157	10.18	0.00023	0.4034	108	11.5	Acceptable
cipher image-35	7.9886	0.01575	10.175	0.00024	0.4035	107	11.6	Acceptable
cipher image-36	7.9885	0.0158	10.17	0.00025	0.4036	106	11.7	Acceptable
cipher image-37	7.9884	0.01585	10.165	0.00026	0.4037	105	11.8	Acceptable
cipher image-38	7.9883	0.0159	10.16	0.00027	0.4038	103	11.9	Acceptable
cipher image-39	7.9882	0.01595	10.155	0.00028	0.4039	102	12	Acceptable
cipher image-40	7.9881	0.016	10.15	0.00029	0.404	101	12.1	Acceptable
cipher image-41	7.9799	0.0201	9.74	0.0012	0.4122	20	20.3	Weak
cipher image-42	7.9798	0.02015	9.735	0.0013	0.4123	19	20.4	Weak
cipher image-43	7.9797	0.0202	9.73	0.0014	0.4124	18	20.5	Weak
cipher image-44	7.9796	0.02025	9.725	0.0015	0.4125	17	20.6	Weak
cipher image-45	7.9795	0.0203	9.72	0.0016	0.4126	16	20.7	Weak
cipher image-46	7.9794	0.02035	9.715	0.0017	0.4127	15	20.8	Weak
cipher image-47	7.9793	0.0204	9.71	0.0018	0.4128	14	20.9	Weak
cipher image-48	7.9792	0.02045	9.705	0.0019	0.4129	13	21	Weak
cipher image-49	7.9791	0.0205	9.7	0.002	0.413	12	21.1	Weak
cipher image-50	7.979	0.02055	9.695	0.0021	0.4131	11	21.2	Weak
cipher image-51	7.9789	0.0206	9.69	0.0022	0.4132	10	21.3	Weak
cipher image-52	7.9788	0.02065	9.685	0.0023	0.4133	9	21.4	Weak
cipher image-53	7.9787	0.0207	9.68	0.0024	0.4134	8	21.5	Weak
cipher image-54	7.9786	0.02075	9.675	0.0025	0.4135	7	21.6	Weak
cipher image-55	7.9785	0.0208	9.67	0.0026	0.4136	6	21.7	Weak
cipher image-56	7.9784	0.02085	9.665	0.0027	0.4137	5	21.8	Weak
cipher image-57	7.9783	0.0209	9.66	0.0028	0.4138	4	21.9	Weak
cipher image-58	7.9782	0.02095	9.655	0.0029	0.4139	3	22	Weak
cipher image-59	7.9781	0.021	9.65	0.003	0.414	2	22.1	Weak
cipher image-60	7.978	0.02105	9.645	0.0031	0.4141	1	22.2	Weak

propose a new image encryption technique based on multiple chaotic systems [24]. The main aim of the proposed technique was to reduce the necessary processing time while also increasing the available concealment. In [10], a chaotic logistic map (CLM) [25]-based image encryption algorithm is proposed. In this work, the author addressed the issues of a using single substitution box (S-box) encryption by using multiple S-box image encryption in which the selection of a particular S-box depends on the random values generated by the CLM. In chaos-based image encryption, S-boxes are a frequent component, given their powerful, nonlinear provision of a diffusion source. S-boxes thus play a vital role in transforming the original data into an encoded format.

Because the strength of chaos-based encryption algorithms depends on the robustness of the S-box, this component must be strong enough to resist statistical attacks. The development of strong S-boxes is a critical research area for security professionals.

To overcome the issues of using weak S-box, we previously proposed a CLM-based methodology capable of creating a new S-box in [26]. The values of the S-box thus generated may vary by a slight change in the initial values of CLM. Apart from the gray scale image encryption, a color image is even more challenging than the encryption of a gray image. This is because with color image encryption, all three channels (R, G, B) must be encrypted. In [27], a color image encryption technique is proposed that utilizes a hybrid chaotic system. The authors used the phenomenon of confusion for the encryption of each R, G, and B component separately and then a mitochondrial DNA sequence was used to diffuse the confused components.

Each of the encryption algorithms explained above has a different level of security: i.e., some are strong, some are acceptable, and some are weak. Which category an algorithm falls into depends on how complex its mathematical structure is.

III. SUPPORT VECTOR MACHINE AS A CLASSIFIER

The SVM algorithm is commonly used for classification purposes, particularly those such as classifying objects from unseen data samples [28]. Here, SVM is used to test various algorithms and determine whether each one has a security level of strong, acceptable, or weak.

This purpose requires several inputs that can be treated as features or feature vectors. Suppose a series of samples consists of $(X_1, Y_1), (X_2, Y_2), (X_3, Y_3) \ldots (X_n, Y_n)$, in which X_i signifies the inputs and Yi signifies the output. The dimensions of the data depend upon the number of features, as demonstrated below:

$$\text{For 2-D dataset: } Y = (X_1, X_2)$$
$$\text{For 3-D dataset: } Y = (X_1, X_2, X_3)$$
$$\text{For n-D dataset: } Y = (X_1, X_2, X_3 \ldots .X_n)$$

where X_1 and X_2 are two independent features on the basis of which SVM classifies the output labels (Y_i).

