Liu *et al. J Wireless Com Network* (2022) 2022:21
https://doi.org/10.1186/s13638-022-02111-9

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Application of machine learning in intelligent encryption for digital information of real-time image text under big data

Liang Liu[1], Melody Gao[2], Yong Zhang[3*] and Yuxiang Wang[4]

*Correspondence:
zhangy1123@163.com
[3] School of Electrical Information, Changchun Guanghua University, Changchun 130033, China
Full list of author information is available at the end of the article

Abstract

In the context of big data, the exploration of the application effect of machine learning in intelligent encryption for real-time image text digital information aims to improve the privacy information security of people. Aiming at the problem of digital information leakage of real-time image text, the convolutional neural network is introduced and improved by adding a preprocessing module to form AlexNet, to encrypt the digital information of real-time image text. Besides, to take into account both the security effect and the real-time performance of the system, the image text is encrypted by the chaotic sequence generated by a one-dimensional chaotic system called Logistic-Sine and a multi-dimensional chaotic system named Lorenz. In this way, a real-time image text encryption model is constructed by combining the chaotic function and AlexNet. Finally, a simulation experiment is performed to analyze the performance of this model. The comparative analysis indicates that the recognition accuracy of feature extraction of image text by the intelligent encryption model reaches 94.37%, which is at least 3.05% higher than that of other neural network models by scholars in related fields. In the security analysis of image text encryption, the information entropy of pixel values at (0, 0) of the proposed model is close to the ideal value 8. Meanwhile, the value of the number of pixels change rate is generally more than 99.50%, and the value of the unified average changing intensity is generally more than 33.50%. This demonstrates that the model has good security in resisting attacks. Therefore, the constructed model can provide good security guarantee under the premise of ensuring the recognition accuracy, which can provide experimental basis for improving the security performance of real-time image text data in the future.

Keywords: Big data, Machine learning, Real-time image text information, Encryption, Convolutional neural network

1 Introduction

Under the background of big data, the continuous development of artificial intelligence (AI) has profoundly changed the way of life and work of contemporary people. People began to shift from the traditional paper image text reading to more intelligent multimedia real-time image text reading. Nevertheless, on the open Internet, real-time image text brings people useful information while also exposing people to

© The Author(s) 2022. **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

the risk of privacy leakage, like a double-edged sword affecting the work and life of people. For example, fraud cases caused by privacy leakage occur frequently, or the homeowner is frequently harassed by the intermediary telephone [1, 2]. Therefore, personal information encryption for users has become the focus of many researchers in related fields, to ensure the security of personal data and avoid the user privacy leakage to the third party.

To ensure the security of personal data, the user can choose to encrypt the image text, and then send the encrypted copy of the data to the cloud server for storage. However, after users upload the image text to the cloud server, some common operations in the plaintext field become difficult, such as searching for a specific file [3]. The simplest and intuitive solution is to search the file after the user downloads all encrypted files from the cloud server locally and restores them to plaintext. However, in the implementation process of this method, unnecessary network and storage costs will be caused by the huge redundant data. Meanwhile, a huge computational burden will occur due to the encryption and decryption operations of large-scale data. In addition, the limitation of objective conditions such as network bandwidth further reduces its feasibility [4]. Therefore, intelligent digital information encryption is particularly important to the current real-time image text. As a critical branch of AI technology, machine learning plays an extremely vital role in many fields, such as machine translation, speech recognition, image segmentation, and natural language processing [5–7]. Among them, the convolutional neural network (CNN) is the most booming feedforward neural network model with optimal performance. Its biggest advantage is the characteristics of local connection and weight sharing. In CNN, numerous neurons are organized in a certain way to respond to overlapping areas in the field of vision. In the process of feature extraction, CNN can autonomously learn the multi-level features of data from the original data such as image text. Besides, the learning process does not require the participation of human experts in relevant fields, which greatly saves manpower, material resources, and time costs [8]. In this way, the problem of huge loss of computational storage space caused by the traditional encryption for digital information of image text is solved, which has important practical value for the further realization of intelligent digital information encryption for real-time image text.

To sum up, in the rapid development of the information age today, it is of great practical value to encrypt real-time images driven by practical needs to ensure people's privacy and security. The innovations of the present work are as follows. First, CNN is transferred into AlexNet by adding a preprocessing module to encrypt the digital information of real-time image text. Secondly, the one-dimensional chaotic system named Logistic-Sine system (LSS) and the multi-dimensional chaotic system called Lorenz system are used to generate chaotic sequences to encrypt the image text. This operation can ensure the security effect and the real-time performance of the system simultaneously. Thirdly, a real-time image text encryption model based on chaotic function and AlexNet is constructed, and its performance is verified by simulation. The present work can provide experimental reference for enhancing the privacy encryption performance of image text in the later stage.

