ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

CLASSIFICATION OF ENCRYPTED IMAGES USING DEEP LEARNING –RESNET50

JAWAD YOUSEF IBRAHIM ALZAMILY[1], SYAIBA BALQISH ARIFFIN[2], SAMY S. ABU NASER[3]

[1,2]University Malaysia of Computer Science & Engineering (UNIMY), Cyberjaya, Malaysia.

[3]Faculty of Engineering and Information Technology, Al-Azhar University, Gaza, Palestine.

E-mail:[1]p05210004@student.unimy.edu.my, [2]syaiba.ariffin@unimy.edu.my, [3]abunaser@alazhar.edu.ps

ABSTRACT

Background: With the entry into the world of cloud computing, which has become an essential in our lives, especially after the pandemic of the era of COVID-19, and with the increase of overlapping data over the Internet and networks with an increasing and great speed, the need to protect those data and applications, especially as the usage of cloud computing, increases. **Objectives**: Searching for the best solutions to provide the necessary protection against data attacks via cloud computing, so the need has become more urgent to access huge storage resources and applications with ease and process them anywhere with flexibility and more security. **Methods**: In this paper, a large group of images has been encoded using one of the encryption algorithms, then we used the Convolutional Neural Network (CNN) algorithm, which is a widely applied deep learning technique for image recognition. There is no doubt that deep learning has many models that contribute to increasing the speed and accuracy in the appearance of the results, including the ResNet50 model, where we took the model by training many encrypted images. Through this model, it was able to classify and identify the encrypted images without decoding them. **Results**: It was found that the classification of encoded images using the deep learning technique of the ResNet50 model has the potential to identify the encrypted image without decoding it. The proposed model achieved accuracy (99.75%), Recall (94.12%), Precision (94.23%) and F1-score (94.70%) on the test dataset, which indicates the feasibility of this approach in classifying encoded images.

Keywords: *Deep learning, Cryptographic algorithms, Image Encryption, Encryption, ResNet50 model, Artificial Intelligence*

1. INTRODUCTION

Image encryption can be defined in such a way that it is the procedure of encoding secret image with the help of some encryption algorithm in such a way that unauthorized users can't access it. The primary purpose of encryption is to protect the confidentiality of digital data stored on computer systems or transmitted over the internet or any other computer network. Providing such security and privacy to the user, image encryption is very important to protect from any unauthorized user access. Image and video encryption have applications in various fields including internet communication, multimedia systems, medical imaging, Tele-medicine and military communication.

The conversion of encrypted data into its original form is called decryption. It is generally a reverse process of encryption. It decodes the encrypted information so that an authorized user can only decrypt the data because decryption requires a secret key or password.

The topic of this paper is the classification of encrypted images using deep learning technology with the ResNet50 model, thus it aims to analyze and identify the encrypted image without decrypting it. Although this test evaluates one of the encryption algorithms for these images, the general methodology can be applied to a variety of algorithms, due to the success of these models with deep learning techniques. With the integration of cryptography with artificial intelligence science, activities have become shorter, smaller and easier to deal with data or images on a large scale.

This type of a system is a novel one because as far as the authors are aware no one worked on multi label classification with encrypted images.

1.1 Artificial Intelligence and Deep learning

Artificial intelligence (AI) can be better defined as a set of tools and techniques that aim to converge aspects of human or animal cognition using machines as defined by researchers [1]-[4] Calo and Kurzweil discussed artificial intelligence that the computer is the computational package of the ability to perceive goals in the world, so it is considered the engineering and science of making intelligent machines, especially if they are related to similar tasks in the use of computers and their programs to understand human intelligence, where the degrees and types of intelligence in humans vary. Some machines and many animals.

But there are some authors who have another definition of deep learning which refers to layers based on multiple hidden deep networks, with multiple levels to learn various benefits of abstraction, which is a new field of machine learning that has achieved great popularity in recent years. In order to investigate good representations, most deep learning algorithms seek to invest the unknown structure in classifying the inputs at multiple levels, with some higher-level acquired features defined by lower-level features [5].

Where deep learning enters into many industries and different tasks, including open-source systems with consumer recommendation applications and also enters into commercial applications that are used in image recognition and also used in medical research to a large extent in the possibility of discovering many diseases by deep learning and the use of drugs for those diseases Those are some examples of integrating deep learning.

1.2 Convolutional Neural Network

The name "Convolutional Neural Network" refers to a network of neural networks that uses convolution rather than general matrix multiplication in at least one of its layers, and is also used in arithmetic operations, and convolution is a specialized type of linear operation that is widely used in deep learning (Figure 1 is an example of CNN architecture) [6].