For a dataset, it is not necessary that the number of features and the number of classes are equal. Instead, the number of classes may vary according to the required output. In the case of a two-dimensional dataset, a line (support vector) is required to separate the data with maximum margins. That margin between the data points represents the maximum distance between the closest data points. In the case of a higher-dimensional dataset, though, a plane may be used to separate the data instead of a line.

As the data used in this work is seven dimensional (7-D), which means seven different features are used to predict the final output label, we are required to find the best plane through which to classify the data with a minimum rate of error. We can define the classification function as follows:

$$F(x) = S.X + B \tag{1}$$

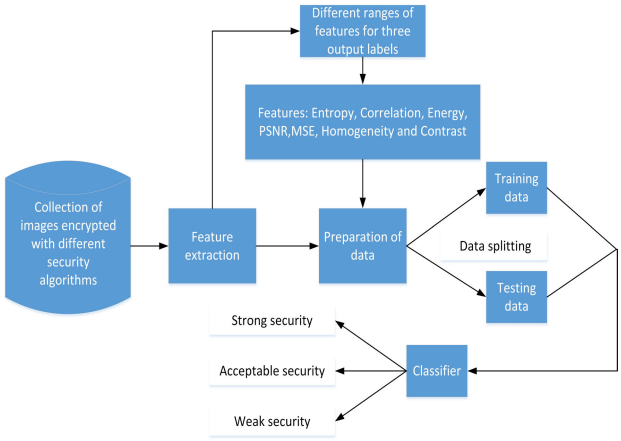


FIGURE 2. Flow diagram of the proposed work.

where S is the weight vector and B is the intercept. Weight (S) can be defined as:

$$S = \frac{xf - xp}{yf - yp} \tag{2}$$

For the linearly separable structure, all the input points should be classified according to equation (1). To maximize the margin, a hyperplane is used, here the margin is signifies the distance from the hyperplane to the nearest data points. To achieve the maximum margin, the factor "w" should be minimum. This equation can be written as:

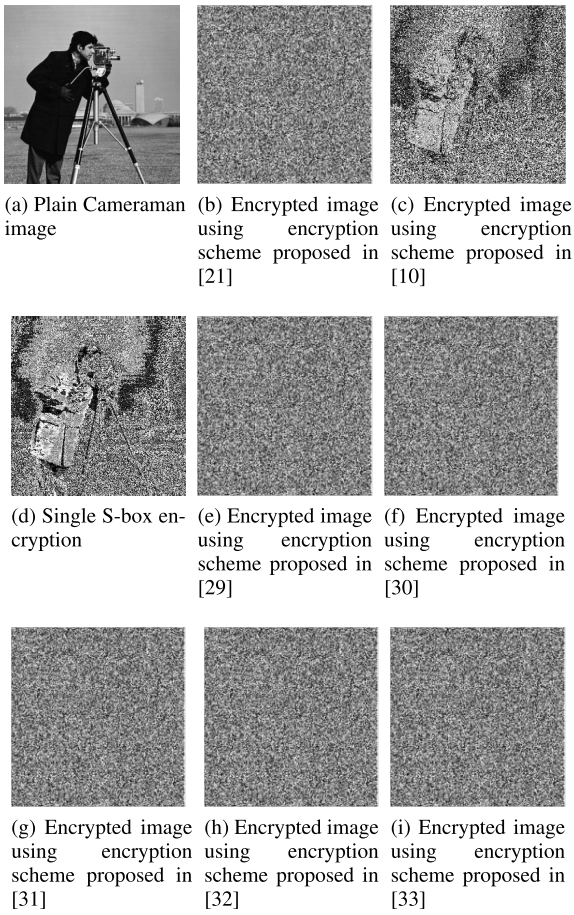
$$\text{Max}_{mar} = \frac{1}{|w|}$$

IV. PROPOSED MODEL FOR SECURITY LEVEL DETECTION OF CRYPTOSYSTEM

In the last few several years, a plethora of encryption algorithms including chaos and transformation-based are proposed. By analyzing the statistical results of the existing encryption algorithms, it is found that some of those algorithms are insecure and do not provide strong security. One way to detect the security level of an encryption algorithm is by analyzing the statistics of its security parameters. Traditional ways of doing this usually entail drawing these comparisons one by one, which can take a great deal of time. To select an appropriate encryption algorithm more quickly, we have developed a machine learning model that incorporates SVM. The schematic diagram of the proposed work is given in Figure 2

In order to detect the security level of a given algorithm, the following steps should be performed:

- Take a big collection of data from different cipher images generated using various encryption algorithms [10], [21], [29]–[33]. The cipher images are shown in Figure 3.
- Extract features from the cipher images. The different features used in the dataset are explained below:



(a) Plain Cameraman image (b) Encrypted image using encryption scheme proposed in [21] (c) Encrypted image using encryption scheme proposed in [10]

(d) Single S-box encryption (e) Encrypted image using encryption scheme proposed in [29] (f) Encrypted image using encryption scheme proposed in [30]

(g) Encrypted image using encryption scheme proposed in [31] (h) Encrypted image using encryption scheme proposed in [32] (i) Encrypted image using encryption scheme proposed in [33]

FIGURE 3. Encrypted images using exiting schemes.