2 Recent related work

2.1 Current status of big data analysis based on deep learning

Nowadays, with the explosive growth of massive and complex data, more and more scientific research institutions and social enterprises are increasingly demanding big data analysis and security functions, especially the use of deep learning (DL), so many researchers have conducted research on it. Chen et al. [9] proposed a method to improve the robustness of 2D/3D optical image encryption by using extended deep CNN. Meanwhile, they improved the security of encryption by introducing pixel scrambling method and using the private key of pixel scrambling operation. They finally proved that this method had good robustness, noise immunity, and security through experiments. Yu et al. [10] used DL to analyze the characteristics of clinical data, discuss various types of clinical data (such as medical images, clinical notes, laboratory results, vital signs, and demographic information), and provide some details of public clinical data sets. They found that although there were challenges in applying DL technology to clinical data, the application of DL in clinical big data was still worth expecting in the direction of precision medicine. Lv et al. [11] constructed the Fuzzy C-means algorithm based on objective function by using K-means and fuzzy theory in big data analysis technology. Through simulation, they found that the improvement of the electric vehicle transportation network by big data analysis technology could significantly reduce the delay of network data transmission performance, change the path, and effectively inhibit the spread of congestion. Ahmed et al. [12] applied the DL method to the clinical or behavioral recognition of autism spectrum disorder. Besides, the authors designed an image generator to generate a single-volume brain image from the whole brain image by considering the voxel time points of each participant separately. Finally, they evaluated four different DL methods, the corresponding ensemble classifiers, and the performance of the algorithm model, and obtained better results on large-scale multi-site brain imaging data set.

2.2 Statue analysis of the information encryption for real-time image text

In this digital information age, sensitive real-time image information is highly likely to be accessed or even attacked by opponents when it is transmitted over unsafe channels. Many scientific researchers focus on information protection methods such as converting sensitive information in real-time images into incomprehensible data, to prevent such unauthorized access. Li et al. [13] proposed a chaotic image encryption algorithm based on information entropy (IEAIE), and analyzed the security of the algorithm in detail. Meanwhile, the scholars evaluated the effectiveness of the adopted quantifiable security measure. They discovered that IEAIE could only be used as a counterexample to illustrate the common defects in the design of secure communication methods for image data. Tresor [14] utilized two-dimensional discrete wavelet transform to decompose and approximate the details of the image, and employed Henon chaotic map to scramble the position of the decomposed image pixels. Finally, they furth57er encrypted the mixed image by XOR operation. Through the experiment, they found that the algorithm had the advantages of large key space, high security, and anti-attacking performance to multiple attacks, which was more suitable for real-time applications. Shah et al. [15] proposed an efficient image

encryption algorithm using the efficient permutation technology based on modular logistic map to encrypt, which reduced the size of chaotic value vector required for real-time image permutation. Moreover, they tested the algorithm's performance on real-time images. Their experimental results showed that the algorithm had good immunity to differential attacks to various statistics such as entropy, histogram analysis, and spectral feature analysis, and could well encrypt and protect the information of real-time images. Hasan et al. [16] constructed an efficient and lightweight encryption algorithm for image security in the medical field, to develop safe image encryption technology for the medical industry. They utilized two replacement techniques for the proposed lightweight encryption algorithm to protect medical images, and proved that this algorithm had higher efficiency than the traditional image encryption algorithm.

Through the above analysis of the relevant research, DL has increasingly expanded the application field in the era of big data. However, image encryption algorithms, such as the chaotic image encryption algorithm, are generally used in real-time image information encryption, which increases the operational memory of computer hardware and software in the process of image text information encryption but reduces the feasibility. Therefore, DL is of great value for real-time image text digital information encryption, with the increasingly widespread application of AI algorithms in various fields at present.

2.3 Methods and text digital information encryption mode

2.3.1 Demand analysis of real-time image text digital information encryption

In the era of big data, users' personal information is transparent to the cloud server to some extent, since most of the files are not encrypted when real-time images and texts are uploaded to the Internet using cloud storage services. Cloud servers can easily view user's personal data based on images or texts, even divulge user's personal information to untrusted third parties, or divulge information due to malicious attacks, which clearly violates user privacy.

The traditional encryption technology has great advantages in protecting image flow data and text data, but shows great weakness in the processing of image data with large redundant information [17, 18]. With the popularization of multimedia communication technology, image data and audio data gradually become the focus of

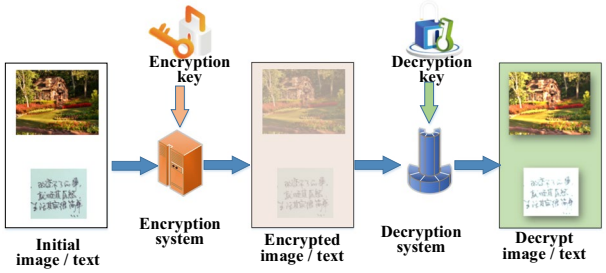

Fig. 1 Image text encryption and decryption system

daily life replacing text data, so how to propose the corresponding encryption algorithm for multimedia data has become mainstream research in recent years. Figure 1 reveals the image text encryption and decryption system.

Figure 1 shows the composition of image encryption and decryption system. From the perspective of key classification, image encryption systems can be divided into the symmetric encryption system with the same encryption and decryption key and the public key encryption system with different encryption and decryption keys [19]. At present, researchers mainly pay attention to the symmetric key image encryption, but the latter also has great research potential.

In summary, the encryption of digital image text information released by people in real life can not only protect people's privacy information, but also prevent attacks from third-party or hackers, which plays a vital role in the era of big data.

2.3.2 Analysis on the application of CNN in image text encryption

CNN, as the fastest growing feedforward neural network model with the best performance, has been successfully applied in image classification and speech recognition. However, these classical CNN structures have not achieved good results in the field of image encryption. Therefore, the network structure needs to be designed due to the particularity of encryption tasks. Therefore, the network structure is designed here according to the analysis of encryption tasks in view of characteristics of image text, and accuracy of encryption results is studied by changing the network structure.

