Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 218 (2023) 644–650

Procedia Computer Science

www.elsevier.com/locate/procedia

International Conference on Machine Learning and Data Engineering

Towards Deep Learning for Efficient Image Encryption

Session id: ICMLDE.003

Kirtee Panwar[a], Sonal Kukreja[a], Akansha Singh[a], Krishna Kant Singh[b]

[a]*Bennett University, Greater Noida, Uttar Pradesh, India*
[b]*Amity University, Noida, Uttar Pradesh, India*

Abstract

Deep learning has become a topic of great concern in many domains and also in end-to-end image encryption. Traditional image encryption techniques employ rounds of diffusion and confusion to obtain an explicit trade-off between security and efficiency. With deep learning approach adequate solutions are obtained for current challenges in image encryption schemes such as efficiency, cryptographic strength, etc. In this paper, the latest trends in end-to-end encryption schemes based on deep learning are summarized. Firstly, the existing deep learning-based encryption systems are categorized into three categories: encryption with style transfer, Style transfer with enhanced diffusion properties, and Combining Deep Neural networks with chaotic systems. Each of these methodologies is discussed and relevant conclusions are made. Secondly, these methods are compared and analyzed for their achievements and drawbacks in terms of cryptographic properties of generated cipher images and quality of the recovered images. Third, the possibility of new cryptographic attacks are discussed such as Hidden Factors Leakage and Network Architecture Leakage as consequences of combination of deep learning approaches with an encryption system. Finally, conclusions are made based on comparison and analysis of deep learning approach in end-to-end encryption/decryption systems, providing basis for further research.

Keywords: Deep Learning ; Image Encryption ; Cryptographic Attacks ; Encryption Keys ; Style Transfer

1. Introduction

In the present modern era, there has been a tremendous increase in the frequency of transmission of digital images and delivery on the internet. The sender expects that the transmission channel is secure whereas in reality, security threat of transmission of multimedia data is high. With increase in machine learning techniques in various domains [1], large amount of data is required for training purposes which is one of the main issues in protection of human privacy rights. Digital images have large data size with redundant data and high adjacent pixel correlation. The conventional encryption techniques like DES (Data Encryption Standard), AES (Advanced Encryption Standard) are inappropriate

E-mail address: kirtee.panwar@bennett.edu.in

10.1016/j.procs.2023.01.046

for image encryption [2]. To protect the privacy of an individual on public network platforms [3], researchers have been working to propose solutions that provide image security and robustness. The protection of data in images is ensured by various techniques like image encryption, image stenography, and image authentication. Recently, Deep learning is playing a vital role in techniques like detection of object of interest in images, classification of images, image segmentation, image style transfer, image reconstruction and image compression. Deep Learning based image security has also gained researchers attention recently and achieved breakthrough progress.

Traditional image encryption schemes are based on chaos, due to its cryptography properties. Chaotic encryption scheme was initially proposed by Matthews in 1989 [4]. Many effective image encryption system designs based on chaos have been proposed [5, 6, 7, 8, 9], since then more encryption systems are designed based on chaos and DNA coding [10], wavelet transform, game theory, *etc.* Image encryption schemes are a combination of rounds of diffusion and permutation. In the permutation phase arrangements of pixels are randomly distributed, this enhances resistance against statistical attacks, by this process no information is gained from mosaics of the permuted image. In the diffusion phase the pixel values are modified with help of secret keys. Secret keys play an important role in image encryption.

Due to properties of deep learning such as its non linear structure and ability to learn [11], efforts are being made to combine deep learning with image encryption. Deep learning for image encryption is still in its infancy. Its fusion with cryptography is yet to be explored and this is what attracts attention for further research. This paper summarizes the recent works in literature in deep learning for image encryption to help in understanding the resemblances and differences between deep learning systems and image encryption systems. In this paper, we have described the evolution of deep learning mechanisms in image encryption and summarized increase in research in this direction. We have classified the mechanisms into various categories and analyzed their development in past few years. We have compared these methods, analyzed their pros and cons. In section 4, directions for further explorations are suggested for image encryption through deep learning mechanism. Finally, the paper is concluded in section 4.

2. Image Encryption using Deep Learning

Traditional image encryption techniques use chaotic sequences as secret keys for encryption. The encryption system consists of rounds of permutation and diffusion that are performed on plain image using secret keys [12]. Recently, deep learning approaches have been used for image encryption. Fig. 1 shows the conference and journal IEEE Xplore publication count of image encryption schemes based on deep learning in the recent years. From Fig. 1, it can be seen that deep learning for image encryption has started to gain interest most recently and the attention in this domain is still increasing.