A. SECURITY PARAMETERS AS FEATURES

1) CONTRAST

Contrast analysis shows the difference in pixel values. The greater the difference between pixel values, the more contrast there will be in the image. Higher contrast in turn means better security while lower values of contrast mean that there is only a minor difference between the original pixel values and the manipulated ones. Mathematically, contrast can be expressed as:

$$Cont = \sum |x - y|^2 z(x, y) \tag{3}$$

where z(x, y) signifies the number of gray level co-occurrence matrices (GLCM). The range of contrast values is different for various levels of security. For instance, plain images show contrast values in approximately the interval of [6 7.8], which simply shows that these images have low contrast. Meanwhile, the cipher images show significantly higher contrast values, though the precise difference will depend upon the security level of the system used to encrypt them. To achieve an weak and acceptable security level, the range of the contrast values must lie in the interval of [8.2600 9.7400] and [9.7450 10.2450] respectively, and for strong encryption or high-security level cryptosystems, the range of contrast values lies in the interval [10.2500 10.7500].

2) ENTROPY

Entropy analysis reveals how much randomness an encryption algorithm has created in the cipher image. Maximum entropy values for different images are different depending upon the number of bits of the image. For example, if the image is an 8-bit, the maximum value of the entropy for that particular image will be 8. Similarly, for a single-bit image (binary image), the entropy value will never exceed by 1. For strong encryption, the entropy value for the cipher image must be close to the maximum value. Entropy can be calculated as:

$$Entropy = \sum_{d=1}^{M} p(s_m) log_2(p(s_m)) \tag{4}$$

where $p(s_m)$ is the probability of occurrence of message s_m and M signifies the total number of pixels in the image. According to the entropy value of the 8-bit plain image, we have divided it from 0 to 8 into three intervals, which are given as:

$$[8.0000\ 7.9901] \Rightarrow \text{for strong security}$$
$$[7.9900\ 7.9800] \Rightarrow \text{for acceptable security}$$
$$[7.9799\ 7.9503] \Rightarrow \text{for weak security}$$

3) ENERGY

This parameter is used to find the amount of information present in an image. Higher energy values indicate that the image has more information. The relationship between energy and information is as follows:

$$\text{Energy} \propto \text{Information}$$

Plain images contain more information, which means that their energy value is higher than that of the cipher image, simply because the cipher image contains less information. The mathematical expression for the calculation of energy is given in Equation (5).

$$Energy = \sum_{K=1}^{L} im(x, y)^2 \tag{5}$$

where L signifies the number of pixels present in the plain image and im(x,y) is the pixel position placed at the x^{th} row and y^{th} column. The deficiency in the energy values of the cipher images will impact the ultimate security level of the cryptosystem. More secure cryptosystems will generate cipher images with less energy value.

Energy values are divided into three sections:

$$[0.01000\ \ 0.01500] \Rightarrow \text{for strong security}$$
$$[0.01505\ \ 0.02005] \Rightarrow \text{for acceptable security}$$
$$[0.02010\ \ 0.03490] \Rightarrow \text{for weak security}$$

4) CORRELATION

Correlation is another important parameter for evaluating the security of a given cryptosystem. Correlation refers to how close pixel values are to each other. A large correlation value

shows that the pixel values are very close to each other. For example, if a certain area in the plain image has a gradient black color that changes color slowly, this means that the correlation in the respective area is high. In the plain image, there are many such regions in which the pixel values are close to each other, so the correlation of the plain image is always higher than that of the cipher image. Correlation can be calculated as:

$$\mu_{ab} = \frac{E[a - E(a)][y - E(b)]}{\sqrt{D(a)}\sqrt{D(b)}} \tag{6}$$

where:

$$\mathrm{E(a)} = \frac{1}{M}\sum_{i=1}^{M} a_i$$

Similarly:

$$\mathrm{E(b)} = \frac{1}{M}\sum_{i=1}^{M} b_i$$
$$\mathrm{D(a)} = \frac{1}{M}\sum_{i=1}^{M} [a_i - \mathrm{E(a)}]^2$$

Similarly:

$$\mathrm{D(b)} = \frac{1}{M}\sum_{i=1}^{M} [b_i - \mathrm{E(b)}]^2$$

For strong encryption, correlation values must be minimum. The maximum and minimum correlation value in the image can be $+1$ and -1 respectively. So, if the cipher image is encrypted properly, the correlation value will be close to -1.

The range of possible correlation values is given below:

Range of Correlation value: Corr E $[-1\ +1]$

Based on the above interval, we have divided it into three sub-intervals as follows:

$$[-0.5000\ \ 0.0000] \Rightarrow \text{for strong security}$$
$$[0.0001\ \ 0.0011] \Rightarrow \text{for acceptable security}$$
$$[0.0012\ \ 0.0308] \Rightarrow \text{for weak security}$$

5) HOMOGENEITY

The gray level occurrence matrix (GLCM) illustrates the brightness of pixels in tabular form. For a strong encryption, homogeneity values should be smaller. Homogeneity can be calculated as:

$$\sum_a \sum_b \frac{P(a,b)}{1 + |a - b|} \tag{7}$$

We have divided the homogeneity values into three intervals, as demonstrated below. These intervals are defined for algorithms offering strong, acceptable, and weak security.