Firstly, like image classification, encryption analysis also requires batch-normalization in the encryption preprocessing of image text. The purpose of batch-normalization preprocessing is to ensure that the loss function of the network model can converge and better extract the characteristics of the image text. The batch-normalization preprocessing is shown in Fig. 2 when preprocessing large quantities of image texts.

From Fig. 2, 128 batches of feature image text with the size of 32*32*64 are input to calculate the mean value as the eigenvalues of 128 batches with the size of 1*1*64. Then, 128 batches of feature image text are fused into a feature vector of 1*1*1*64.

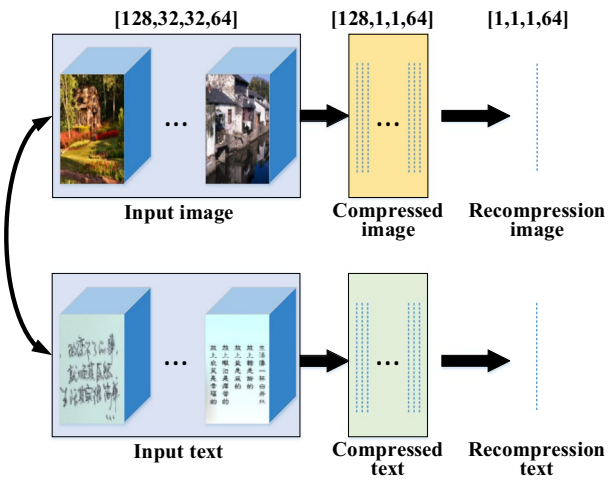

Fig. 2 Optimization principle of batch-normalization preprocessing

When encrypting the image text, a high pass filter (HPF) is also essential for image preprocessing by CNN in addition to batch-normalization preprocessing. Since the digital information encryption for image text is almost always performed in the high frequency part of the image, the image text filtered by HPF can highlight the characteristics of the encrypted part. Besides, the HPF can suppress the influence of image text content on analysis, and enhance the signal-to-noise ratio (SNR) in the image [20, 21], to enable the network to learn the feature expression more effectively.

In the process of image encryption by CNN, fuzziness can guarantee the privacy information of image text. Meanwhile, fuzziness has quite practical applications in many management and engineering problems [22]. There is an equation for the fuzzy number $\tilde{A}(\alpha, C)$ as shown in equation.

$$\mu_{\tilde{A}}(x) = \begin{cases} \begin{cases} 1 - \frac{|x-\alpha|}{C}, & |x-\alpha| \le C, \\ 0, & \text{otherwise}, \end{cases} & C > 0 \\ \begin{cases} 1, & x = \alpha \\ 0, & \text{otherwise}, \end{cases} & C = 0 \end{cases} \tag{1}$$

According to Eq. (1), it is easy to conclude that $\lambda\tilde{A}$ is the fuzzy number $\tilde{A}(\lambda\alpha,\ \lambda C)$, and $\tilde{A}_1 + \tilde{A}_2$ is the fuzzy number $\tilde{A}(\alpha_1 + \alpha_2,\ C_1 + C_2)$.The final structure of CNN image text encryption system is presented in Fig. 3.

In Fig. 3, there are the encrypted image text library, the pre-training module, the DL module, and the classification module in the encryption frameworks. Details are as follows. First, in the encrypted image text library, the encrypted image text can be either a sample library image text of a single encryption algorithm or a sample library image text mixed with multiple encryption algorithms. The sample is generally divided into a training set and a verification set. The training set is used to train CNN, and extract feature images for classification, while the verification set is used to verify the accuracy of training. The training of encryption analysis belongs to supervised training with labels. Second, according to the specific problems, the pre-training module performs various operations on the image sample data, such as batch-normalization, adding a Gaussian filter, image rotation and clipping, and data set enhancement. The purpose of the pre-training module is to make the network converge quickly. Third, the DL module contains some common DL modules including convolution, pooling, full connection, and activation functions. Fourth, the classification module can determine the category of a single sample based on a given output. Whether a sample is an encrypted image can be directly converted to a binary problem like 0, 1. For multi-classification tasks, it is necessary to design multiple classifiers to determine the encryption algorithm, generally using softmax function as a classification function.

The AlexNet neural network with more network layers and stronger learning ability is adopted here [23], to further reduce the computational burden and strengthen the generalization performance of CNN. Besides, the functional layer of the AlexNet neural network model is further improved by exchanging the order of first local normalization and then pooling operation. This improvement has two main advantages. First, it can further enhance the generalization ability of AlexNet neural network, and weaken the over-fitting phenomenon, which greatly reduces the training time. Secondly, the overlapping pooling operation before local normalization can not only preserve more data