Based on different approaches, some methods have been categorised as follows:

2.1. Image Encryption with style transfer

A set of plain images and set of encrypted images is collected which are the input to the encryption network. The encryption network extracts the style of plain image and transforms it to style of encrypted image. After the encryption network is trained, the model can encrypt a given plain image. This can be performed using GAN, Cycle-GAN [13], [14] and its variants. GANs are capable of transforming image from one domain to another using set of unpaired and unlabelled data. In [13], the encryption model transforms a given plain image to a cipher image. The network parameters are considered as secret keys. With help of these secret keys one can retrieve back the original plain image due to two cycle consistency losses in the model, one to transform plain image to encrypted image and another to retrieve back plain image. Here, the set of encrypted images used for training the network are considered as hidden factors.

As can be observed from Fig. 2, the flow of encryption network in style transfer methodology consists of encryption network that generates cipher image and decryption network that generates recovered image back, to ensure that the network generates desired cipher image quality, discriminator network distinguishes between the desired outcome and actual outcome and penalises the encryption/decryption network accordingly.

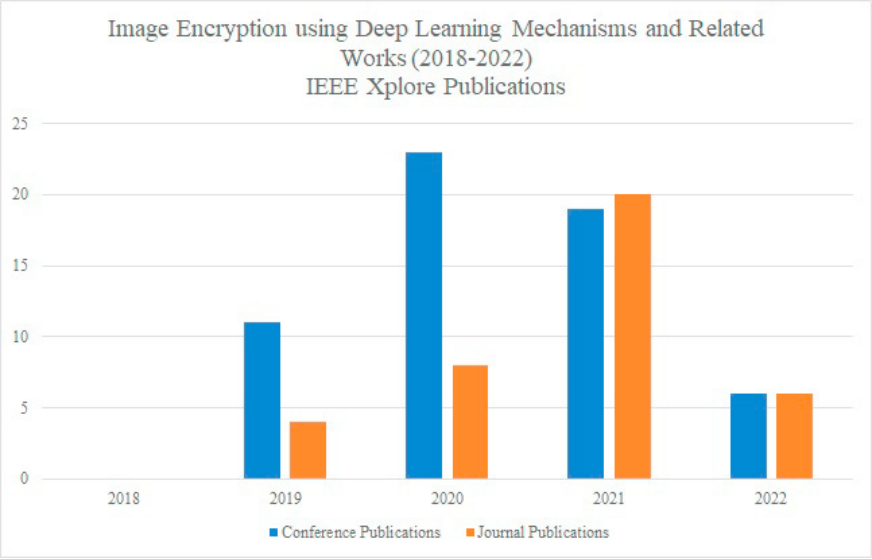

Fig. 1. Statistics of Image encryption using Deep learning mechanisms and related works (2018-2022)

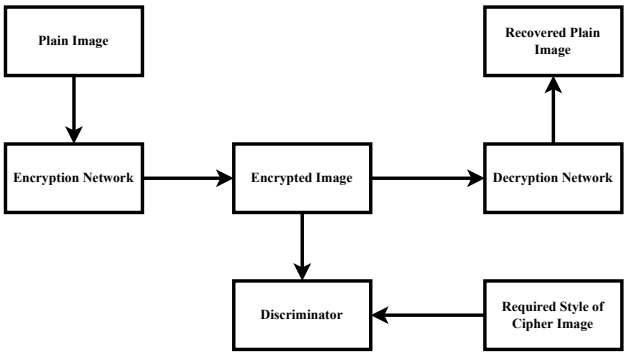

Fig. 2. Cycle-GAN based end-to-end image encryption

2.2. *Style transfer with enhanced diffusion properties*

In [14], the encryption model disguises the plain image with a cover image and communicates the plain image in domain of the cover image. The transformed images from both domain is extracted and used as public-private keys. In [15], the Plain image is first diffused before introducing to the encryption model. The encryption model is similar to [13], except for the loss function where the loss function takes into account the diffused image given as input to the encryption network. In [16], the deep neural network is used to generate cipher images directly without training the network hence the encryption scheme is efficient. The weights of the network are controlled by scrambled DCT coefficients. The non linearity in encryption scheme due to multiple layers and activation functions makes it secure against attacks.

Fig. 3 shows the flow of encryption system with enhanced diffusion properties. Models with enhanced diffusion properties takes in diffused image as input to encryption network [14, 15, 16]. The encryption network generates a cipher image and discriminator distinguishes between output image and desired image thus penalising the encryption network when output deviates from desired output. Similarly, decryption network generates recovered plain image.