$$[0.3920\ \ 0.4020] \Rightarrow \text{for strong security}$$
$$[0.4021\ \ 0.4121] \Rightarrow \text{for acceptable security}$$
$$[0.4122\ \ 0.4418] \Rightarrow \text{for weak security}$$

6) PEAK SIGNAL TO NOISE RATIO (PSNR) AND MEAN SQUARE ERROR (MSE)

PSNR value can be calculated between any two images. Before calculating the PSNR value, it is necessary to calculate the MSE value between the two desired images. If the PSNR value between the two images (original and cipher) is high, this means that the processed image is very close to the original image. Meanwhile, the MSE is inversely proportional to the PSNR, as shown in equation 8. So, for a strong encryption, there should be a minimum PSNR value difference between the plain image and the cipher. Likewise, the error between the plain and the cipher image should be close to maximum. PSNR and MSE can be calculated using equations 8 and 9 respectively.

$$PSNR = 20log_{10}(\frac{max_{val}}{\sqrt{MSE}}) \tag{8}$$

where max_{val} signifies the highest pixel value present in the plain image.

$$MSE = \frac{1}{XY}\sum_{a=1}^{X}\sum_{b=1}^{Y}(P_{im}(a,b) - C_{im}(a,b)) \tag{9}$$

where XY represents the total number of pixels in the plain image while P_{im} and C_{im} are the plain and the cipher images respectively.

To categorize the PSNR and MSE value for strong, acceptable, and weak security levels in various cryptosystems, we have divided the PSNR and MSE value into three intervals, given as:

ForPSNR

$$[0.1000\ \ 10.1000] \Rightarrow \text{for strong security}$$
$$[10.2000\ \ 10pt20.2000] \Rightarrow \text{for acceptable security}$$
$$[20.3000\ \ 10pt49.9000] \Rightarrow \text{for weak security}$$

ForMSE

$$[1\ 100] \Rightarrow \text{for weak security}$$
$$[101\ 200] \Rightarrow \text{for acceptable security}$$
$$[201\ 400] \Rightarrow \text{for strong security}$$

- The dataset is created using the intervals explained above. Once the dataset is created, a portion of it will be separated for training purposes while the rest is used for testing.
- After the training and testing stages, we will extract the features from another cipher image in order to attempt the prediction of the security level achievable by the encryption algorithm through which the cipher image is generated.
- Finally, to evaluate our proposed model, we will test its accuracy, F1 score, recall, and precision.

Table 3 provides the statistics of the security parameters for different cipher images generated using existing cryptosystems. The status of each system's security level is also given, based on the value of both features and intervals.

TABLE 3. Evaluation of Security Statuses of Existing Encryption Schemes Using the Proposed Algorithm.

Existing encryption schemes	Contrast	Entropy	Energy	Correlation	Homogeneity	PSNR	MSE	Security status
Ref [21]	9.9970	7.97609	0.0182	0.00058	0.4093	11.6830	240	Acceptable
Ref [10]	8.9650	7.9285	0.02335	0.0062	0.4193	23.1580	231	Acceptable
Single S-box encryption	8.4130	7.8634	0.02451	0.0067	0.4028	25.3678	185	Weak
Ref [29]	10.3573	7.9938	0.0158	-0.1350	0.3934	8.9980	257	Strong
Ref [30]	11.3587	7.9983	0.0150	-0.0950	0.3981	9.1375	271	Strong
Ref [31]	10.9876	7.99315	0.1683	-0.0650	0.3995	9.8642	286	Strong
Ref [32]	9.6382	7.9836	0.0177	0.00064	0.4073	13.9863	225	Acceptable
Ref [33]	10.8938	6 7.9930	0.0149	-0.045	0.3930	9.9786	295	Strong

TABLE 4. Generalized Confusion Matrix for the Proposed Model.

Total No. of Test Samples (N)	Predicted Strong Security	Predicted Acceptable Security	Predicted Weak Security
Actual Strong Security	True Positive	(False Negative)$_{(1)}$	(False Negative)$_{(2)}$
Actual Acceptable Security	(False Positive)$_{(1)}$	(True Negative)$_{(1)}$	(False Negative)$_{(3)}$
Actual Weak Security	(False Positive)$_{(2)}$	(False Negative)$_{(4)}$	(True Negative)$_{(2)}$

TABLE 5. Confusion Matrix When Test Samples are 20% of Total Dataset.

Total No. of Test Samples (N)	Predicted Strong Security	Predicted Acceptable Security	Predicted Weak Security
Actual Strong Security	21	1	1
Actual	0	21	0
Actual	0	0	56

V. STATISTICAL ANALYSIS OF THE PROPOSED MODEL

To evaluate the performance of the proposed model, we have done some experimental analysis, as outlined below.

A. CONFUSION MATRIX

The confusion matrix is a two-dimensional array that can be utilized to find accuracy, recall. and precision. The generalized confusion matrix for our proposed model is given in Table 4 while Table 5 shows this confusion matrix when we have taken a 20% test sample from the dataset.

In the classification of accuracy, four unavoidable terms (given in Table 4) can be helpful in gauging our model's performance. An explanation of these four terms according to the proposed model is given below.

1) TRUE POSITIVES

When the system predicts "strong security" while the real output was also "strong security".