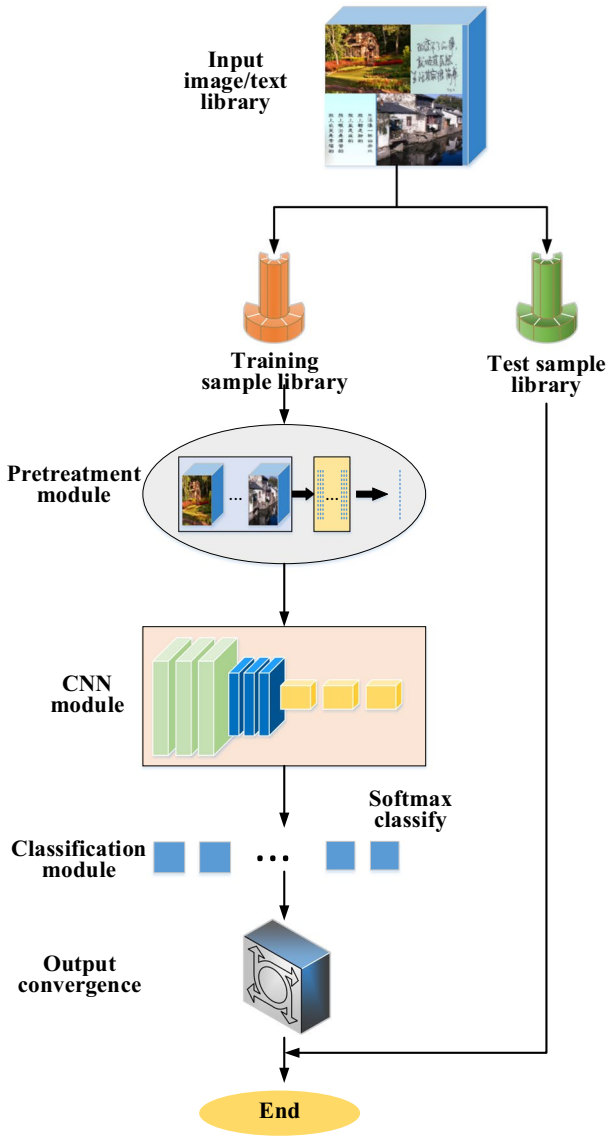

Fig. 3 Structure of CNN real-time image text encryption system

information and weaken redundant information in the process of pooling, but also accelerate the convergence rate of image text digital information encryption training process, and highlight the superiority of overlapping maximum pooling compared with previous maximum pooling methods.

2.3.3 Analysis of RITEM-CF-AN

When encrypting real-time image text, the AlexNet network is formed to encrypt the digital information of real-time image text by adding a preprocessing module to CNN. Moreover, two chaotic functions are utilized to generate chaotic sequences to encrypt image text based on the improvement of AlexNet model, to guarantee the security effect of the model and the real-time performance of the system simultaneously. The

chaotic sequence generated by LSS is used to encrypt the four low-position planes, and the chaotic sequence generated by multi-dimensional chaotic system Lorenz system is used to encrypt the four high-position planes. Figure 4 illustrates the framework of RITEM-CF-AN.

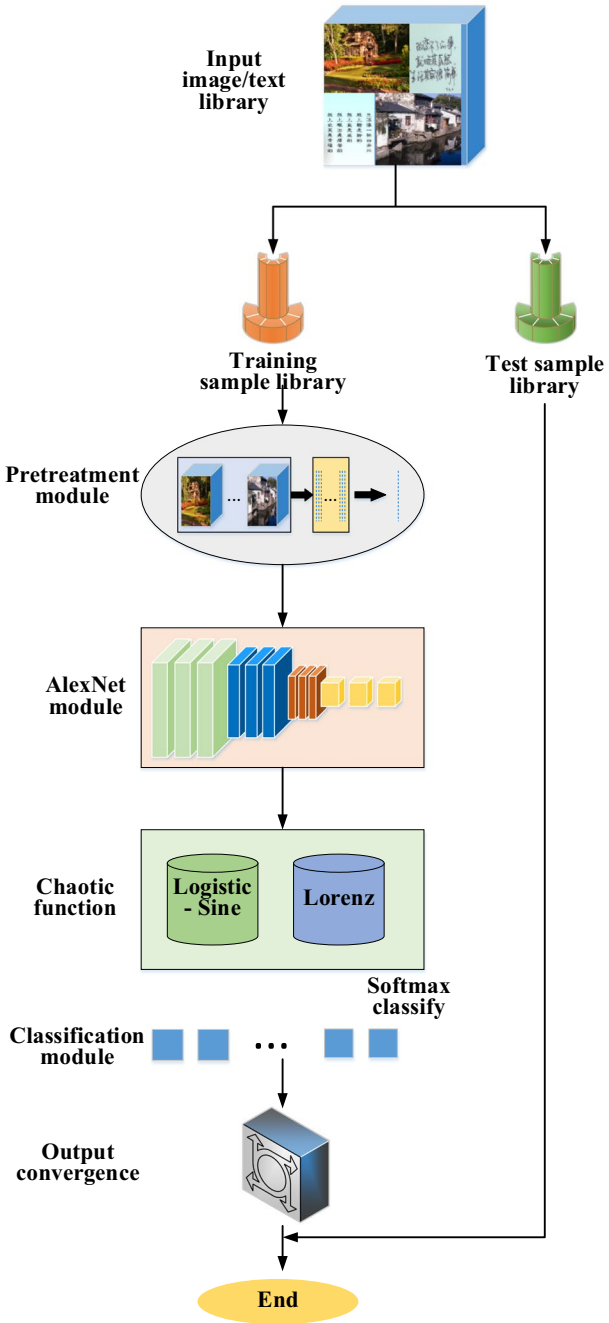

Fig. 4 Framework of RITEM-CF-AN

For a convenient expression, the i-th important bit in the pixel value at the position of (x, y) of the image is denoted as $f_i(x, y) = p_i$, where p_i refers to the percentage of different bits in each pixel value, which is calculated according to Eq. (2).

$$p_i = \frac{2^{i-1}}{\sum_{i=1}^{8} 2^{i-1}} \tag{2}$$

In Eq. (2), the value range of i is $i = \{1, 2, 3, \ldots, 8\}$. G_i represents the i-th bit plane consisting of bits on the same layer in image G, which can be expressed as Eq. (3).

$$G_i = \bigcup_{x=0,y=0}^{x=M,y=N} f_i(x, y) \tag{3}$$

In Eq. (5), $\cup$ refers to the character sequence connection operation, while M and N represent the height and width of the image. Besides, G_1 denotes the bit plane with the maximum information content in image G, and G_8 represents the bit plane with the minimum information content in image G.