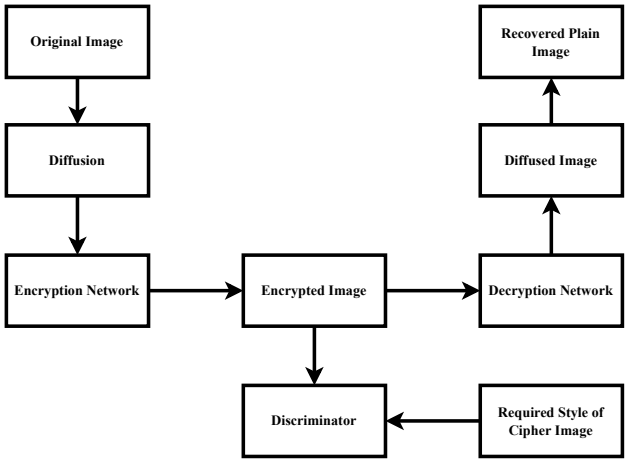

Fig. 3. Image Encryption based on style transfer with enhanced diffusion properties

2.3. Deep Neural network and chaotic sequences

Image encryption is performed by performing convolution over the plain image. The convolution kernel is updated by the chaotic sequences of a given chaotic map and the encryption network does not require training which makes encryption efficient. In [17], image is encrypted by combination of permutation and diffusion operations. To perform permutation operation convolution kernel for convolution neural network is generated using chaotic sequences. After convolution, duplicate data is removed from the result of convolution to obtain permutation sequence for scrambling operation. Then diffusion is performed which is based on fractional Fourier transform or XOR operation with chaotic sequences. The encryption scheme performs fusion, permutation and diffusion. The encryption scheme has a large key space and is efficient. In [16], the encryption network consists of layers in which the weights of the matrices are built of Discrete Fourier Transform (DCT) coefficients.In this encryption system, initial chaotic parameters are the keys instead of network parameters. The encryption scheme is efficient and secure due to non linearity of the deep neural network. Traditional image encryption is performed with secret keys generated through deep learning methods. In [18], deep learning model based on cycle-GAN is used to generate private keys for image encryption. For a given image a private key is spawned by the network which is XORed with the plain image. The key space of the spawned private key is capable of resisting brute force attacks. In [19], deep learning is employed to create dynamic key secret keys that are used for traditional Diffusion through bit-XOR operation. In [20], iris image is used as key to image encryption scheme. Feature vector of iris image is extracted using deep learning model and diffused with plain image using XOR operation to obtain encrypted image.

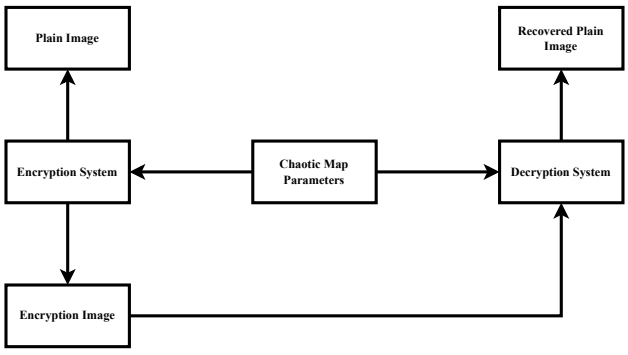

Fig. 4. Image Encryption with combination of convolutional neural network and chaotic sequences

Process of generating cipher images with deep learning is shown in Fig. 4 as performed in [17, 16, 18, 19, 20]. Here, the encryption/decryption system is combined with chaotic system to obtain cipher image with good cryptographic properties.

2.4. Performance Comparison of Different Image Encryption systems based on Deep Learning

Image encryption using Deep learning approaches are summarised in Table 1.