In the traditional approach to programming, we put data and input into the computer and what it has to do, and the computer breaks down big problems into many well-defined and small tasks, which the computer can do with ease, unlike neural networks, if several problems arise, we don't tell the computer how to solve its problems, but rather, it learns from the monitoring data, and discovers its own solution to the problem presented to it. Therefore, neural networks are considered one of the most beautiful programming models ever [7].

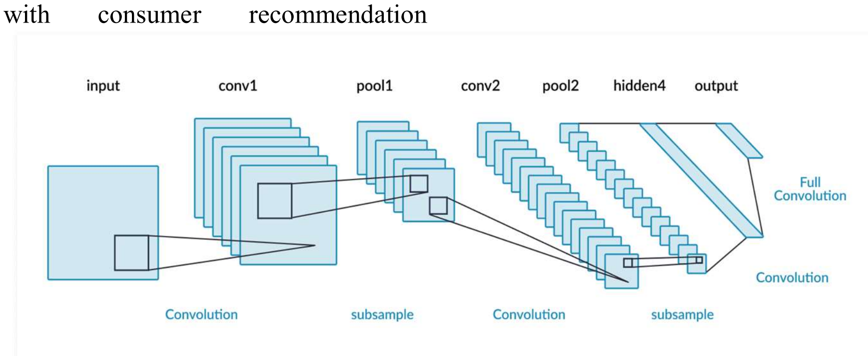


Figure 1. Architecture of Convolutional Neural Network

1.3 Network Architectures (ResNet50)

ResNet-50 is a neural network used primarily in many computer vision tasks and is a convolutional neural network with a depth of 50 layers. ResNet, short for Residual Networks, is sometimes called a classic neural network. It is an innovative neural network that was first in a 2015 computer vision research paper titled Residual Deep Learning for Image Recognition. Previously, a major breakthrough with ResNet was that it allowed us to train deep neural networks extremely with more than 150 layers [8].

Convolutional Neural Networks have a major disadvantage — 'Vanishing Gradient

Problem'. During backpropagation, the value of gradient decreases significantly, thus hardly any change comes to weights. To overcome this, ResNet is used. It makes use of "SKIP CONNECTION". The original ResNet50 architecture is shown in Figure 2 and the modified architecture is shown in Figure 3.