2) TRUE NEGATIVES

When the system predicts "acceptable security" while the real output was also "acceptable security".

Or

When the system predicts "weak security" case while the real output was also "weak security".

3) FALSE POSITIVES

When the system predicts "strong security" while the real output was "acceptable or weak security".

4) FALSE NEGATIVES

When the system predicts "acceptable security" or "weak security" while the real output was "strong security".

Or

When the system predicts "weak security" while the real output was "acceptable security"

By using the confusion matrix, accuracy can be expressed as:

$$\text{Accuracy} = \frac{\text{Addition of all the values of first diagonal}}{\text{total number of samples}} \tag{10}$$

According to Table 5, the percentage of accuracy from the proposed work will be:

$$\text{Percentage Accuracy} = \frac{21+21+56}{21+21+56+1+1} \times 100\%$$
$$\text{Percentage Accuracy} = 98\%$$

B. CLASSIFICATION ACCURACY

The accuracy of this system reveals the information about how many correct predictions have been made by the model. The more correct predictions made, the higher the resulting accuracy. This classification accuracy can be measured as:

$$\text{Classification accuracy} = \frac{\text{No. of correct predictions}}{\text{Total number of predictions}} \tag{11}$$

According to the Table 5, the percentage classification accuracy of our proposed work will be:

$$\text{percentage Classification accuracy} = \frac{21+21+56}{21+21+56+1+1} \times 100$$
$$\text{percentage Classification accuracy} = 98\%$$

It can also be found as follows:

$$\text{percentage Classification accuracy} = \frac{\text{T.P} + \text{T.N}}{\text{Total samples}} \times 100\% \tag{12}$$

In the case of our proposed work, the percentage of classification accuracy will be:

$$= \frac{\text{T.P} + (\text{T.N})_{(1)} + (\text{T.N})_{(2)}}{\text{Total samples}} \times 100\%$$
$$\text{Percentage of Classification accuracy} = \frac{21+21+56}{21+21+56+1+1} \times 100$$
$$\text{Percentage of Classification accuracy} = 98\% \tag{13}$$

TABLE 6. Statistical Values of Different Parameters Wen the Proposed Model is Implemented Using SVM, KNN, RF and DT.

	DT				KNN				RF				Proposed (When selected) (SVM)			
Percentage of test samples	%ag Accuracy	Precision	Recall	F1 score	%ag Accuracy	Precision	Recall	F1 score	%ag Accuracy	Precision	Recall	F1 score	%ag Accuracy	Precision	Recall	F1 score
15 percent	95.5	0.94	0.85	0.89	94.4	0.85	0.78	0.81	0.85	0.82	0.79	0.80	97.3	1	0.87	0.93
20 percent	90.6	0.85	0.79	0.81	88	0.83	0.81	0.81	0.90	0.90	0.80	0.84	98	1	0.91	0.94
25 percent	95.9	0.95	0.81	0.87	92	0.94	0.84	0.88	0.91	0.82	0.79	0.80	96	1	0.8	0.93
30 percent	95	0.94	0.82	0.87	92	0.94	0.82	0.87	94.8	0.94	0.81	0.87	98	1	0.90	0.94
35 percent	94.5	0.92	0.89	0.90	91	0.92	0.85	0.88	92.5	0.89	0.83	0.85	97.7	0.97	0.91	0.93
40 percent	92	0.91	0.81	0.85	90	0.94	0.80	0.86	0.89	0.78	0.80	0.78	96	1	0.85	0.91
45 percent	91.5	0.84	0.79	0.81	94	0.84	0.81	0.82	94	0.84	0.82	0.82	97.3	0.9	0.95	0.92

TABLE 7. Statistical Values of Different Parameters for the Proposed and Existing Work (A Comparison).

	[34]				[35]				[36]			
Percentage of test samples	%ag Accuracy	Precision	Recall	F1 score	%ag Accuracy	Precision	Recall	F1 score	%ag Accuracy	Precision	Recall	F1 score
15 percent	96.5	0.95	0.86	0.90	94.6	0.89	0.80	0.84	0.88	0.87	0.81	0.83
20 percent	91.6	0.89	0.81	0.84	91	0.93	0.87	0.89	0.96	0.99	0.85	0.91
25 percent	96.9	0.98	0.85	0.91	95	0.98	0.86	0.91	0.95	0.89	0.81	0.84
30 percent	97	0.98	0.89	0.93	96	0.97	0.87	0.91	96.8	0.96	0.86	0.90
35 percent	96.5	0.97	0.90	0.93	96	0.95	0.89	0.91	95.5	0.91	0.88	0.89
40 percent	95	0.96	0.83	0.89	92	0.97	0.81	0.88	0.91	0.89	0.82	0.85
45 percent	95.5	0.89	0.81	0.84	97	0.88	0.84	0.85	96	0.87	0.89	0.87

C. PRECISION AND RECALL

Precision is the ratio between the true positive predicted observations and the total number of positive predicted observations. Mathematically, this can be expressed as:

$$\text{Precision} = \frac{\text{T.P}}{\text{T.P} + \text{F.P}} \tag{14}$$

In the case of our proposed work, the precision will be:

$$\text{Precision} = \frac{\text{T.P}}{\text{T.P} + (\text{F.P})_{(1)} + (\text{F.P})_{(2)}} \tag{15}$$

