Ensuring Data Security in Images through Improved SVM Classifier

Wafaa Ali[1], Walaa Alajali[2], Abdulrahman D. Alhusaynat[3]

[1]Thi-Qar University, Education College for Pure Science, Nassiriya, Thi-Qar, 64001, Iraq
Email: *wafaa-a[at]utq.edu.iq*

[2]Thi-Qar University, Education College for Pure Science, Nassiriya, Thi-Qar, 64001, Iraq
Email: *walaakhshlan[at]utq.edu.iq*

[3]Thi- Qar Education Directorate, Nassiriya, Thi-Qar, 64001, Iraq
Email: *rahmandakhil2[at]gmail.com*

Abstract: ***In the era of information and communication technology, ensuring image security has become a priority and a concern to confront cyber threats, unauthorized access and tampering. Traditional techniques provide a certain level of security but in fact lack the ability to process image anomalies, hence the challenge to propose a machine learning technique and improve the Support Vector Machine (SVM) classifier. This study presented a classifier to enhance data security in images by working with an encryption and feature extraction system that relies on higher chaotic weights for specific sections of the image. The proposed method reduces the dimensions of the image to sections and from there to the real dimensions of the image. The improved classifier achieved higher accuracy in terms of creating complex randomness in the two main stages of confusion and diffusion. The experimental results demonstrate the effectiveness of the classifier in terms of entropy = 8 and is an effective value, histogram uniformity, anomaly detection and encryption complexity. These results provide a reliable and scalable solution in many fields such as healthcare, economics and information transmission in social media. A comprehensive approach can be provided by integrating the proposed method with other methods to protect image data.***

Keywords: Support Vector Machine, Image, Encryption

1. Introduction

In our current time and the development of Internet and communications technology, images are one of the most important forms of exchange over the Internet. Images are used in many facilities such as security, social communication, the medical field, and communications. Hence, due to their wide spread, security concerns have arisen about the use of data by unauthorized persons. Images often contain sensitive data and must be preserved, especially with the current widespread cyber-attacks [1]. Hence, the challenge and proposal of traditional encryption algorithms came. Despite their effectiveness, the acceleration of cyber-attacks has become everyone's obsession and requires a challenge to find new and advanced methods that keep pace with the rapid technological development.

In recent years, with the development of technology and communications and the spread of social networking sites and cloud storage, exposure to attacks has become widespread within the framework of cyber attacks and data security has become a priority in all military, financial, economic and other specialties [2]. Images are the most vulnerable data to attacks because they have high capacity, strong interconnection and repetition between pixels. The goal that the whole world is currently seeking is data security, and one of the most effective methods is encryption, which makes the data unreadable only by authorized persons who can retrieve it. As there are many encryption methods mentioned in previous studies, this makes encryption a subject of challenge.

Artificial Intelligence (AI) techniques have emerged in abundance recently, and one of the most important of these techniques is machine learning, especially Support Vector Machines (SVM). It has been used as a promising tool in maintaining the security of data in images in particular. SVM is widely used in the field of classification and anomaly detection, which helps in identifying malicious activities in images. SVM can distinguish between normal and hacked data through the internal features of images [3]. However, such classifiers face some problems and limitations in very high-resolution and high-dimensional images.

In digital image encryption, there are two main factors: diffusion and confusion, and thus the encryption is very secure. The encryption in the image is in the frame of pixels, which are the basic units of the image or changes in columns and rows, as well as the process of changing the values of the original pixels, in other words, there is a change in the value of the pixel and its location in the encrypted image [4]. Encryption can be done using machine learning, which is the classification of pixel locations in the image and choosing their locations according to their weights. As well as the process of changing the locations of columns and rows within the randomness of the image. In some methods, you change the locations of the bits of a single pixel in the image in order to change its value, so it is different from its original value. This is the basis of image encryption.

In this paper, we explore the improvement of a well-known SVM classifier specifically designed to address the challenges of image data security. By enhancing the feature extraction process, tuning the kernel function and improving the dimensions, it achieves better accuracy and detects anomalies in the image that lead to any security threat. In this paper, we leverage the strengths of SVM and overcome its previous limitations to ensure higher accuracy and more reliability of image data.

This research aims to provide a more effective solution by developing an SVM-based algorithm to secure data in images, focusing on improving the performance of the classifier to process large and complex data. As well as improving data extraction from image data and determining whether or not there is tampering in the image data. The conclusion is to ensure the security of data in images in various applications.

Contributions of this Study

- We have improved a new model for image data security to ensure higher security level by machine learning and SVM algorithm.
- Depict an encryption method based on merging chaos of image pixels with complex encryption key to secure data in the image.
- Obtain results and analysis for criteria such as accuracy, recall, histogram, etc. to evaluate the proposed method.