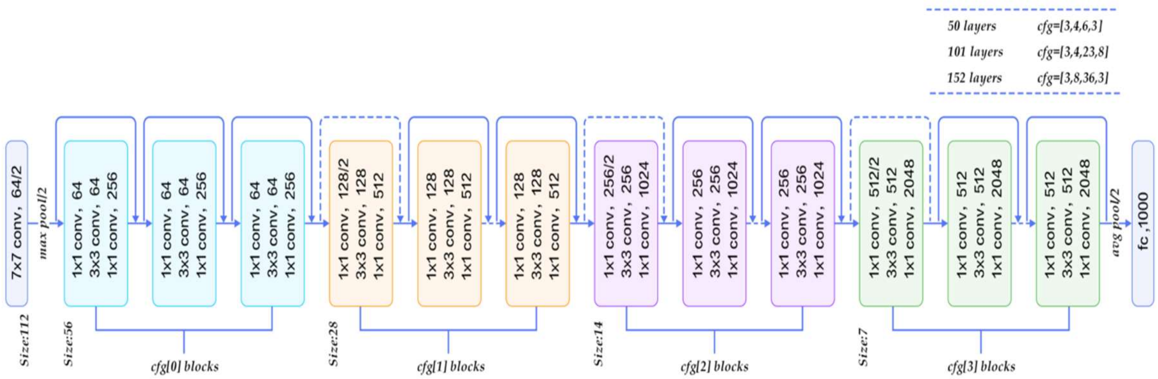


Figure 2. The original ResNet50 architecture

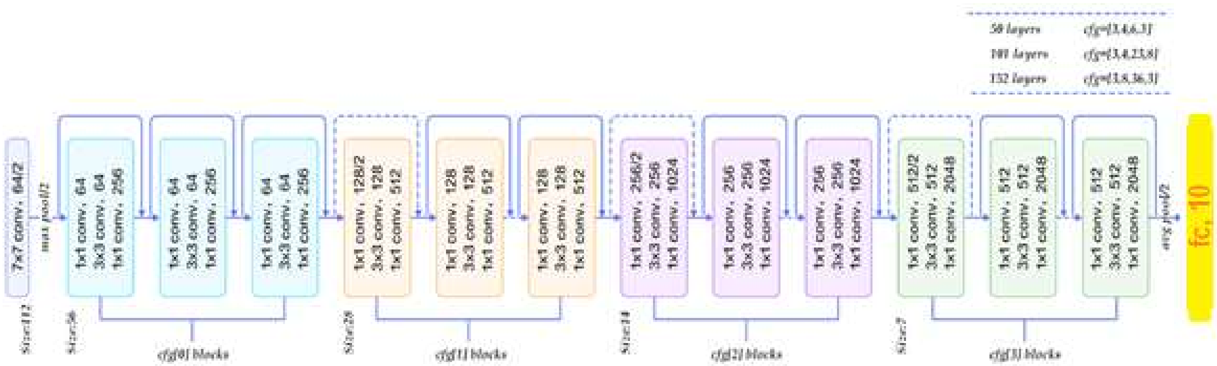


Figure 3. The modified ResNet50 architecture

1.4 Cryptographic and Image Encryption Algorithms

There is an inherent view of the authors that: Encryption is a method of sending data or a message to a single entity that holds a secret key, which is who can access the concept of the data or message and also from the other perspective, encryption is access to encrypted data so that one learns nothing at all about the text Other than its normal length, one can decode oneself to read the entire plaintext [9] , In general, some of them said that it is an encryption process, and it is among the processes that provide confidentiality for sensitive data or information. As for decryption, it is the reverse process of encryption [10].

Image encryption is one of the well-known mechanisms for maintaining the confidentiality of images across trusted, unrestricted public media. This medium is vulnerable to attacks, thus effective encryption algorithms are essential for secure data transmission. Various techniques have been proposed in the literature so far, each with an advantage over the other, to keep pace with the growing need for security [11]. Here are more comparisons between the most popular encryption algorithms that the authors have written in their research papers to date and the most famous ones.

2. PROBLEM STATEMENT"

In recent years, privacy preservation has become a significant issue in order to protect private images not to be revealed during querying by the organizations. For example, many private images such as trip photos, family photos, etc. can be stored in the cloud in order to be easily shared to authenticated users. However, personal information (such as appearance, gender, etc.) and family information (members and relationships of the family) may be easily revealed to the unauthorized entities. Hence, privacy preservation scheme such as encryption is applied to the cloud that however incurs a significant slowdown on the retrieval efficiency.

From this perspective, an efficient image retrieval system is necessary to work on the encrypted database because decrypting and then querying from millions of encrypted photos consumes huge amounts of computation, especially in huge databases."

In this study, we are proposing to train a model using the dataset to help users to develop an efficient image retrieval system that preserves information privacy, and in order to be able to classify the images and define their algorithm directly without decoding them. Computerized applications can use deep learning techniques to increase accuracy and efficiency in classification.

3. OBJECTIVES

3.1 Main objective

Implementation a software model used to discover and classify encryption algorithms by classifying encoded images on popular handwritten digits of the following types: (0, 1, 2, 3 , 4 , 5 , 6 , 7 , 8 , 9) . Among the encryption algorithms used to encode images on popular handwritten digits are (AES).

3.2 Specific objectives:

- Efficiency: efficient and effective retrieval of the queried images from the huge encrypted image dataset and upsurge the aptitude using deep learning methods to identify encrypted images.
- Data privacy: preservation of private information on all images.
- Reduce the cost of diagnosis and repetitive images.

4. RELATED WORK

At a glance, using neural networks to break cryptographic algorithms has the theoretical qualifications to be successful; however, there have been few attempts to put it to the test. There are only a handful of papers that do the same thing. In one of these papers, "Barbosa uses encrypted text files in order to identify their encoding algorithm. Plain texts were encoded with distinct cryptographic algorithms and then some metadata were extracted from these codifications. It was through texts in Portuguese, English and Spanish were encrypted using DES, Blowfish, RSA, and RC4 algorithms. The encrypted files were submitted to data mining techniques such as J48, FT, PART, Complement Naive Bayes, and Multilayer Perceptron classifiers." Despite this, he was able to obtain the identification of the algorithm using data mining techniques [12].

Through the research paper [13]" the authors talked about Cryptographic Algorithm Identification Using Deep Learning Techniques. It was through a different parsing of encrypted text files, where they applied modern deep learning classification methods and compared them with existing machine learning methods , thus leading to an increasing the chances of a successful full/partial plain text recovery . It was through a generated cipher text corpus encrypted with AES and Blowfish algorithm for multilingual dataset that contains 700 files with an average of 4000 characters per file. From their research, they were able to determine the encryption algorithm through ciphertexts using deep learning technology."