According to the values given in Table 5, the precision value for our proposed model will be:

$$\text{Precision} = \frac{21}{21 + 0 + 0} = 1$$

Recall refers to the sensitivity of the model. The greater the recall score, the more sensitive the model will be. In other words, this expresses the ratio of true positive observation and the total number of true positive and false negative observations. Mathematically, recall can be calculated as:

$$\text{Recall} = \frac{\text{T.P}}{\text{T.P} + \text{F.N}} \tag{16}$$

In the case of our proposed work, the equation 16 can be written as:

$$\text{Recall} = \frac{\text{T.P}}{\text{T.P} + (\text{F.N})_{(1)} + (\text{F.N})_{(2)} + (\text{F.N})_{(3)} + (\text{F.N})_{(4)}} \tag{17}$$

According to the values given in Table 5, the recall value for our proposed model will be:

$$\text{Recall} = \frac{21}{21 + 1 + 1 + 0 + 0} = 0.91$$

D. F1 SCORE

Accuracy and F1 score both are important metrics when evaluating the performance of machine learning models. Accuracy is important when true positive and true negative samples are more valuable, while the F1 score is important when false positive and false negative samples are more important. F1 score can be calculated as:

$$\begin{aligned}\text{F1 Score} &= \left[\frac{(\text{Recall})^{-1} + (\text{Precision})^{-1}}{2}\right]^{-1} \\ &= 2\left(\frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}\right)\end{aligned} \tag{18}$$

When the proposed model is tested on a 20% sample of the total data, the F1 score calculated (using equation 18) will be:

$$\text{F1 score} = 2 \times \frac{1 \times 0.91}{1 + 0.91} = 0.94$$

The precision, percentage, accuracy, recall, and F1 scores achieved by our proposed model using SVM, K-nearest neighbour (KNN), random forest (RF) and decision tree (DT) when the different percentages of the test samples are selected from the total data, is given in Table 6. We preferred to choose SVM over other machine learning algorithms due to the better performance of SVM as it can be seen on Table 6, the the proposed model exhibits better results when we use SVM instead of other machine learning algorithms such KNN, RF and DT. Apart from the comparison between different machine learning algorithms, we have also compared the proposed model with the existing ones given in Table 7 to show the superiority of the proposed model.

VI. CONCLUSION

In this article, we have developed and proposed a model that can detect the security level of various encryption schemes quickly and accurately. We began by creating a dataset and incorporating the security parameters common to various encryption schemes as features. To prepare a dataset, we have divided the values of all features into three intervals—strong, acceptable, and weak—that describe the resulting security levels. Next, the different encryption schemes are tested on our proposed model in order to detect the level of security each one offers. We can also detect the security level of these encryption schemes manually by determining the statistical values of each one. With traditional testing methods, this process takes a great deal of time to accomplish but with our proposed model, testing can be achieved within a few seconds. To conclude, we also tested our proposed model using different experiments to evaluate its performance, and we found that it produces 98% correct predictions at much faster speeds than other models currently available.

In the future work, the use of deep learning techniques to detect the security level of cryptosystems will be investigated [37], [38].