In the chaotic function, LSS is used to generate the key of the round function in the encryption system [24]. LSS can be described as Eq. (4).

$$t_{n+1} = (ut_n(1 - t_n) + (4 - u)\sin(\pi t_n)/4) \bmod l \tag{4}$$

Among Eq. (5), the value range of parameter u is (0, 4), and parameter t represents the chaotic sequence generated by the chaotic system. The output of the chaotic system is a sequence between 0 and 1. The Lorenz chaotic system [25] can be written as:

$$\frac{\mathrm{d}x}{\mathrm{d}t} = \sigma(y - x) \tag{5}$$

$$\frac{\mathrm{d}y}{\mathrm{d}t} = x(\rho - z) - y \tag{6}$$

$$\frac{\mathrm{d}y}{\mathrm{d}t} = xy - \beta z \tag{7}$$

where x, y, and z represent the system state, t signifies the time, and σ, ρ, and β denote the system parameters. When $\sigma = 10$, $\rho = 28$, and $\beta = 8/3$, the system generates chaos.

2.3.4 Analysis of simulation experiments

A simulation experiment is conducted here to analyze the performance of the constructed model. The built-in advanced API, keras of the tensorflow framework is adopted to build the network structure, and then the modelummary () function is utilized to print the output network layer and parameters. Besides, the BOSSbase data set is taken as the encrypted data in the simulation experiment. This dataset contains 10,000 Gy images of PGM format with resolution of 512*512 [26]. Since there is insufficient sample data in this data set and the sample needs to reduce the size of the image to reduce the training time, one single 512*512 image in the data set is cut into four 256*256 images. Consequently, the extended data set contains 40,000 images, among which 32,000 images are selected as a training set and 8000 as a test set.

The hyperparameters of the neural network are set as follows. The number of iterations is 60, the simulation time is 2000 s, and the batch size is 128. The specific simulation experiment configuration is mainly considered from both hardware and software. In the software, the operating system is Linux of 64bit, with Python 3.6.1, and the development platform is PyCharm. In the hardware, the CPU is Intel core i7-7700@4.2 GHz of 8 cores, the memory is Kingston ddr4 2400 MHz of 16G, and GPU is Nvidia GeForce 1060 of 8G.

In the recognition accuracy analysis, the proposed model is compared with the algorithms applied by other scholars in the related field. Long Short-Term Memory (LSTM) [27], CNN [28], recurrent neural network (RNN) [29], AlexNet [30], and Multilayer Perceptron (MLP) [31] are selected for comparative analysis from the perspectives of Accuracy, Precision, Recall and F1 value.

Furthermore, information entropy is used for the security analysis of image digital information. The information entropy of an image is the most obvious sign of the randomness of an image [32]. Denote $H(x)$ as the information entropy of image x, which can be presented as Eq. (8).

$$H(x) = \sum_{i=0}^{2^n-1} p(x_i) \log_2 \frac{1}{p(x_i)} \tag{8}$$

In Eq. (8), $p(x)$ represents the probability of sign x. Besides, the closer the information entropy $H(x)$ is to the ideal value, the higher the randomness of the encrypted image is, so the image is more in line with the security standards.

In addition, the differential attack is a selective plaintext attack. The attacker often makes some changes to the original image and then uses the existing encryption algorithm to encrypt the original image and the changed image, and analyzes the relationship between the encrypted image before and after the change to find clues about the encryption key. To resist differential attacks, even if the original image has only one different pixel, the image after encryption must be completely inconsistent. In the analysis, two evaluation criteria are often used to test the difference degree of the encrypted image from the original image. One is the number of pixels change rate (NPCR), and the other is the unified average change intensity (UACI) [33]. In the image encryption performance test, these two standards are often used to judge the sensitivity of the encryption algorithm to the original image, as shown in Eqs. (9) and (10):

$$NPCR = \frac{\sum_{i,j} D(i,j)}{L} \times 100\% \tag{9}$$

$$UACI = \frac{1}{L}\left[\sum_{i,j} \frac{C(i,j) - C'(i,j)}{255}\right] \times 100\% \tag{10}$$

where L represents the total number of pixels in the image, generally can be expressed as M^*N, where M denotes the height of the image, and N refers to the width of the image. Besides, C signifies the encrypted image after the encryption of the original image, and

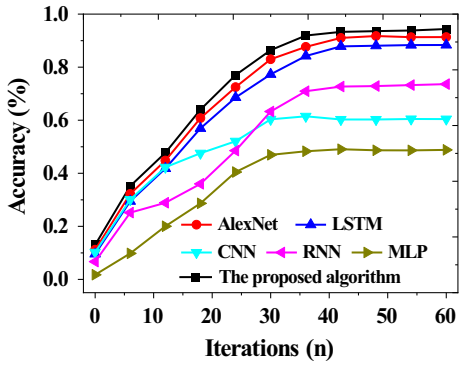

Fig. 5 Accuracy curves of different algorithms with the increase of iteration times