One of the proposed techniques in [14]" for Encrypted image classification based on multilayer extreme learning machine, they proposed an encrypted image classification framework based on multi-layer extreme learning machine that is able to directly classify encrypted images without decryption. Experiments were conducted on popular handwritten digits and letters databases and achieved accuracy of 90.44 and 79.83% on MNIST, respectively encrypted under DES and AES. Results demonstrate that the proposed framework is secure, efficient and accurate for classifying encrypted images but it is a binary system and unable to define encryption algorithms.``

Another technique in [15] "for encrypted image classification is "Deep Neural Networks over Encrypted Data ", where they developed a new technique to adopt deep neural networks within the practical limitation of current homomorphic encryption schemes. More specifically, they focus on classification of the well-known convolutional neural networks (CNN). They designed methods for approximation of the activation functions commonly used in CNNs (i.e. ReLU, Sigmoid, and Tanh) with low degree polynomials which is essential for efficient homomorphic encryption schemes. Then, they trained convolutional neural networks with the approximation polynomials instead of original activation functions and analyzed the performance of the models. Finally, these results show that CryptoDL provides efficient, accurate and scalable privacy-preserving predictions."

One of the technique in [16] for identification and Classification of Encryption Algorithms is "Deep Learning Based Cryptographic Primitive Classification" where they managed "CryptoKnight is successfully able to classify the sample algorithms with minimal loss. Via the model blueprint, a Dynamic Convolutional Neural Network (DCNN), is fittingly configured to learn from variable-length control flow diagnostics output from a dynamic trace. To rival the size and variability of contemporary data compendiums. The library CryptoKnight, rendered an algorithmic pool of AES, RC4, Blowfish, MD5 and RSA to synthesis combinable variants which are automatically fed in its core model."

One of the techniques in [17] for identification and Classification of Encryption Algorithms are also Encryption Scheme Classification: A Deep Learning Approach "where this research was able to use of recent advancement in machine learning algorithms specifically deep learning algorithms to classify encryption schemes based on entropy measurements of encrypted data with no feature engineering. By applying standard encryption algorithms Data Encryption Standard (DES) and Advanced Encryption Standard (AES) with block cipher modes namely Electronic Codebook (ECB) and Cipher Block Chaining (CBC) over the image dataset from CIFAR10. Two ImageNet winning Convolutional Neural Network deep learning models namely AlexNet and GoogleNet are used to perform the classification. Transfer learning and layer modification were applied to evaluate the classification effectiveness. "

4.1 Comment on the previous Studies

Commenting on the previous studies: It was mentioned in one of the studies that it was done Cryptographic Algorithm Identification Using Deep Learning Techniques. It was through a different parsing of encrypted text files. It was through a generated cipher text corpus encrypted with AES and Blowfish algorithm for multilingual dataset that contains 700 files with an average of 4000 characters per file. From their research, they were able to determine the encryption algorithm through ciphertexts using deep learning technology but unable to identify and classify encryption algorithms used in the images [19]-[22].

"Also, as mentioned in one of the previous studies it was done extracting information from encrypted data using Deep Neural Networks, where it explored various approaches to using deep neural networks to perform cryptanalysis. We find that although the network is unable to decipher encrypted data, it is able to perform classification on encrypted data.

The researchers also mentioned that they had used encrypted text files in order to identify their encoding algorithm. Plain texts were encoded with distinct cryptographic algorithms using DES, Blowfish, RSA, and RC4 algorithms and then some metadata were extracted from these codifications and the encrypted files were submitted to data mining techniques such as J48, FT, PART, Complement Naive Bayes, and Multilayer Perceptron classifiers. Through which they were able to identify the algorithm using data mining techniques [23]-[26].

In the last research it depends on the framework which is based on ML-ELM that is capable of extracting higher order features from the encrypted images for classification directly. Through experiments, their proposed framework based on ML-ELM achieves accuracy of 90.44 and 79.83% on MNIST, respectively encrypted under DES and AES [27]-[30]. These accuracies are almost identical to those obtained by traditional time-consuming methods.

Finally, we see that the proposed methods provide accurate and effective segmentation and identification and classification results.