REFERENCES

[1] 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, pp. 317–330, 2019.
[2] A. Anees, I. Hussain, A. Algarni, and M. Aslam, "A robust watermarking scheme for online multimedia copyright protection using new chaotic map," *Secur. Commun. Netw.*, vol. 2018, pp. 1–20, Jun. 2018.
[3] A. Shafique and J. Ahmed, "Dynamic substitution based encryption algorithm for highly correlated data," *Multidimensional Syst. Signal Process.*, May 2020.
[4] F. Ahmed, A. Anees, V. U. Abbas, and M. Y. Siyal, "A noisy channel tolerant image encryption scheme," *Wireless Pers. Commun.*, vol. 77, no. 4, pp. 2771–2791, Aug. 2014.
[5] M. A. B. Farah, R. Guesmi, A. Kachouri, and M. Samet, "A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation," *Opt. Laser Technol.*, vol. 121, Jan. 2020, Art. no. 105777.
[6] C. E. Shannon, "Communication in the presence of noise," *Proc. IEEE*, vol. 72, no. 9, pp. 1192–1201, Sep. 1984.
[7] S. Heron, "Advanced encryption standard (AES)," *Netw. Secur.*, vol. 2009, no. 12, pp. 8–12, Dec. 2009.
[8] H. Liu, A. Kadir, and X. Sun, "Chaos-based fast colour image encryption scheme with true random number keys from environmental noise," *IET Image Process.*, vol. 11, no. 5, pp. 324–332, Apr. 2017.
[9] Y.-L. Lee and W.-H. Tsai, "A new secure image transmission technique via secret-fragment-visible mosaic images by nearly reversible color transformations," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 24, no. 4, pp. 695–703, Apr. 2014.
[10] A. Anees, A. M. Siddiqui, and F. Ahmed, "Chaotic substitution for highly autocorrelated data in encryption algorithm," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 19, no. 9, pp. 3106–3118, Sep. 2014.
[11] L. Liu, Y. Lei, and D. Wang, "A fast chaotic image encryption scheme with simultaneous permutation-diffusion operation," *IEEE Access*, vol. 8, pp. 27361–27374, 2020.
[12] M. Khalili and D. Asatryan, "Colour spaces effects on improved discrete wavelet transform-based digital image watermarking using Arnold transform map," *IET Signal Process.*, vol. 7, no. 3, pp. 177–187, May 2013.
[13] L. Zhang, J. Wu, and N. Zhou, "Image encryption with discrete fractional cosine transform and chaos," in *Proc. 5th Int. Conf. Inf. Assurance Secur.*, vol. 2, 2009, pp. 61–64.
[14] M. Zhang, X.-J. Tong, J. Liu, Z. Wang, J. Liu, B. Liu, and J. Ma, "Image compression and encryption scheme based on compressive sensing and Fourier transform," *IEEE Access*, vol. 8, pp. 40838–40849, 2020.
[15] J. S. Khan, W. Boulila, J. Ahmad, S. Rubaiee, A. U. Rehman, R. Alroobaea, and W. J. Buchanan, "DNA and plaintext dependent chaotic visual selective image encryption," *IEEE Access*, vol. 8, pp. 159732–159744, 2020.
[16] A. Qayyum, J. Ahmad, W. Boulila, S. Rubaiee, Arshad, F. Masood, F. Khan, and W. J. Buchanan, "Chaos-based confusion and diffusion of image pixels using dynamic substitution," *IEEE Access*, vol. 8, pp. 140876–140895, 2020.
[17] F. Masood, W. Boulila, J. Ahmad, Arshad, S. Sankar, S. Rubaiee, and W. J. Buchanan, "A novel privacy approach of digital aerial images based on mersenne twister method with DNA genetic encoding and chaos," *Remote Sens.*, vol. 12, no. 11, p. 1893, Jun. 2020.
[18] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Inf. Sci.*, vol. 480, pp. 403–419, Apr. 2019.
[19] G. Kaur, R. Agarwal, and V. Patidar, "Chaos based multiple order optical transform for 2D image encryption," *Eng. Sci. Technol., Int. J.*, vol. 23, no. 5, pp. 998–1014, Oct. 2020.
[20] Abhishek, S. N. George, and P. P. Deepthi, "PWLCM based image encryption through compressive sensing," in *Proc. IEEE Recent Adv. Intell. Comput. Syst. (RAICS)*, Dec. 2013, pp. 48–52.
[21] J. S. Khan and J. Ahmad, "Chaos based efficient selective image encryption," *Multidimensional Syst. Signal Process.*, vol. 30, no. 2, pp. 943–961, Apr. 2019.
[22] L. G. Nardo, E. G. Nepomuceno, J. Arias-Garcia, and D. N. Butusov, "Image encryption using finite-precision error," *Chaos, Solitons Fractals*, vol. 123, pp. 69–78, Jun. 2019.
[23] A. Anees and I. Hussain, "A novel method to identify initial values of chaotic maps in cybersecurity," *Symmetry*, vol. 11, no. 2, p. 140, Jan. 2019.
[24] A. Shafique and J. Shahid, "Novel image encryption cryptosystem based on binary bit planes extraction and multiple chaotic maps," *Eur. Phys. J. Plus*, vol. 133, no. 8, p. 331, Aug. 2018.
[25] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image Vis. Comput.*, vol. 24, no. 9, pp. 926–934, Sep. 2006.
[26] A. Shafique, "A new algorithm for the construction of substitution box by using chaotic map," *Eur. Phys. J. Plus*, vol. 135, no. 2, pp. 1–13, Feb. 2020.
[27] H. G. Mohamed, D. H. ElKamchouchi, and K. H. Moussa, "A novel color image encryption algorithm based on hyperchaotic maps and mitochondrial DNA sequences," *Entropy*, vol. 22, no. 2, p. 158, Jan. 2020.
[28] C. Assia, C. Yazid, and M. Said, "Segmentation of brain MRIs by support vector machine: Detection and characterization of strokes," *J. Mech. Med. Biol.*, vol. 15, no. 5, Oct. 2015, Art. no. 1550076.
[29] R. Guesmi, M. A. B. Farah, A. Kachouri, and M. Samet, "A novel chaos-based image encryption using DNA sequence operation and secure hash algorithm SHA-2," *Nonlinear Dyn.*, vol. 83, no. 3, pp. 1123–1136, Feb. 2016.
[30] Y. Li, C. Wang, and H. Chen, "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation," *Opt. Lasers Eng.*, vol. 90, pp. 238–246, Mar. 2017.
[31] R. Ge, G. Yang, J. Wu, Y. Chen, G. Coatrieux, and L. Luo, "A novel chaos-based symmetric image encryption using bit-pair level process," *IEEE Access*, vol. 7, pp. 99470–99480, 2019.
[32] P. R. Krishna, C. V. M. S. Teja, S. R. Devi, and V. Thanikaiselvan, "A chaos based image encryption using tinkerbell map functions," in *Proc. 2nd Int. Conf. Electron., Commun. Aerosp. Technol. (ICECA)*, Mar. 2018, pp. 578–582.
[33] A. Roy, A. P. Misra, and S. Banerjee, "Chaos-based image encryption using vertical-cavity surface-emitting lasers," *Optik*, vol. 176, pp. 119–131, Jan. 2019.
[34] T. B. Dijkhuis, F. J. Blaauw, M. W. van Ittersum, H. Velthuijsen, and M. Aiello, "Personalized physical activity coaching: A machine learning approach," *Sensors*, vol. 18, no. 2, p. 623, Feb. 2018.
[35] M. S. Anwar, J. Wang, W. Khan, A. Ullah, S. Ahmad, and Z. Fei, "Subjective QoE of 360-degree virtual reality videos and machine learning predictions," *IEEE Access*, vol. 8, pp. 148084–148099, 2020.
[36] J. Ker, Y. Bai, H. Y. Lee, J. Rao, and L. Wang, "Automated brain histology classification using machine learning," *J. Clin. Neurosci.*, vol. 66, pp. 239–245, Aug. 2019.
[37] M. Al-Sarem, W. Boulila, M. Al-Harby, J. Qadir, and A. Alsaeedi, "Deep learning-based rumor detection on microblogging platforms: A systematic review," *IEEE Access*, vol. 7, pp. 152788–152812, 2019.
[38] S. B. Atitallah, M. Driss, W. Boulila, and H. B. Ghézala, "Leveraging deep learning and IoT big data analytics to support the smart cities development: Review and future directions," *Comput. Sci. Rev.*, vol. 38, Nov. 2020, Art. no. 100303.

