

CryptoGAN: a new frontier in generative adversarial network-driven image encryption

Ranjith Bhat^{1,2}, Raghu Nanjundegowda³

¹Faculty of Engineering and Technology, JAIN (Deemed to be University), Bengaluru, India

²Department of Robotics and Artificial Intelligence Engineering, NMAM Institute of Technology, NITTE (Deemed to be University), Nitte, India

³Department of Electrical and Electronics Engineering, JAIN (Deemed to be University), Bengaluru, India

Article Info

Article history:

Received Feb 11, 2024

Revised Jun 12, 2024

Accepted Jun 14, 2024

Keywords:

Cryptography

Deep learning

Generative adversarial networks

Image encryption

Image-to-image translation

ABSTRACT

There is a growing need for an image encryption scheme, for huge amount of social media data or even the medical data to secure the privacy of the patients or the user. This study introduces a ground-breaking deep learning architecture named crypto generative adversarial networks (CryptoGAN), a novel architecture for generating cipher images. This architecture has the ability to generate both encrypted and decrypted images. The CryptoGAN system consists of an initial encryption network, a generative network that verifies the output against the desired domain, and a subsequent decryption phase. The generative adversarial networks (GAN) are utilised as the learning network to generate cipher images. This is achieved by training the neural network using images encrypted from a conventional image encryption scheme such as advanced encryption standards (AES), and learning from the resulting losses. This enhances security measures when dealing with a large dataset of photos. The assessment of the performance metrics of the encrypted image, including entropy, histogram, correlation plot, and vulnerability to assaults, demonstrates that the suggested generative network may get a higher level of security.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Ranjith Bhat

Research Scholar, Faculty of Engineering and Technology, JAIN (Deemed to be University)

Bengaluru, India

Email: ranjithbhat@gmail.com

1. INTRODUCTION

As network communication and multimedia technology advance quickly, an increasingly higher number of digital images are being saved, duplicated, and sent via unprotected channels or third-party platforms [1]. As a result, image security is currently very popular [2]. There are several ways to safeguard the security of images, including steganography [3], [4], watermarking [5], [6], and encryption [7]–[11], the more popular and useful method being picture encryption. Two stages are typically involved in image encryption: the stage of diffusion and the step of scrambling. Scrambling modifies the relative positioning of pixels in the image, while diffusion modifies their precise value. Data encryption standard (DES), international data encryption algorithm (IDEA), and advanced encryption standard (AES) are instances of block ciphers; in comparison, stream ciphers are more secure, faster to encrypt and decrypt, less prone to error expansion, more synchronised, and affordable to implement [12], [13]. Nevertheless, creating a security stream cipher generator that makes the process of creating the random and unpredictable sequence easier is one issue. Linear feedback shift registers, nonlinear feedback shift registers, chaotic systems, finite automation, linear congruence generators, and linear feedback shift registers are examples of common stream cipher generators. The majority of current methods utilising private key generators include manually designing the generators (for instance, by applying

mathematical formulae) to produce the private key in order to accomplish a higher level of security. In numerous computer vision applications, deep learning has been effective [14]. Generative adversarial networks (GAN) [10] is recognised as one of the most widely adapted deep learning techniques [15], [16]. The generator generates samples, and the discriminator figures out how to tell them apart from real-world samples. These two parts combine to form a GAN. The discriminator and generator engage in a contest to produce data that is as realistic as possible. It appears that GAN-based methods are effective for translating images between different domains. Consequently, we combine the cipher generator and image-to-image translation network to create a novel deep learning-based cipher image generation network (CryptoGAN). In Figure 1, components of the GAN system are exemplified by the neural network G, referred to as the generator, and the discriminator network D.

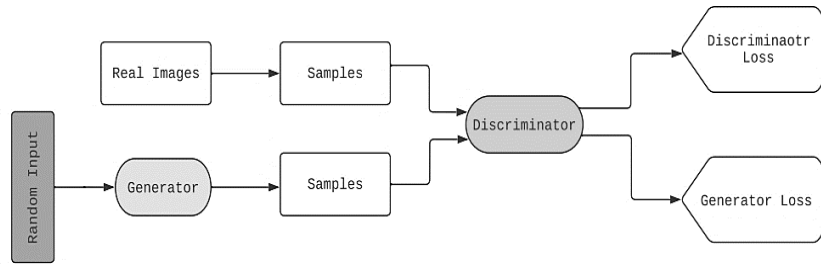


Figure 1. GAN architecture [10]

The main objective of the discriminator network D is to improve its performance by utilizing feedback and backpropagation. In this case, we encrypt using this neural network architecture that has been formed using the weights available after training using the target domain images, which are the ground truth of the traditional cipher image, and the images generated by the encryption. As per the generator's output, we are able to provide the precise data. The discriminator is trained using the generated cases as a negative example as well. The discriminator can now more accurately recognize the difference between the generator's real and synthesised data. The discriminator punishes the generator using appropriate loss function if it produces results that are highly improbable.