In addition, for the current cloud database containing trillions of encrypted images, an efficient retrieval system providing data privacy is required. Under this motivation, system performance can be improved by proposed for identification and classification of encryption algorithms framework fulfilling this requirement which works directly on the encrypted images, i.e., does not require decryption of images for classification and identification provides an image retrieval system that works directly on encrypted database using multiclass [31]-[33]. "

In the current study, we used a deep learning pre-trained model called ResNet50 with 50 convolutional layers followed by a fully connected hidden layer for detection and classification of encrypted images.

5. METHODOLOGY

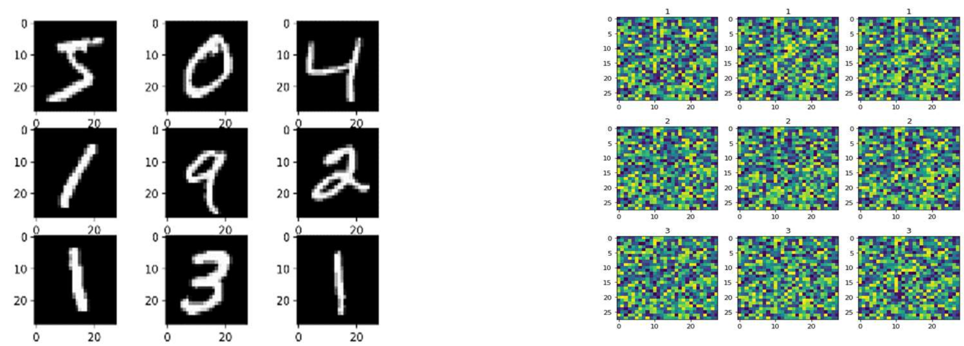
5.1 Dataset

The dataset in this study consists of a collection of 70,000 images of popular handwritten Arabic numeral digits.

When creating properly encrypted databases we need two steps: encryption and conversion, in the first step the encryption where the entire databases are encrypted by common AES encryption algorithms and a sample of encrypted and unencrypted images based on MNIST are shown as in Figure 3. Whereas, the original MNIST contains a training set of 60,000 images and a test set of 10,000 images that are appropriately divided equally with the images as shown in table 1.

Table 1. Split of the Dataset

Label	0	1	2	3	4	5	6	7	8	9	Total
Number of Images for Training	6000	6000	6000	6000	6000	6000	6000	6000	6000	6000	60,000
Number Images for Testing	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	10,000
Total	7000	7000	7000	7000	7000	7000	7000	7000	7000	7000	70,000



A B

Figure 3. A: Original MNIST, B: encrypted using AES

Journal of Theoretical and Applied Information Technology
15th November 2022. Vol.100. No 21

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

5.2 Building network using ResNet50

The training data set (60,000) images were divided into training (50,000) and validation (10,000). Thus, we have 50,000 training images, 10,000 validation images, and 10,000 test images. In each of the sections there are the same number of samples from each category, and this is a problem of a balanced multi-classification, which indicates that the accuracy of the classification will be a measure of success or loss, our conv_base will be a stack of alternate conv_base (with relu activated) and (Flatten Layers).

However, we are facing a big challenge especially since we are dealing with images and it is a more complex problem, so we will make our network bigger and it will have another switching base, in this way we will reduce the size of the feature maps further and increase the capacity of the network, and from here we will start from the input size of 150 x 150 (slightly random selection) until we end up with 7 x 7 feature maps just before the Flatten layer, so they aren't too big when we get to the Flatten layer.

One of the model problems is the multi-classification problem, so we terminate the network with only one unit (dense layer of size 10) and the softmax activation function[34]-[36], and because of that we encode the units until the network looks at one or the other, see the summary of Figure 4 for ResNet50 model.

Layer (type)	Output Shape	Param #
Resenet50 (Functional)	(None, 1, 1, 2048)	23587712
Flatten_1	(None, 2048)	0
Dense_2 (Dense)	(None, 2048)	1049088
Dense_3 (Dense)	(None, 2048)	5130

Total params: 24,641,930
Trainable params: 24,588,810
Non-trainable params: 53.120

Figure 4. ResNet50 Model Summary.

5.3 Data Pre-processing

Image size is a problem in training deep learning and its dependent models as the first thing that is used in data pre-processing is to change the size of the images, due to the presence of images of different sizes, and this the size of the images goes against the balance between providing high enough accuracy to classify the images encoded by the model and effective training, the images were resized to 75 × 75 pixels, and all images were normalized to ImageNet standards. So, the steps to enter it into our network are:

- Read all existing image files.
- RBG pixel grids we converted them by decoding JPEG content.
- The floating-point tensor is completely transformed.
- Interval [0, 1] we converted the images pixel values (between 0 and 255) to [0..1].