2. Related Works

Many algorithms that have been considered as image security have been proposed by previous studies to secure the image before transmission. The encryption methods in development are based on chaos or transform methods such as discrete cosine transform, discrete wavelet transform, and discrete Fourier transform (DFT) [5]. There are many methods that have been proposed in previous studies, including: In [6] proposed an algorithm combining chaos and cosine transform and using three types of chaos maps which increase the overall complexity to show effective chaotic behavior of encryption which enhances more data security. [7] Proposed a second type optical image encryption scheme for complex images which is based on chaos and in this study it was demonstrated that it can generate multiple vectors for this purpose.

For fast image encryption, [8] Proposed a selective encryption scheme based on chaos in complex parts of image data. [9] Proposed a fast algorithm based on fast encryption using changing each bit in the image but in a different way from the other pixel sequence, and from this came the complexity of the algorithm. An algorithm proposed by [10] achieved a high level of accuracy using one of the machine learning algorithms and generating complex random numbers to solve the weakness of traditional methods. In an innovative way, [11] proved that keeping secret data is done using encryption better than the steganography method, which depends on the strength of hiding, as encryption is often strong if the method is correct and depends on chaos.

In addition, [12] Relied on deep learning to predict the randomness of the algorithm, on which the complexity of the encryption algorithm depends, as the randomness that depends on deep learning is more chaotic than traditional methods. A study based on statistical methods [13] claimed that traditional methods that rely on a strong encryption key are more likely to secure data than those that rely on merging more than one method to create a high level of chaos. While a study [14] based on SVM confirmed that the more training operations for the algorithm leads to better encryption and optimal data security. A study [15] has shown that securing data in images is better than securing text data due to the many details related to the pixel bits and their location in the image, which can create a more chaotic approach than others. A study based on SVM [16] has confirmed that complex chaos is created by applying traditional methods to the image components and including them within SVM to extract new features and ensure the security of image data.

3. Machine Learning

Machine learning (ML) is one of the most important applications of AI that we will take into consideration in this study. To review the applications of ML in image security, it is first necessary to understand the basic concepts related to this field. Below we present some basic principles and definitions. Artificial intelligence techniques are used in many applications such as military, industrial, security, etc. [17-19] AI techniques have helped in analyzing data obtained from images, which is often necessary and has a large security and economic dimension.

ML is an application of artificial intelligence that enables systems to learn on their own and improve their performance through experience and expertise without the need for specific programming. This field focuses on developing computer programs that can access and use data in the learning process [20]. This process begins with observations or data, such as practical examples, direct experiences, or instructions, where this data is used to discover patterns and make more effective decisions based on the examples provided. The main goal of machine learning is to enable machines to learn independently without human intervention, and to adapt their actions according to the results they reach.

Machine learning algorithms are usually classified into supervised and unsupervised algorithms. However, this classification is very broad and does not cover all available methods [21].

- Supervised ML algorithms can use knowledge gained from past experiences and training on pre-defined examples to predict future events using unseen data. These algorithms start by analyzing a set of training data (pre-defined examples) to predict possible output values. After sufficient training, the system is able to provide appropriate predictions for each new input. In addition, the algorithm can compare its results to the correct outputs, identifying errors to modify and improve the model. Examples of such algorithms include: Support Vector Machine (SVM), Decision Tree, Random Forest, KNN algorithm, and Regression [22].
- Unsupervised ML algorithms are used in cases where the training data is unlabeled or unlabeled. These algorithms aim to understand how the system can infer a function that describes the hidden pattern in the unlabeled data. Although these algorithms may not determine specific results, they explore the data and can infer and describe hidden structures in the unlabeled data. Examples of such

algorithms include Apriori, K-means, and Expectation-Maximization (EM) [23].

- Semi-supervised ML algorithms fall somewhere between supervised and unsupervised algorithms, and are trained on both labeled and unlabeled data. Typically, a small portion of the data is labeled, while a larger portion is unlabeled. Systems using these algorithms can achieve a high level of accuracy. Semi-supervised learning is preferred when labeled data requires specialized and efficient resources to obtain, as producing such data is expensive and time-consuming. In contrast, accessing unlabeled data typically does not require additional resources [24].

Machine learning is considered a part of artificial intelligence, which is considered a main title, and in turn it consists of a smaller part that contains it, which is deep learning, as in Figure 2. For each application, artificial intelligence algorithms work to solve it, and one of them can work efficiently and another may not work with the same efficiency.

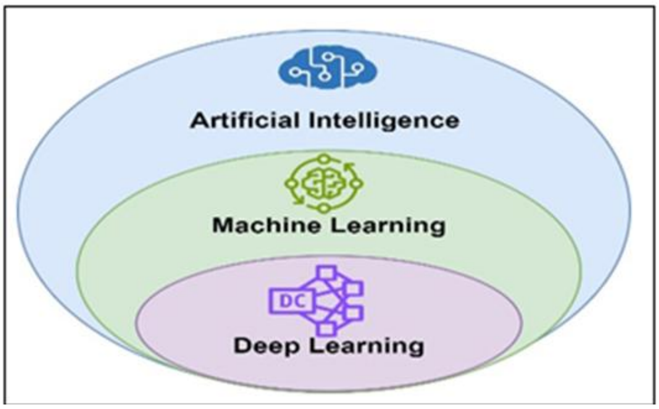


Figure 1: Relation among AI, ML and DL

ML allows for the analysis of large amounts of data, and typically provides faster and more accurate results for identifying profitable opportunities or high risks. However, machine learning can require additional time and resources to ensure it is properly trained. Machine learning relies on curated data that is used to analyze and build the learning model, which means the need for a suitable set of data that can be used effectively in the learning process.