Table 1. Image encryption using Deep learning approaches

Ref	**Year**	**Techniques**	**Problems Solved**	**Drawbacks**
[13]	2020	Image Encryption with Cycle GAN	Use case of Cycle-GAN in image encryption	low Diffusion Metrics
[14]	2019	Image Stgegnography based on Cycle GAN	Image communication in the style of cover image	The secret image needs to be inserted over the cover image, therefore larger cover image is required
[15]	2021	Image encryption using cycle GAN with improved diffusion	Diffusion metrics of image encryption scheme	Traditional diffusion is employed which consists of only XOR operation [12], [5]
[16]	2022	Image encryption using deep neural network with weights controlled by scrambled discrete cosine transform (DCT) coefficients matrices	The encryption scheme is efficient as it does not require training and non linear encryption scheme makes it secure	Histogram is not uniformly distributed and the encryption scheme is not robust against occlusion attacks
[17]	2021	Image encryption with image fusion, convolutional neural network based image scrambling and optical/digital diffusion	Improved diffusion in CNN based image encryption	Requires 2 images for encryption
[18]	2021	Image encryption scheme with dynamic key generation system based on deep learning approach	Generation of dynamic secret key with deep learning approach	Efficiency of the encryption scheme needs to be improved
[19]	2020	Use of deep neural network to generate secret keys and then use it for traditional encryption	Using deep learning mechanism for generation of fine tuned dynamic keys dependent on increase in security threat	After obtaining secret keys through deep neural network, the encryption scheme adopts weak traditional diffusion mechanism for encryption [12], [5]
[20]	2018	Generation of encryption key from Iris Image with Deep Learning Mechanism	Resistance against brute force attack	Weak encryption scheme [12], [5]
[21]	2022	Image Encryption using Chaotic Sequence and Deep Autoencoder	Encoding scrambled image using auto-encoder to obtain uniformly distributed cipher image	Histogram is less uniform as compared to traditional encryption schemes [12], [5], [8]

From Table 1, it can be observed that deep learning based image encryption schemes are still on the verge of improvement. Further, comparison is made with respect to quality of cipher images generated by such models such as image entropy, correlation coefficient, NPCR, UACI. The results are shown in Table 2

Table 2. Comparison of performance of different end-to-end encryption models

Ref	PSNR between recovered image and plain image	Entropy of cipher image
[13]	35.74	–
[14]	17.5992	–
[15]	33.18	7.99
[17]	–	7.99
[18]	–	7.99
[19]	inf	7.98
[21]	–	7.96

From Table 2, it can be observed that cipher images generated by these models have random pixels in them and further research can be continued in this direction. Such a model has greater potential for obtaining a secure encryption network. More focus can be made on quality of recovered image as in [14], the quality of recovered image can be improved further.

3. Attacks on encryption schemes based on Deep Learning Approaches

An ideal image encryption scheme must be scrutinized rigorously to see its resistant towards various attacks [22], [23]. Some of the most common metrics for testing the security of image encryption schemes are: key sensitivity for resistance against brute force attacks, plaintext sensitivity for resistance against plain text attacks, histogram analysis, correlation analysis and entropy analysis for resistance against statistical attacks, Number of Pixel Change Rate (NPCR) for resistance against differential attacks, etc. Even after testing against these metrics, most encryption scheme are found to be vulnerable against attacks especially, plaintext attacks. It is a good practice to analyse the fundamentals of underlying encryption scheme through cryptanalysis point of view. Apart from these traditional attacks, deep learning based image encryption schemes may be subjected to attacks [13] most common to deep learning models such as:

1. **Hidden Factors Leakage**: The attacker tries to develop a deep learning model using the images on which the encryption network was built. The encryption/decryption network can be developed using hidden factors with which secret image can be revealed.
2. **Network Architecture Leakage**: Attacker has access to network architecture but hidden factors remain inaccessible. The attacker employs different hidden factors to obtain secret image. Ideally an image encryption scheme must be able to resist attacks even if the architecture of encryption system is known.
3. **Both Hidden Factors and Network Architecture Leakage**: If both hidden factors on which the encryption/decryption network were trained on and the encryption/decryption system is accessible to attacker, the attacker might be able to obtain secret image from its corresponding cipher image.

4. Conclusion and Future Scope

In this paper, end-to-end image encryption based on deep learning approach is discussed. Deep learning methods for image encryption have been categorized in 3 categories: only style transfer, enhanced diffusion with style transfer and combination of chaotic systems with deep neural network. Each strategy has its pros and cons depending on the application areas. Deep learning-based image encryption schemes with enhanced diffusion properties is preferable when the information secrecy is crucial. Style-transfer with deep learning is preferable when there is a trade-off between efficiency and secrecy. Cryptographic properties of cipher images such as entropy and quality of recovered images,

generated through deep learning approach indicates that encryption systems can be revolutionized with deep learning. Although, introduction of deep learning approach to encryption systems introduces new attacks. Deep learning-based approaches for image encryption are still in its infancy and there is scope for improvement of such systems against cryptographic attacks. Further, possible research directions are modification in architecture of deep learning models to enhance the performance of the security system, identification of better loss functions to obtain better quality of cipher images and recovered images, identification of suitable optimizer for finding an optimal model for encryption, etc. Further exploration can be performed on security against new cryptographic attacks on image encryption network obtained through deep learning models.

References

[1] Sharma, P, Singh, A., Raheja, S. and Singh, K.K. (2019) "Automatic vehicle detection using spatial time frame and object based classification". *Journal of Intelligent & Fuzzy Systems*, 37(6): 8147-8157.