It might sound a bit tricky, but Keras has some utilities to take care of those steps automatically, inside are a few image processing modules and utilities, located in "keras.preprocessing.image". In particular, it also contains an ImageDataGenerator class that allows setting up on-disk Python generators that automatically convert image files into sets of pre-processed integers.

5.4 Evaluation Metrics

In this study, we used three evaluation metrics to evaluate the performance of the proposed classification model: accuracy, recall, precision, and F1-score. They are defined in the equations (1), (2), (3) and (4) respectively. The calculations are made based on the statistical results of multiple experiments.

$$Precision = \frac{TP}{TP+FP} \quad (1)$$

$$Recall = \frac{TP}{TP+FN} \quad (2)$$

$$Accuracy = \frac{TP+TN}{TP+FP+FN+TN} \quad (3)$$

$$F1 - Score = \frac{2*Precision*Recall}{Precision+Recall} \quad (4)$$

Where TP, FP, TN and FN are true positive, false positive, true negative and false negative, respectively [10].

6. EXPERIMENTS AND DISCUSSIONS

After we trained and tested the model, we noticed that the accuracy value of 'val_acc' started to increase. This means that the model works correctly and is built for better learning, as the training accuracy reached 99.36%, the validation accuracy was 94.94% and the testing accuracy 94.23% (as shown in Table 2 and Figure 5 and Figure 6).

Table 2. Accuracy And Loss Of Training, Validation And Testing

Type	Accuracy	Loss
Training	99.36%	0.0189
Validation	94.94%	0.2301
Testing	94.23%	0.2011

A comparison was made with the methods used in the literature and the results of the current study in terms of the evaluation metrics accuracy, Sensitivity, and Specificity.

The results obtained from the current proposed method were much better than the methods that were used in the literature as can be seen in Table 3.

Table 3. Comparison with Other Methods Proposed In the Literatures

Method	**No. of Classes**	**Accuracy**	**Recall**	**Precision**	**F1-score**
Weiru Wang et al. [8]	10	92.60%	91.40%	91.65%	92.58%
Ehsan Hesamifard et al. [9]	10	93.30%	92.90%	92.80%	93.23%
Gregory et al. [10]	10	91.91%	91.14%	92.82%	91.90%
Pan [11]	10	92.41%	92.34%	92.52%	92.40%
Algorithm of this study	10	94.75%	94.12%	94.23%	94.70%

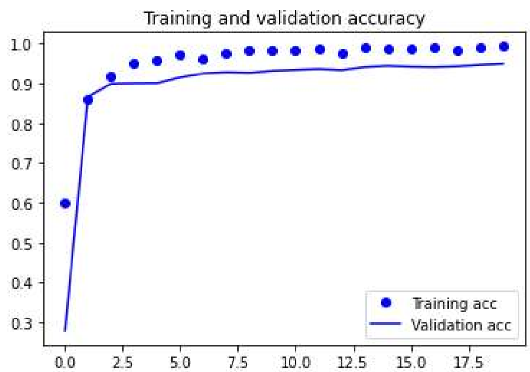


Figure 5. Training And Validation Accuracy Curve Of Resnet50.

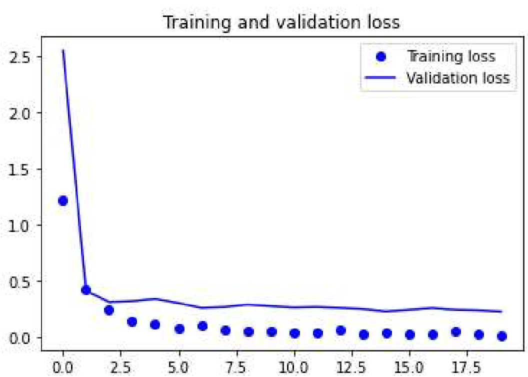


Figure 6. Training And Validation Loss Curve Of Resnet50.

7. CONCLUSION

In this study, a large group of images has been encoded using one of the encryption algorithms (ASE), then we used the Convolutional Neural Network, which is a widely applied deep learning technique for image recognition. There is no doubt that deep learning has many models that contribute to increasing the speed and accuracy in the results, including the ResNet50 model, where we trained the model using 70,000 encrypted MINST images. This model was able to classify and identify the encrypted images without decoding them. It was found that the classification of the encoded images using the deep learning technique of the ResNet50 model has the potential to know the encrypted image without decoding it.