Many ML algorithms suggested in literature, and choosing the most suitable algorithm for a particular problem depends on a set of characteristics such as speed, accuracy, training time, prediction time, amount of data required for training, type of data, ease of implementation, etc. Often, the time factor is of utmost importance, especially in image applications.as shown in Table 1 [25].

Table 1: Time complexity of some ML algorithms

Algorithm	Learning	Predicting
Regression	$O(p^2n+p^3)$	O(p)
Decision Tree	$O(n^2p)$	O(p)
Random Fores0t	$O(n^2pn_t)$	$O(pn_t)$
Naïve Bayes	O(np)	O(p)
SVM	$O(n^2p+n^3)$	$O(pn_{sv})$
KNN	---	O(np)
K-means	$O(n^{pk+1})$	O(k)

For avoiding dependency on certain condition, have to analyze algorithm runtime for asymptotic sense. Thus, n represent training number, and p is feature number, while n_t is the tree number and n_{sv} support vector number, k represent the cluster number. And the complexity of ML is calculated according the table.

Learning time is the time required to train the model using the dataset, and depends on the size of the data and the type of algorithm used.

Prediction time is the time required to test the model using a new dataset or predict unseen data, and also varies depending on the size of the data and the type of algorithm used.

In most cases, about 80% of the dataset is allocated for training, while the rest is used for fine-tuning and testing. It is worth noting that the training phase is often performed offline, which makes prediction time even more important for developers.

In general, the above criteria can be used to select a number of suitable algorithms, but it is difficult to determine the best algorithm at the beginning. Therefore, it is preferable to follow an iterative approach to work. A set of potential algorithms can be selected from among the machine learning algorithms, and tested on the data by running them in parallel or serially, and then their performance is evaluated to select the most effective algorithm.

4. Main Principles in Image Security

4.1 Biplane

The image is basically made up of pixels and each pixel consists of 8 bits. That is, the total image consists of eight binary levels. In the encrypted image, according to the proposed method, it consists of data bits and the eighth bit is used as a key to encrypt the original image [26]. The image that the algorithm works on has a resolution of (256.256). As shown in Figure 2.

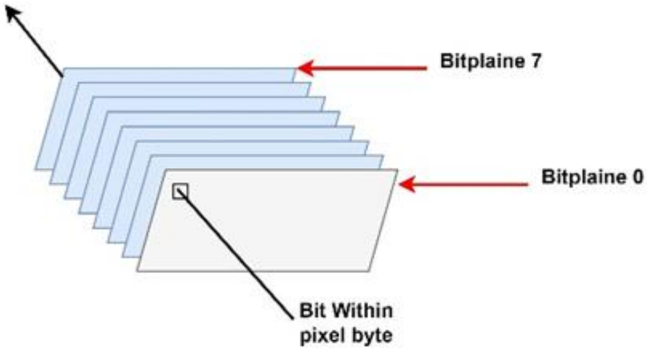


Figure 2: Bitplaine In Image Encryption

4.2 Histogram

The histogram of an image is a graph of the pixel values in the image. It represents the number of pixels with a certain intensity and their number in the image. In a grayscale image, which is basically made up of 8 bits, where a single pixel does not exceed 2^8, or 256, so the histogram displays

256 numbers that show the distribution of pixels at that frequency. One of the characteristics of good encryption is that the distribution of color intensity in the encrypted image is uniform, as we will see in the results section [27].

In the encrypted image, no description is provided in the histogram, especially if the encryption is strong and uniform in the vertices. Often, when detecting attacks, the image with equal borders in the histogram is very immune and cannot be decrypted in any way. In grayscale, the values are distributed according to the color gradient in the image, but in the encrypted one, they are not.

4.3 Correlation

One of the most important measures that can be relied upon in encryption is correlation, which symbolizes the strength of the relationship between a pixel and its surrounding pixels. The correlation between neighboring pixels is stronger than its distant counterparts, and they are said to be less correlated as there is a correlation coefficient that can be calculated for that. In the case of encryption, we manipulate the pixel correlations so that neighboring pixels are less correlated, and this is the process of hiding details in the image [28].

$$cor = \frac{cov(x,y)}{\sigma x \times \sigma y} \tag{1}$$

Such as : $\sigma x = \sqrt{var(x)}\ \ and\ \sigma y = \sqrt{var(y)}$ and *var* can be find as :

$$var(x) = \frac{1}{N}\sum_{i=1}^{N}(xi - E(x))^2 \tag{2}$$

$$cov(x,y) = \frac{i}{N}\sum_{i=1}^{N}(xi - E(x))(yi - E(y)) \tag{3}$$

Where *x,y* are the grey value of adjacent values, and *N* is the number of pixels in image.