[2] Kocarev, L. (2001) "Chaos-based cryptography: a brief overview. IEEE Circuits and Systems Magazine", 1(3): 6-21.

[3] Singh, P, Singh, N., Singh, K.K. and Singh, A. (2021) "Diagnosing of disease using machine learning. *In Machine Learning and the Internet of Medical Things in Healthcare*, Academic Press, 89-111.

[4] Matthews R. (1989) "On the derivation of a chaotic encryption algorithm." *Cryptologia* **8** (1): 29–41.

[5] Panwar, K., Purwar, R.K. and Jain, A. (2018) "Cryptanalysis and improvement of an image encryption scheme using combination of one-dimensional chaotic maps". *Journal of Electronic Imaging*, 27(5): p.053037.

[6] Wang X , Yang J. (2021) "A privacy image encryption algorithm based on piecewise coupled map lattice with multi dynamic coupling coefficient." *Inf Sci (Ny)* **569** 217–40.

[7] Wang X , Chen X. Chen. (2021) "an image encryption algorithm based on dynamic row scrambling and zigzag transformation". *Chaos, Solitons & Fractals* **147** 110962.

[8] Panwar, K., Purwar, R.K. and Srivastava, G. (2021) "A Fast Encryption Scheme Suitable for Video Surveillance Applications Using SHA-256 Hash Function and 1D Sine–Sine Chaotic Map". *International Journal of Image and Graphics*, 21(02): p.2150022.

[9] Wang X , Gao S. (2020) "Image encryption algorithm based on the matrix semi-tensor product with a compound secret key produced by a boolean network". *Inf Sci (Ny)* 539 195–214.

[10] Panwar, K., Purwar, R.K. and Jain, A. (2019) "Design of a SHA-2 Hash Based Image Encryption Scheme using 1D chaotic systems and DNA sequences". *IEEE International Conference on Computing, Power and Communication Technologies (GUCON)* 769-773.

[11] Sharma, P. and Singh, A., (2017), July. Era of deep neural networks: A review. *8th IEEE International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 1-5.

[12] Panwar, K., Purwar, R.K. and Jain, A. (2019) "Cryptanalysis and improvement of a color image encryption scheme based on DNA sequences and multiple 1D chaotic maps". *International Journal of Bifurcation and Chaos*, 29(08): p.1950103.

[13] Ding, Y., Wu, G., Chen, D., Zhang, N., Gong, L., Cao, M. and 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.

[14] Zheng, Z., Liu, H., Yu, Z., Zheng, H., Wu, Y., Yang, Y. and Shi, J. (2019)" EncryptGAN: Image Steganography with Domain Transform". arXiv preprint arXiv:1905.11582.

[15] Bao, Z. and Xue, R. (2021)" Research on the avalanche effect of image encryption based on the Cycle-GAN". *Applied Optics*, 60(18): 5320-5334.

[16] Wang, C. and Zhang, Y. (2022) "A novel image encryption algorithm with deep neural network". *Signal Processing*, 196: p.108536.

[17] Man, Z., Li, J., Di, X., Sheng, Y. and Liu, Z. (2021) "Double image encryption algorithm based on neural network and chaos". *Chaos, Solitons & Fractals*, 152: p.111318.

[18] Ding, Y., Tan, F., Qin, Z., Cao, M., Choo, K.K.R. and Qin, Z. (2021) " DeepKeyGen: a deep learning-based stream cipher generator for medical image encryption and decryption". *IEEE Transactions on Neural Networks and Learning Systems* 1-5.

[19] Maniyath, S.R. and Thanikaiselvan, V. (2020) "An efficient image encryption using deep neural network and chaotic map". *Microprocessors and Microsystems*, 77: p.103134.

[20] Li, X., Jiang, Y., Chen, M. and Li, F. (2018) "Research on iris image encryption based on deep learning". *EURASIP Journal on Image and Video Processing*, (1): 1-10.

[21] Sang, Y., Sang, J. and Alam, M.S. (2022) "Image encryption based on logistic chaotic systems and deep autoencoder". *Pattern Recognition Letters*, 15: 59-66.

[22] Li, C., Zhang, Y. and Xie, E.Y. (2019) "When an attacker meets a cipher-image in 2018: A year in review". *Journal of Information Security and Applications*, 48: p.102361.

[23] Chen, L., Li, C. and Li, C. (2022) "Security measurement of a medical communication scheme based on chaos and DNA coding". *Journal of Visual Communication and Image Representation*: p.103424.