The proposed model achieved accuracy (99.75%), Recall (94.12%), Precision (94.23%) and F1-score (94.70%) on the test dataset, which indicates the feasibility of this approach in classifying encoded images.

The more images we have, we think the results will be much better and there will be better accuracy with other models in deep learning.

In terms of the objectives outlined, our study achieved all of them by creating a deep learning model that can identify encrypted images with decrypting them successfully.

8. FUTURE WORKS AND LIMITATION

For future work: we can try different techniques for feature selection and analysis. We can experiment with hyper parameters for the different machine learning algorithms. Furthermore, we can use Ensemble techniques that use a group of machine learning algorithms and combine them according to some methodology (like Voting) to get better accuracy results. Furthermore, we will try different encoding encryption algorithms like Blowfish, DES and RSA.

Author Contribution Statement

The authors confirm contribution to the paper as follows: study conception and design: JYA, SBA, SSA; data collection: JYA, SBA, SSA; analysis and interpretation of results: JYA. Author; draft manuscript preparation: JYA, SSA, SBA. All authors reviewed the results and approved the final version of the manuscript.

REFERENCES:

[1] Abunasser, B. S., et al., "Breast Cancer Detection and Classification using Deep Learning Xception Algorithm" International Journal of Advanced Computer Science and Applications(IJACSA), vol. 13, no. 7, pp. 223-228, 2022. http://dx.doi.org/10.14569/IJACSA.2022.0130729

[2] Obaid, T., et al. "Factors Contributing to an Effective E- Government Adoption in Palestine" Lecture Notes on Data Engineering and Communications Technologies, 127, pp. 663–676, 2022

[3] Abunasser, B. S., et al., "Prediction of Instructor Performance using Machine and Deep Learning Techniques" International Journal of Advanced Computer Science and Applications(IJACSA), vol. 13, no. 7, pp. 78-

83, 2022. http://dx.doi.org/10.14569/IJACSA.2022.0130711
[4] Saleh, A., et al. "Brain tumor classification using deep learning" Proceedings - 2020 International Conference on Assistive and Rehabilitation Technologies, iCareTech 2020, 2020, pp. 131–136, 9328072
[5] Arqawi, S., et al. "Integration of the dimensions of computerized health information systems and their role in improving administrative performance in Al-Shifa medical complex" Journal of Theoretical and Applied Information Technology, vol. 98, no. 6, pp. 1087–1119, 2020.
[6] Elzamly, A., et al. "Assessment risks for managing software planning processes in information technology systems" International Journal of Advanced Science and Technology, vol. 28, no. 1, pp. 327–338, 2019.
[7] Albatish, I.M., et al. Modeling and controlling smart traffic light system using a rule based system. Proceedings - 2019 International Conference on Promising Electronic Technologies, ICPET 2019, pp. 55–60, 2019, 8925318
[8] Weiru Wang, Chi-Man Vong, Yilong Yang, Pak-Kin Wong. Encrypted image classification based on multilayer extreme learning machine. Multidim Syst Sign Process, 2017, 28, pp. 851–865.
[9] Ehsan Hesamifard, Hassan Takabiy, and Mehdi Ghasemiz. "CryptoDL: Deep Neural Networks over Encrypted Data" , arXiv:1711.05189, 2017.
[10] Gregory D. Hill, Xavier J. A. Bellekens. "Deep Learning Based Cryptographic Primitive Classification " . arXiv:1709.08385v1, 2017.
[11] Pan, J. "Encryption scheme classification: a deep learning approach". International Journal of Electronic Security and Digital Forensics, 9(4), 2017.
[12] Elzamly, A., et al. "A new conceptual framework modelling for cloud computing risk management in banking organizations" International Journal of Grid and Distributed Computing, vol. 9, no. 9, pp. 137–154, 2016.
[13] Mady, S.A., et al. "Lean manufacturing dimensions and its relationship in promoting the improvement of production processes in industrial companies" International Journal on Emerging Technologies, vol. 11, no. 3, pp. 881–896, 2020,
[14] Abu Ghosh, M.M., et al. "Secure mobile cloud computing for sensitive data: Teacher services for Palestinian higher education institutions" International Journal of Grid and Distributed Computing, vol. 9, no. 2, pp. 17–22, 2016.
[15] Gulshan, V., & Peng, L. et al. Development and Validation of a Deep Learning Algorithm for Detection of Diabetic Retinopathy in Retinal Fundus Photographs. JAMA, vol. 316, no. 22, pp. 2402-2420, 2016.
[16] Buhisi, N. I., et al. "Dynamic programming as a tool of decision supporting" Journal of Applied Sciences Research, vol. 5, no. 6, pp. 671-676, 2009.
[17] Russakovsky, O., & Deng, J. et al. ImageNet Large Scale Visual Recognition Challenge. International Journal of Computer Vision, vol. 115, no. 3, pp. 211–252, 2015.
[18] Naser, S. S. A. "Developing an intelligent tutoring system for students learning to program in C++" Information Technology Journal, vol. 7, no. 7, pp. 1051-1060, 2008.
[19] Moreno-García, Carlos, et al. Assessing the clinicians pathway to embed artificial intelligence for assisted diagnostics of fracture detection. CEUR Workshop Proceedings, 2020.
[20] Naser, S. S. A. "Developing visualization tool for teaching AI searching algorithms" Information Technology Journal, vol. 7, no. 2, pp. 350-355, 2008.
[21] Bar, Y., & Diamant, I. et al. Chest pathology detection using deep learning with non-medical training. 2015 IEEE 12th International Symposium on Biomedical Imaging (ISBI), pp. 294–297, 2015.
[22] Fawzy A., et al. "Mechanical Reconfigurable Microstrip Antenna" International Journal of Microwave and Optical Technology, vol. 11, no. 3, pp.153-160, 2016.
[23] CERNAZANU-GLAVAN, C., & HOLBAN, S. Segmentation of Bone Structure in X-ray Images using Convolutional Neural Network. Advances in Electrical and Computer Engineering, vol. 13, no. 1, pp. 87–94, 2013.
[24] Naser, S. S. A. "Intelligent tutoring system for teaching database to sophomore students in Gaza and its effect on their performance" Information Technology Journal, vol. 5, no. 5, pp. 916-922, 2006.