4.4 Encryption Quality

Encryption quality refers to the total changes in pixel values or grayscale intensity between the original and encoded images [29]. Can be calculated as:

$$Q = \frac{\sum_{i=0}^{255}|HL(F) - HL(\acute{F})|}{256} \tag{4}$$

Where *L* consider as grey level, *HL(F)* number of pixels with grey level in original image and $HL(\acute{F})$ number of pixels with grey level in encrypted image

4.5 Key sensitivity

The sensitivity key is used to measure the amount of change that has occurred in the encrypted image. With this key, we can sense any small change, even 1 bit. The image *I* is entered into the program with the encryption key and the key *K*1 is used for encryption to get the image *C*1. The same image *I* is entered into the program but with a second key *K*2 that differs by one bit from the previous one to get the image *C*2. The difference is obtained from the difference between the two images [30].

5. Methodology

The process of securing data in images is done through encryption and there are three main processes to achieve this goal other than pre-processing and evaluation processes, which are: The first stage called diffusion involves the process of changing the pixel locations in the image, i.e. mixing the image components, in order to destroy the relationship between adjacent pixels. This process includes two secondary processes: key generation and mixing. The encryption key is generated using a Gaussian map with the help of the SVM classifier. The second process is diffusion, which aims to change the pixel values themselves and change randomly. The histogram in this case must be approximately uniform after encryption in order to resist interference with the data and erase any evidence of it.

In the diffusion process, a chaotic map is used with Gaussian noise added to it to create the diffusion key. In the first step, a random matrix is generated for diffusion with the size of the normal image, and then an XOR is performed between the diffusion matrix and the encrypted image.

First, the image is selected from the dataset. In the case of grayscale, the pixel is 8 bits, while in the case of color image, the bits are 24 bits for each primary color: red, green, and blue. In the form of three channels, as shown in the Figure 4.

In Confusion, a random key is generated to randomly change the pixel locations and make the image chaotic. Henon maps help in generating the random key and adding Gaussian noise to the random key, and to ensure more chaos, we use the famous SVM classifier to choose the best randomness and which is more complex. The idea of SVM is based on extracting features from the chaotic image and calculating the weights on the basis of which the image randomness is accepted. The classifier redistributes the complexities of the image segments and takes different dimensions, and thus through training it can predict the best random system, as shown in the Figure 5

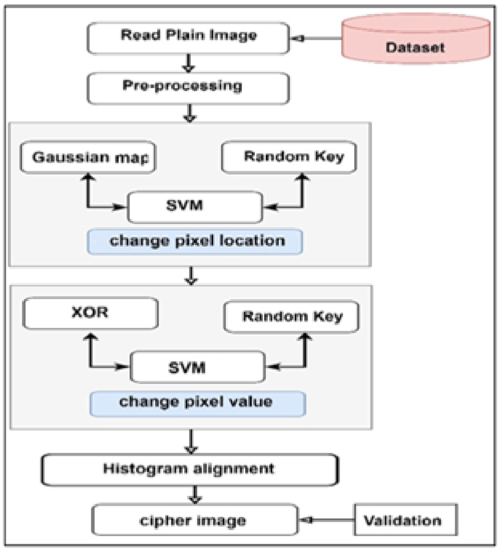
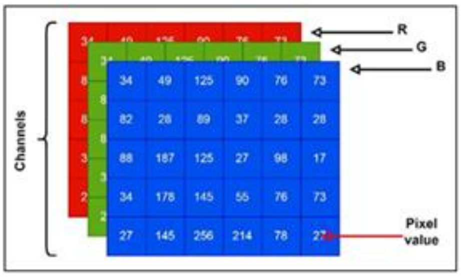


Figure 3: General Flowchart of Proposed Method



34	49	125	90	76	73
82	28	89	37	28	28
88	187	125	27	98	17
34	178	145	55	76	73
27	145	256	214	78	27

Figure 4: Three channels of color image

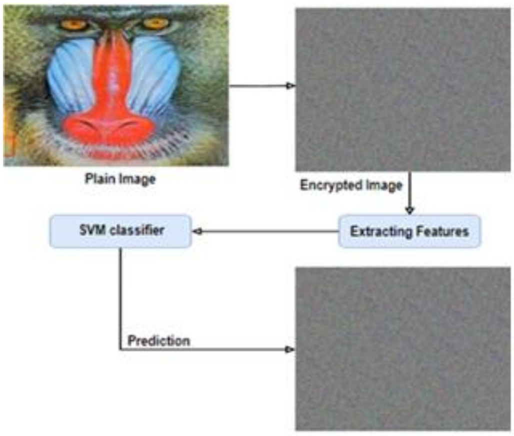


Figure 5: Confusion method

Diffusion is the second main process in encryption and its importance lies in erasing the image information completely by changing the places of the pixels in the same pixel. Its purpose in encryption is to unify the peaks of the histogram that indicates the exact information of the image. The numbers of the random matrix are in the form of numbers from 0 - 1 where 0 indicates a zero value for the pixel and 1 indicates a value of 255 and the resulting matrix is the diffusion part.