ARSLAN SHAFIQUE received the B.E. degree in mechatronics engineering from the Wah Engineering College, Wah Cantt, in 2014, and the M.S. degree in electrical engineering from Heavy Industries Taxila Education City (HITEC) University, Taxila, in 2017. He is currently pursuing the Ph.D. degree with the Faculty of Engineering and Applied Sciences, Riphah International University, Islamabad, Pakistan. He is also serving as a Research Associate for Riphah International University. His research interests include cryptography, secure communication, and machine learning.

JAMEEL AHMED (Member, IEEE) received the B.E. degree in electronic engineering from the NED University of Engineering and Technology, Karachi, the M.S. degree in electrical engineering from the National University of Science and Technology, and the Ph.D. degree from Pakistan and Nanyang Technological University (NTU), Singapore. Subsequently, he has carried out a Postdoctoral Fellowship twice with NTU. He is actively involved in teaching and research for the last 25 years. He is currently a Professor and the Dean of the Faculty of Engineering and Applied Sciences, Riphah International University, Islamabad. He has published more than 50 national and international research publications. In addition, he has authored four international and one national book. He is a member of NCRC and HEC and an Elected Member of the Governing Body of the Pakistan Engineering Council.

WADII BOULILA (Senior Member, IEEE) received the B.Eng. degree (Hons.) in computer science from the Aviation School, Borj El Amri, in 2005, the M.Sc. degree from the National School of Computer Science (ENSI), University of Manouba, Tunisia, in 2007, and the Ph.D. degree conjointly from ENSI and Telecom-Bretagne, University of Rennes 1, France, in 2012. He is currently an Associate Professor of computer science with the IS Department, College of Computer Science and Engineering, Taibah University, Medina, Saudi Arabia. He is also a Senior Researcher with the RIADI Laboratory, University of Manouba, and also a Senior Research Fellow with the ITI Department, University of Rennes 1. He participated in many research and industrial funded projects. His current research interests include big data analytics, deep learning, cybersecurity, data mining, artificial intelligence, uncertainty modeling, and remote sensing images. He is a Senior Fellow of the Higher Education Academy (SFHEA), U.K. He has served as a TPC member, the chair, and a reviewer for many leading international conferences and journals.

HAMZAH GHANDORH received the Ph.D. degree from the Faculty of Engineering, University of Western Ontario, London, ON, Canada, in 2017, under the supervision of Roy Eagleson. Since 2018, he has been an Assistant Professor with the Faculty of Computer Science and Engineering, Taibah University, Medina, Saudi Arabia, doing his research as a Principal Investigator with the Mixed Reality Laboratory, Taibah University, Medina. His research interests include software engineering and surgical simulation, human–computer interface design, the integration of immersive experiences, and artificial intelligence.

JAWAD AHMAD (Senior Member, IEEE) is currently an experienced researcher with more than ten years of cutting-edge research and teaching experience in prestigious institutes including Edinburgh Napier University, U.K., Glasgow Caledonian University, U.K., Hongik University, South Korea, and HITEC University, Taxila, Pakistan. He has coauthored more than 50 research articles, in international journals and peer-reviewed international conference proceedings. He has taught various courses both at undergraduate (UG) and postgraduate (PG) levels during his career. He regularly organizes timely special sessions and workshops for several flagship IEEE conferences. His research interests include cybersecurity, multimedia encryption, and machine learning and applications. He is an invited reviewer for numerous world-leading high-impact journals (reviewed more than 50 journal papers to date).

MUJEEB UR REHMAN received the B.Eng. (Hons.) and M.S. (Hons.) degrees in electrical engineering from Riphah International University (RIU), Islamabad, Pakistan, in 2014 and 2018, respectively, where he is currently pursuing the Ph.D. degree. He is also serving as a Research Associate for the Faculty of Engineering and Applied Sciences, RIU. His research interest includes the design of passive microwave filters.