[25] Sitaula, C., & Hossain, M. B. Attention-based VGG-16 model for COVID-19 chest X-ray image classification. Applied Intelligence, vol. 51, no. 5, pp. 2850-2863, 2021.
[26] Esteva, A., Kuprel, B. et al. Dermatologist-level classification of skin cancer with deep neural networks. Nature, vol. 542, no. 7639, pp. 115–118, 2017.
[27] Moran, M. B. H., & Faria, M. et al. On using convolutional neural networks to classify periodontal bone destruction in periapical radiographs. 2020 IEEE International Conference on Bioinformatics and Biomedicine (BIBM), pp. 2036–2039, 2020.
[28] El-Saadawy, H., & Tantawi, M. et al. A Two-Stage Method for Bone X-Rays Abnormality Detection Using MobileNet Network. Advances in Intelligent Systems and Computing, pp. 372–380, 2020.
[29] Ananthu, K. S., & Krishna Prasad, P. et al. Acute Lymphoblastic Leukemia Detection Using Transfer Learning Techniques. Intelligent Sustainable Systems, pp. 679–692, 2021.
[30] Naser, S. S. A. "JEE-Tutor: An intelligent tutoring system for java expressions evaluation" Information Technology Journal, vol. 7, no. 3, pp. 528-532, 2008.
[31] Wang, S., & Dong, L. Classification of pathological types of lung cancer from CT images by deep residual neural networks with transfer learning strategy. Open Medicine, vol. 15, no. 1, pp. 190–197, 2020.
[32] Dhungel, N., Carneiro, G., & Bradley, A. P. Fully automated classification of mammograms using deep residual neural networks. 2017 IEEE 14th International Symposium on Biomedical Imaging (ISBI 2017), pp. 310–314, 2017.
[33] Abu-Naser, S.S., et al. "An expert system for endocrine diagnosis and treatments using JESS" Journal of Artificial Intelligence, vol. 3, no .4, pp. 239-251, 2010.
[34] Moran, M., & Faria, M. et al. Classification of Approximal Caries in Bitewing Radiographs Using Convolutional Neural Networks. Sensors, vol. 21, no. 15, pp. 5192-5199, 2021.
[35] Abu Naser, S.S. "Evaluating the effectiveness of the CPP-Tutor, an intelligent tutoring system for students learning to program in C++" Journal of Applied Sciences Research, vol. 5, no. 1, pp. 109-114, 2009.
[36] Ding, Y., & Sohn, J. H. et al. A Deep Learning Model to Predict a Diagnosis of Alzheimer Disease by Using 18F-FDG PET of the Brain. Radiology, vol. 290, no. 2, pp. 456–464., 2019.