The main operation is to perform an XOR between the random key that has the same dimensions as the image and the image coming from the confusion process. In this case, the histogram is almost uniform because the entropy approaches 8, which means that it is difficult to detect the original image, especially when the result of the diffusion process is repeated more than once with the participation of SVM. The classifier repeats the addition process until the entropy reaches 8, meaning that the histogram is in the best uniform state. As shown in Figure 6.

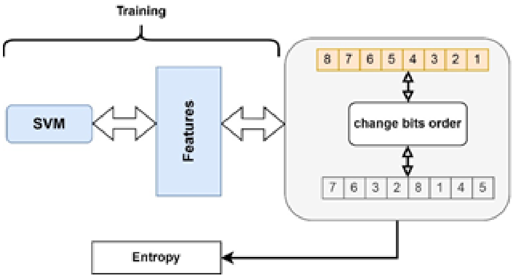


Figure 6: Diffusion process

When evaluating the proposed method in the results section, we will mention in detail the criteria that have an impact on the encryption strength and the relationship of the proposed method to increasing these results and the encryption strength.

6. Results and Discussion

6.1 Correlation and histogram

In this section, we will list the results and the effect of the proposed method on the result in image encryption. In the confusion part, the goal is to reduce the correlation to the minimum possible between the pixels in the image, and breaking the correlation is done by redistributing the pixels and distributing them in the image in a chaotic way. In the Figure 7, the histogram that indicates the correlation for the baboon image is shown.

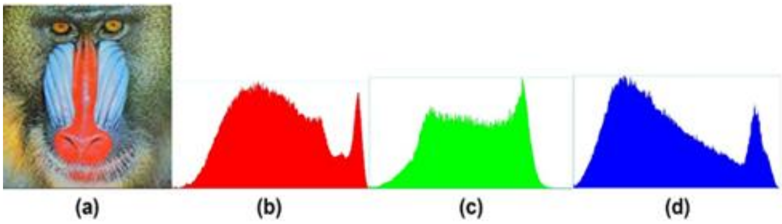


Figure 7: (a) plain image (b)(c)(d) histograms of RGB image

One of the most successful methods in attacks is the statistical method, and in order to resist this attack, the encryption method must be good. To ensure a good encryption method, the horizontal, vertical, and diagonal pixel correlation must be calculated in the plain and encrypted image, and the correlations are calculated according to the following equations.

$$Cor = \frac{cov\ (x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (5)$$

Such as : $D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - x')^2$ (6)

$$D(y) = \frac{1}{N}\sum_{i=1}^{N}(y_i - y')^2 \quad (7)$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - x')(y_i - y') \quad (8)$$

Where *(x,y)* is the pixel position and (x', y') is the next position. The confusion step reduces the correlation between adjacent pixels in the image as shown in the Table 2 while the entropy will not be affected due to the change in the pixel locations.

Table 2: illustrate the correlation of adjacent pixels in cipher image

			Correlation		
Images	Type	Image Size	Horizontal	Vertical	Diagonal
Taken 1	Color	512 x 512	-0.000569	0.00232	0.000910
Baboon	Color	256 x 256	0.001282	0.00182	0.003093
Lena	Gray	512 x 512	0.003469	0.00344	-0.000533
Man	Gray	256 x 256	-0.000971	0.00034	-0.00584
Elaine	Gray	256 x 256	-0.000775	-0.00956	0.000796
Barbara	Color	512 x 512	0.000788	0.00568	0.00374
Girl	Color	256 x 256	0.000982	-0.00457	0.00323
Taken 2	Color	512 x 512	0.000342	0.000239	-0.00765
Taken 3	Color	256 x 256	0.00892	0.000233	0.00066
Cameraman	Gray	512 x 512	-0.00026	-0.00098	-0.00261

The histogram shows the distribution of pixel intensity in the image. One of the specifications of a good encryption method is that the histogram should be uniform to reflect the impossibility of obtaining the encrypted information. After implementing the histogram method, the image will be as shown in the Figure 8, and the image will be of size 256×256 pixels.