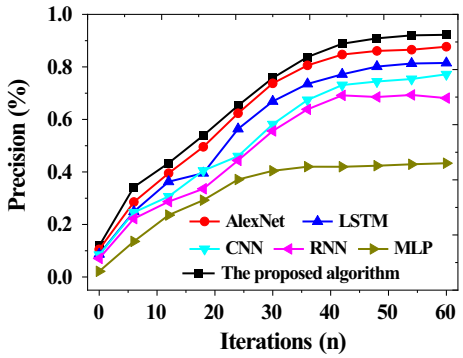

Fig. 6 Precision curves of different algorithms with the increase of iteration times

C' represents the encrypted image after modifying any position pixel. Meanwhile, $D(i, j)$ can be described by Eq. (11).

$$D(i,j) = \begin{cases} 1, & C(i,j) \neq C'(i,j) \\ 0 & C(i,j) = C'(i,j) \end{cases} \tag{11}$$

3 Results

3.1 Analysis of recognition accuracy of different algorithms.

To test the recognition accuracy of the RITEM-CF-AN, it is compared with LSTM model, CNN model, RNN model, AlexNet model and MLP model proposed by other scholars in related fields, from Accuracy, Precision, Recall and F1 value. The results are shown in Figs. 5, 6, 7, and 8.

From Figure 5, 6, 7, and 8, RITEM-CF-AN is compared with the neural network algorithms proposed by scholars in other related fields from the perspectives of Accuracy, Precision, Recall and F1 value. It is found that the recognition accuracy of RITEM-CF-AN is 94.37%, which is at least 3.05% higher than that of other neural network

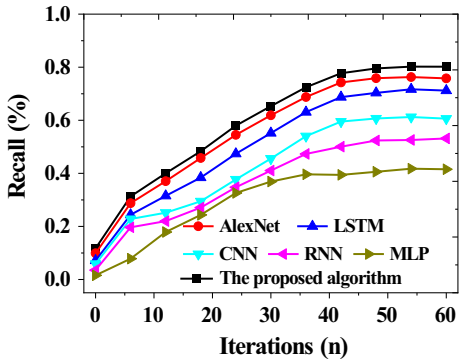

Fig. 7 Recall curves of different algorithms with the increase of iteration times

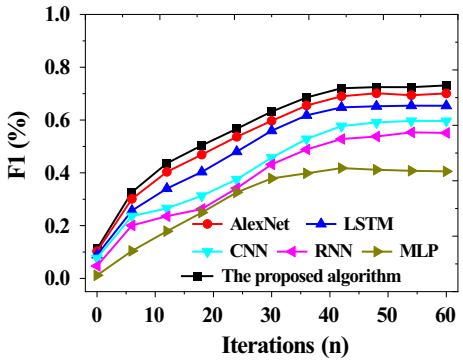

Fig. 8 F1 value curves of different algorithms with the increase of iteration times

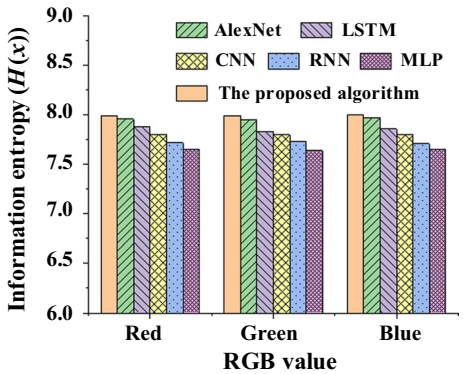

Fig. 9 The influence of different algorithms on the information entropy of pixel value at (0, 0)

algorithms. Meanwhile, it is obvious that the Precision, Recall and F1 values of RITEM-CF-AN are the highest, which are at least 3.03% higher than those of other algorithms.

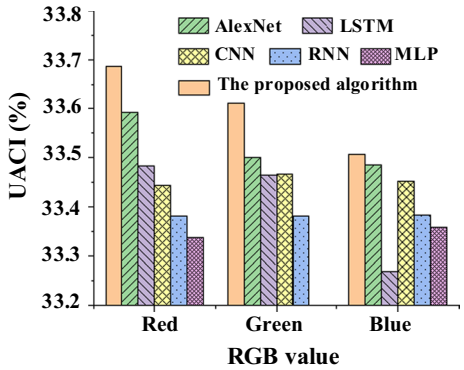

Fig. 10 The influence of different algorithms on NPCR (%) of pixel value at (0, 0)

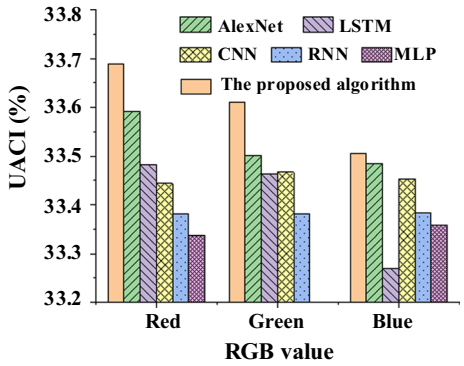

Fig. 11 The influence of different algorithms on UACI (%) of pixel value at (0, 0)

Therefore, compared with other neural network algorithms, RITEM-CF-AN can achieve better encryption accuracy.

3.2 Analysis of the security performance of different algorithms

The security performance of RITEM-CF-AN is compared with that of LSTM, CNN, RNN, AlexNet and MLP algorithms proposed by scholars in related fields, and the results of information entropy, NPCR and UACI are shown in Figs. 9, 10, and 11.