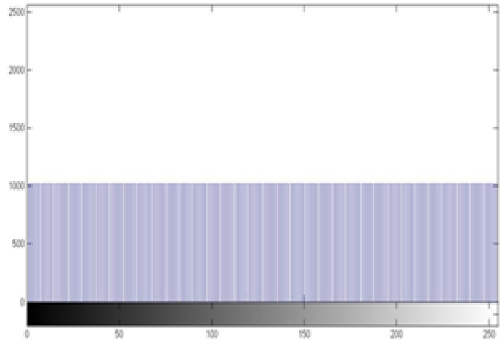


Figure 8: Histogram uniformed through proposed method of baboon image

Chaotic

Chaos is known to be a widespread phenomenon in most nonlinear systems and is highly sensitive and random in behavior. The logistic map is a quadratic boundary that has been used in cryptography due to its simple application and complex result and can be described in the equation.

$$X_{n+1} = r\mathrm{X_n}(1 - \mathrm{X_n}) \tag{9}$$

Consider *r* the control parameter such as $r \in (0,4)$ and *n=1,2,3,… . X1* represent initial condition (seed value) occur (0< X_1 <1). And the chaotic will be in value of (between 3.5699 and 4) as shown in Figure 9.

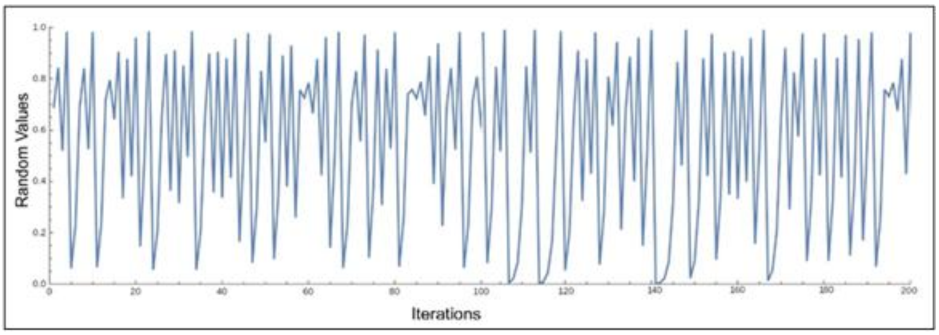


Figure 9: Lgistic map behaviour

In term of cobweb diagram easy can draw the chaotic logistic map as in Figure 10. The behavior in the form is based on the chaos in the encrypted image, which depends on the method used. The more chaos there is, the more impossible it is to decrypt without the encryption key. Image encryption is considered complex due to the limited dimensions of the image to be encrypted and thus the limited data. But when repeating the training process in SVM, we reach a stage where the chaos is almost impossible in order to transfer the image to the other party safely.

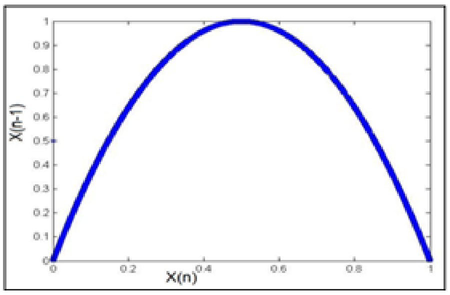


Figure 10: Cobweb behaviour of complex choatic

The main goal of this study is to design a high-level encryption system to ensure the security of image data. In order to achieve this goal, the statistical properties of the image, represented by the correlation, must be eliminated. Since the encryption goes through iterations during the SVM training process, the complexity can be increased by a good amount without losing the information in the image. Any process that includes training procedures achieves the highest desired result because the machine learning that simulates the best of what was entered as the final result is at a high level of accuracy, as shown in the Figure 11.

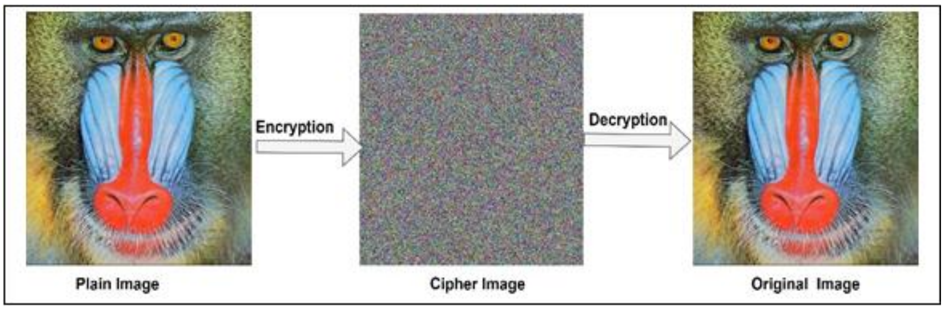


Figure 11: behaviour of choas in proposed method

Entropy

The change from the degree of certainty can be measured by entropy. Entropy is often defined as the degree of randomness or disorder of the system. Hence, entropy came as a standard to measure the degree of randomness in the encrypted image. In the case of the closeness of the red, green or blue color intensity, the entropy is close or most likely = 8, and even in the case of the gray image, when the intensity of the pixels is equal, the entropy = 8, so the entropy of the encrypted image is 8, and this is what the proposed method did, which relied on the number of training times to get the best result. Entropy can find by this equation:

$$H(m) = \sum_{i=0}^{M-1} P(m_i) \log_2 \frac{1}{P(m_i)} \tag{9}$$

Considering M is the total number of pixels, $P(m_i)$ is the possibility of occurrence symbol m_i in binary mode. Then the perfect of entropy in image encryption is 8. In Table 3 shows some encrypted images with their entropy.

Table 3: Entropy with the proposed system

Images	Type	Image Size	Entropy
Baboon	Gray	512 x 512	8
Lena	Color	256 x 256	8
Camera man	Gray	512 x 512	8
Jet	Gray	256 x 256	8
Taken 1	Color	256 x 256	8
Taken 2	Color	512 x 512	8

From here we know that the encryption system is important in securing data and also depends on the method used. The image from the dataset is encrypted and also produces a cipher image and is sent to the other party and at the other party it starts reversing the encryption method to form and return the original image as in the Figure 12.

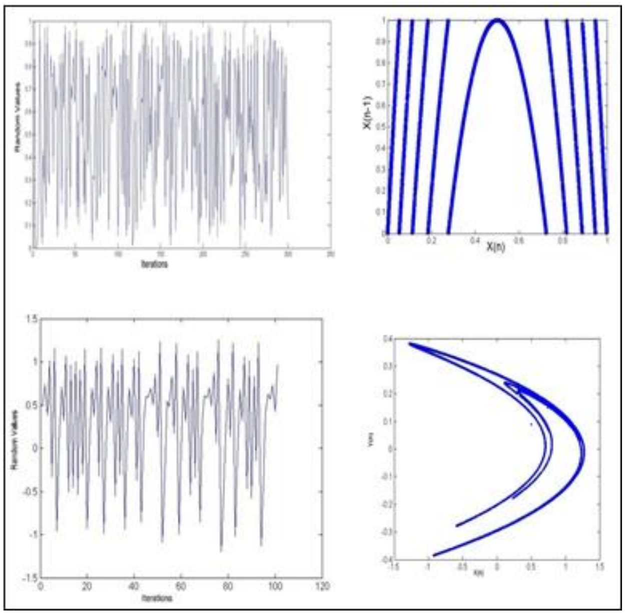


Figure 12: Encryption strategy

7. Conclusion

In this research, an improved Support Vector Machine (SVM) classifier is adopted to increase the security of digital images. Despite the protection provided by traditional methods, there are still challenges in increasing the security of images, especially with the increase in digital technology in our era. SVM addresses the process of increasing the complexity of chaos in image pixels with the help of features extracted from the first step of encryption and then calculating the weights that affect the result and the complexity of encryption and thus reaching the most complex random combination. The improved weight-based SVM showed superiority in resisting statistical attacks and detecting anomalies in image data.

DOI: https://dx.doi.org/10.70729/SE25112030014

There are significant and good improvements in the accuracy, entropy = 8, and uniformity of the histogram shape, which indicates the strength of the encryption. This indicates the potential of SVM in training to obtain the best complex encryption. The proposed method provides a reliable solution for image data protection, which can be used in various fields such as healthcare, economics, and social communication.

References

[1] Faragallah, O. S., Afifi, A., El-Shafai, W., El-Sayed, H. S., Naeem, E. A., Alzain, M. A., ... & Abd El-Samie, F. E. (2020). Investigation of chaotic image encryption in spatial and FrFT domains for cybersecurity applications. *IEEE Access*, *8*, 42491-42503.

[2] Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176-8186.

[3] Jacobs, A. S., Beltiukov, R., Willinger, W., Ferreira, R. A., Gupta, A., & Granville, L. Z. (2022, November). AI/ML for network security: The emperor has no clothes. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1537-1551).

[4] Kaur, M., & Kumar, V. (2020). A comprehensive review on image encryption techniques. *Archives of Computational Methods in Engineering*, *27*(1), 15-43.

[5] Arab, A., Rostami, M. J., & Ghavami, B. (2019). An image encryption method based on chaos system and AES algorithm. *The Journal of Supercomputing*, *75*, 6663-6682.

[6] Hua, Z., Zhou, Y., & Huang, H. (2019). Cosine-transform-based chaotic system for image encryption. *Information Sciences*, *480*, 403-419.

[7] Hazer, A., & Yıldırım, R. (2021). A review of single and multiple optical image encryption techniques. *Journal of Optics*, *23*(11), 113501.

[8] Khashan, O. A., & AlShaikh, M. (2020). Edge-based lightweight selective encryption scheme for digital medical images. *Multimedia Tools and Applications*, *79*(35), 26369-26388.

[9] Zhang, Y. (2020). The fast image encryption algorithm based on lifting scheme and chaos. *Information sciences*, *520*, 177-194.

[10] Lee, J. W., Kang, H., Lee, Y., Choi, W., Eom, J., Deryabin, M., ... & No, J. S. (2022). Privacy-preserving machine learning with fully homomorphic encryption for deep neural network. *iEEE Access*, *10*, 30039-30054.

[11] ALRikabi, H. T. S., & Hazim, H. T. (2021). Enhanced data security of communication system using combined encryption and steganography. *iJIM*, *15*(16), 145.