According to Fig. 9, the information entropy of RITEM-CF-AN is close to the ideal value 8, indicating that the encrypted image is almost impossible to leak information. The information entropy of other model algorithms from large to small is H (AlexNet) > H (LSTM) > H (CNN) > H (RNN) > H (MLP). Therefore, RITEM-CF-AN shows high security from the perspective of information entropy.

Then, the comparative algorithms are discussed from the UACI value and NPCR value reflecting the image encryption effect. Obviously, the NPCR values of pixel values at (0, 0) of RITEM-CF-AN are generally more than 99.50%, and the UACI values are generally more than 33.50%. Although other neural network algorithms generally exceed 99% in NPCR values and 33% in UACI values, they still show a significantly worse image encryption performance compared with RITEM-CF-AN. In conclusion,

RITEM-CF-AN is very sensitive to the change of the original image, and can provide good security in resisting differential attacks.

4 Discussion and conclusion

In recent years, the encryption of images has gradually extended from focusing on real-time to grasping both security and timeliness. Aiming at the security problem of real-time image text information, RITEM-CN-AN is constructed based on the machine learning algorithm. Through simulation analysis, the prediction accuracy reaches 94.37%, the NPCR value under RGB pixel value generally exceeds 99.50%, and the UACI value generally exceeds 33.50%. These results can offer good security guarantee and experimental basis for improving the security of real-time image text data in future.

However, there are also some shortcomings in this work. First, the security of the proposed image encryption algorithm is ignored. The security analysis is conducted on the encrypted image from information entropy and correlation coefficient, without the security analysis of the encryption algorithm itself and the neural network. Therefore, the security analysis can be further modified. Second, the selection of the experimental data set is not comprehensive enough. Limited by the experimental environment, there are insufficient types of images in the data set used in this experiment, but the types of images in reality are generally much larger than the selected images. Correspondingly, the designed CNN structure is shallow with a few parameters, to cooperate with the size of the data set. Therefore, it is necessary to further optimize the system structure by selecting larger data sets and deep CNN in the subsequent work.

Abbreviations

CNN: Convolutional neural network; AI: Artificial intelligence; RITEM-CF-AN: Real-time image text encryption model based on chaotic function and AlexNet neural network; DL: Deep learning; HPF: High pass filter; SNR: Signal-to-noise ratio; LSS: Logistic-Sine system; LSTM: Long Short-Term Memory; RNN: Recurrent neural network; MLP: Multilayer Perceptron; UACI: Unified average change intensity; NPCR: Number of pixels change rate.

Acknowledgements

The authors acknowledge the help from the university colleagues.

Authors' contributions

All authors listed have made a substantial, direct and intellectual contribution to the work, and approved it for publication. All authors read and approved the final manuscript.

Funding

This research received no external funding.

Availability of data and materials

The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

Declarations

Ethics approval and consent to participate

This article does not contain any studies with human participants or animals performed by any of the authors. Informed consent was obtained from all individual participants included in the study.

Competing interest

The authors declare that they have no competing interests.

Author details

[1]Baotou Medical College, Inner Mongolia University of Science and Technology, Baotou 014040, China. [2]University of Wisconsin-Madison, Madison, WI, USA. [3]School of Electrical Information, Changchun Guanghua University, Changchun 130033, China. [4]Whiting School of Engineering, Johns Hopkins University, Baltimore, MD 21218, USA.

Received: 7 September 2021 Accepted: 10 March 2022
Published online: 21 March 2022