[12] Ding, Y., Wu, G., Chen, D., Zhang, N., Gong, L., Cao, M., & Qin, Z. (2020). DeepEDN: A deep-learning-based image encryption and decryption network for internet of medical things. *IEEE Internet of Things Journal*, *8*(3), 1504-1518.

[13] Kolivand, H., Hamood, S. F., Asadianfam, S., & Rahim, M. S. (2024). Image encryption techniques: A comprehensive review. *Multimedia Tools and Applications*.

[14] Huang, H., Wang, Y., & Zong, H. (2022). Support vector machine classification over encrypted data. *Applied Intelligence*, *52*(6), 5938-5948.

[15] Shahna, K. U., & Mohamed, A. (2020). A novel image encryption scheme using both pixel level and bit level permutation with chaotic map. *Applied Soft Computing*, *90*, 106162.

[16] Park, S., Byun, J., Lee, J., Cheon, J. H., & Lee, J. (2020). HE-friendly algorithm for privacy-preserving SVM training. *IEEE Access*, *8*, 57414-57425.

[17] Falih, M., Fadhil, A., Shakir, M., & Atiyah, B. T. (2024, March). Exploring the potential of deep learning in smart grid: Addressing power load prediction and system fault diagnosis challenges. In AIP Conference Proceedings (Vol. 3092, No. 1). AIP Publishing.

[18] Fadhil, A. M., Jalo, H. N., & Mohammad, O. F. (2023). Improved Security of a Deep Learning-Based Steganography System with Imperceptibility Preservation. International journal of electrical and computer engineering systems, 14(1), 73-81.

[19] Abed, N. K., Shahzad, A., & Mohammedali, A. (2023, October). An improve service quality of mobile banking using deep learning method for customer satisfaction. In AIP Conference Proceedings (Vol. 2746, No. 1). AIP Publishing.

[20] Ray, S. (2018). A comparative analysis and testing of supervised machine learning algorithms. International Journal of Advanced Computer Science and Applications, 10(12), 1-8.

[21] Mahesh, B. (2020). Machine learning algorithms-a review. International Journal of Science and Research (IJSR).[Internet], 9(1), 381-386.

[22] Obaido, G., Mienye, I. D., Egbelowo, O. F., Emmanuel, I. D., Ogunleye, A., Ogbuokiri, B., ... & Aruleba, K. (2024). Supervised machine learning in drug discovery and development: Algorithms, applications, challenges, and prospects. Machine Learning with Applications, 17, 100576.

[23] Alangari, S. (2024). An unsupervised machine learning algorithm for attack and anomaly detection in IoT Sensors. Wireless Personal Communications, 1-25.

[24] Mvula, P. K., Branco, P., Jourdan, G. V., & Viktor, H. L. (2024). A Survey on the Applications of Semi-supervised Learning to Cyber-security. ACM Computing Surveys, 56(10), 1-41.

[25] Tohidi, N., & Rustamov, R. B. (2020). A review of the machine learning in gis for megacities application. Geographic Information Systems in Geospatial Intelligence, 29-53.

[26] Song, W., Fu, C., Zheng, Y., Tie, M., Liu, J., & Chen, J. (2023). A parallel image encryption algorithm using intra bitplane scrambling. Mathematics and Computers in Simulation, 204, 71-88.

[27] Ye, H., Su, K., Cheng, X., & Huang, S. (2022). Research on reversible image steganography of encrypted image based on image interpolation and difference histogram shift. *IET Image Processing*, *16*(7), 1959-1972.

[28] Zou, C., Zhang, Q., Wei, X., & Liu, C. (2020). Image encryption based on improved Lorenz system. *IEEE Access*, *8*, 75728-75740.

[29] Hazer, A., & Yıldırım, R. (2021). A review of single and multiple optical image encryption techniques. *Journal of Optics*, *23*(11), 113501.

[30] Chen, C., Sun, K., & He, S. (2020). An improved image encryption algorithm with finite computing precision. *Signal Processing*, *168*, 107340.

Author Profile

Wafaa Ali was born in southern Iraq in 1980. She received her M.Sc. degree in Computer Science from the University of Thi-Qar in 2016. Currently, she works as a teacher in the Computer Science Department at the College of Education for Pure Sciences, University of Thi-Qar. Her research interests include artificial intelligence, data, and computer security."

Dr. Walaa Alajali was born in Iraq. She received her MCA degree in Computer Science with a specialization in AI from Jamia Millia Islamia, India, in 2011. She earned her PhD in Artificial Intelligence from Deakin University, Australia, in 2020. Currently, she works as a lecturer at the University of Thi-Qar, Iraq. Her research areas include smart transportation systems, smart agriculture systems, and AI applications in various fields."

Abdulrahman D. Alhusaynat was born in Iraq. He received his M.Sc. degree in Computer Science from Hamdard University, India, in 2011. Currently, he is a researcher in the field of networking.

DOI: https://dx.doi.org/10.70729/SE25112030014