References

1. Y. Ding, G. Wu, D. Chen, N. Zhang, L. Gong, M. Cao, Z. Qin, DeepEDN: a deep learning-based image encryption and decryption network for internet of medical things. IEEE Internet Things J. **8**(3), 1504–1518 (2020)
2. Y. Ding, F. Tan, Z. Qin, M. Cao, K.K.R. Choo, Z. Qin, DeepKeyGen: a deep learning-based stream cipher generator for medical image encryption and decryption. IEEE Trans. Neural Netw. Learn. Syst., 1–15 (2021).
3. W. Sirichotedumrong, Y. Kinoshita, H. Kiya, Pixel-based image encryption without key management for privacy-preserving deep neural networks. IEEE Access **7**, 177844–177855 (2019)
4. S. Rezaei, X. Liu, Deep learning for encrypted traffic classification: an overview. IEEE Commun. Mag. **57**(5), 76–81 (2019)
5. Z. Chen, A. Fu, Y. Zhang, Z. Liu, F. Zeng, R.H. Deng, Secure collaborative deep learning against GAN attacks in the internet of things. IEEE Internet Things J. **8**(7), 5839–5849 (2020)
6. X. Li, Y. Jiang, M. Chen, F. Li, Research on iris image encryption based on deep learning. EURASIP J. Image Video Process. **2018**(1), 1–10 (2018)
7. T.T. Phuong, Privacy-preserving deep learning via weight transmission. IEEE Trans. Inf. Forensics Secur. **14**(11), 3003–3015 (2019)
8. K. Muhammad, S. Khan, J. Del Ser, V.H.C. de Albuquerque, Deep learning for multigrade brain tumor classification in smart healthcare systems: a prospective survey. IEEE Trans. Neural Netw. Learn. Syst. **32**(2), 507–522 (2020)
9. J. Chen, X.W. Li, Q.H. Wang, Deep learning for improving the robustness of image encryption. IEEE Access **7**, 181083–181091 (2019)
10. Y. Yu, M. Li, L. Liu, Y. Li, J. Wang, Clinical big data and deep learning: Applications, challenges, and future outlooks. Big Data Mining Anal. **2**(4), 288–305 (2019)
11. Z. Lv, L. Qiao, K. Cai, Q. Wang, Big data analysis technology for electric vehicle networks in smart cities. IEEE Trans. Intell. Transp. Syst. **22**(3), 1807–1816 (2020)
12. M.R. Ahmed, Y. Zhang, Y. Liu, H. Liao, Single volume image generator and deep learning-based ASD classification. IEEE J. Biomed. Health Inform. **24**(11), 3044–3054 (2020)
13. C. Li, D. Lin, B. Feng, J. Lü, F. Hao, Cryptanalysis of a chaotic image encryption algorithm based on information entropy. IEEE Access **6**, 75834–75842 (2018)
14. L.O. Tresor, M. Sumbwanyambe, A selective image encryption scheme based on 2d DWT, Henon map and 4d Qi hyper-chaos. IEEE Access **7**, 103463–103472 (2019)
15. A.A. Shah, S.A. Parah, M. Rashid, M. Elhoseny, Efficient image encryption scheme based on generalized logistic map for real time image processing. J. Real-Time Image Proc. **17**(6), 2139–2151 (2020)
16. M.K. Hasan, S. Islam, R. Sulaiman, S. Khan, A.H.A. Hashim, S. Habib, M.A. Hassan, Lightweight encryption technique to enhance medical image security on internet of medical things applications. IEEE Access **9**, 47731–47742 (2021)
17. Y. Chen, Y. Ping, Z. Zhang, B. Wang, S. He, Privacy-preserving image multi-classification deep learning model in robot system of industrial IoT. Neural Comput. Appl. **33**(10), 4677–4694 (2021)
18. A.U.S. Muhammad, F. Özkaynak, SIEA: secure image encryption algorithm based on chaotic systems optimization algorithms and PUFs. Symmetry **13**(5), 824 (2021)
19. Y. Zeng, H. Gu, W. Wei, Y. Guo, $ Deep-full-range $: a deep learning based network encrypted traffic classification and intrusion detection framework. IEEE Access **7**, 45182–45190 (2019)
20. X. Duan, D. Guo, N. Liu, B. Li, M. Gou, C. Qin, A new high capacity image steganography method combined with image elliptic curve cryptography and deep neural network. IEEE Access **8**, 25777–25788 (2020)
21. J. Weng, J. Weng, J. Zhang, M. Li, Y. Zhang, W. Luo, Deepchain: auditable and privacy-preserving deep learning with blockchain-based incentive. IEEE Trans. Depend. Secure Comput., 1–1 (2019)
22. X. Yan, X. Wang, Y. Xian, Chaotic image encryption algorithm based on arithmetic sequence scrambling model and DNA encoding operation. Multimedia Tools Appl. **80**(7), 10949–10983 (2021)
23. X. Liu, H. Li, G. Xu, S. Liu, Z. Liu, R. Lu, PADL: privacy-aware and asynchronous deep learning for IoT applications. IEEE Internet Things J. **7**(8), 6955–6969 (2020)
24. H. Huang, Novel scheme for image encryption combining 2d logistic-sine-cosine map and double random-phase encoding. IEEE Access **7**, 177988–177996 (2019)
25. D. Yousri, T.S. Babu, D. Allam, V.K. Ramachandaramurthy, M.B. Etiba, A novel chaotic flower pollination algorithm for global maximum power point tracking for photovoltaic system under partial shading conditions. IEEE Access **7**, 121432–121445 (2019)
26. D.H. Ko, S.H. Choi, J.M. Shin, P. Liu, Y.H. Choi, Structural image de-identification for privacy-preserving deep learning. IEEE Access **8**, 119848–119862 (2020)
27. J. Duan, J. Zhou, Y. Li, Privacy-preserving distributed deep learning based on secret sharing. Inf. Sci. **527**, 108–127 (2020)
28. C. Zhu, K. Sun, Cryptanalyzing and improving a novel color image encryption algorithm using RT-enhanced chaotic tent maps. IEEE Access **6**, 18759–18770 (2018)
29. A. Al Badawi, J. Chao, J. Lin, C. F. Mun, S.J. Jie, B.H.M. Tan, V. Chandrasekhar, Towards the AlexNet moment for homomorphic encryption: HCNN, the first homomorphic CNN on encrypted data with GPUs. IEEE Trans. Emerg. Top. Comput., 1–1 (2020)
30. X. Duan, J. Liu, E. Zhang, Efficient image encryption and compression based on a VAE generative model. J. Real-Time Image Proc. **16**(3), 765–773 (2019)

31. M. Guan, X. Yang, W. Hu, Chaotic image encryption algorithm using frequency-domain DNA encoding. IET Image Proc. **13**(9), 1535–1539 (2019)
32. G. Zhang, W. Ding, L. Li, Image encryption algorithm based on tent delay-sine cascade with logistic map. Symmetry **12**(3), 355 (2020)
33. W.M. Abd-Elhafiez, M. Heshmat, Medical image encryption via lifting method. J. Intell. Fuzzy Syst. **38**(3), 2823–2832 (2020)

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Submit your manuscript to a SpringerOpen journal and benefit from:

► Convenient online submission
► Rigorous peer review
► Open access: articles freely available online
► High visibility within the field
► Retaining the copyright to your article

Submit your next manuscript at ► springeropen.com