2. RELATED WORKS

Chen *et al.* [17] suggests a GAN-based model for efficient and secure end-to-end color picture encryption. Singh *et al.* [18] shows how to encrypt digital photographs using GANs and then use super-resolution to restore them. This outlines a GAN-enhanced chaotic encryption technique [19] for secure and simple optical code-division multiplexing. According to Hallman [20], it examines GANs' utility in security analysis and their application to cryptanalysis. Purswani *et al.* [21] highlights the improvement of security characteristics by concentrating on the generation of chaotic sequences utilizing GANs for encryption.

2.1. Losses in generative adversarial networks

The use of GANs allows for the replication of a probability distribution. Since the GAN's output distribution differs from the real data distribution, they should employ loss functions that take this disparity into consideration. Generator loss is the generators output being $G(z)$ and the discriminators output being $D(z)$ generator aims to maximize this $D(G(z))$ function i.e. to improve the correct discrimination of the generated output in this case it is the generated encrypted image because of the trained loss functions [16]. In short, its goal is to have the discriminator produce more false positives. Discriminator loss during the training process, the discriminator distinguishes between the authentic data generated by the generator and the fake data. Deep learning algorithms often necessitate the use of a loss function for training the model. Here (1) shows, the overall loss is the aggregate of the losses incurred by the encryption neural network G.

$$L = L_{Gen} + L_{Dis} + L_{RCon} \quad (1)$$

Where L_{Gen} , the discriminator network D, L_{Dis} , and the reconstruction loss of the decryption network F, L_{RCon} . GAN discriminator is the output image of the encryption network is assessed for domain compatibility using the suggested discriminator network, D. To lower the image's resolution [17] and further encode the local features for image discrimination, D uses double convolutional blocks following first convolutional layers. The

final output is expected to be developed using a 3×3 convolutional block and a feature generating block. Leaky rectified linear unit (ReLU) with a value of 0.2 is implicit in every convolutional layer, and the batch normalisation (BN) layer follows [18]. The purpose of training network D is to identify images as either belonging to the network G (cipher text domain) or not. This is where the G-network yields: in (2), G represents the encrypted network, while D represents another encrypted network.

$$L_D = E_{x \sim p_{data}(x)} \log D(x) + E_{x \sim p_{data}(x)} \log (1 - D(G(x))) \quad (2)$$

3. METHODOLOGY

The stages of the proposed methodology are portrayed in Figure 2. In the first stage, input data is encrypted using a secure key and an algorithm is used to prepare them for converting into the targeted encrypted domain. In the second stage, the generative network checks if the output image from the encryption network complies with the desired domain using the loss function mentioned in the next section. The final step is to use decryption, which is quite similar to the encryption process, to regenerate the original image, a process similar to that used for encryption.

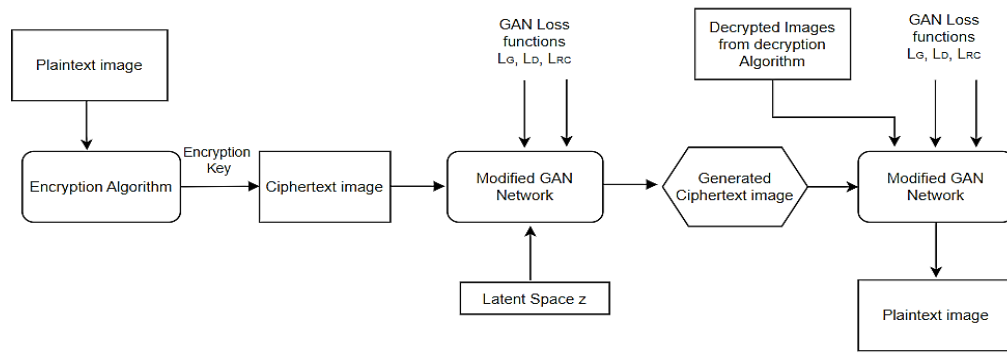


Figure 2. The key generation process for the generative network

Due to the GAN's robust nonlinearity and randomly initialised parameters, the parameters of the learning network can exhibit substantial variation at different phases of training. In simple terms, the instability of a GAN network in computer vision applications is a drawback. Notwithstanding its inherent unpredictability, cryptography offers specific advantages. The proposed encryption approach, which utilises deep learning techniques, can be likened to a one-time pad (OTP) method due to its exploitation of this inherent instability. Specifically, upon training the provided network at distinct time intervals, in summary, the proposed architecture would offer enhanced security as a result of deep and intricate nature of the encrypt-train network.

3.1. Encryption process and the CryptoGAN architecture

Typically, a picture will undergo a process of traditional encryption, such as AES for photos, before being transformed to the target domain. A multi-layer modified GAN supports the encryption process, as seen in Figure 3, by training the GAN's generator with the loss function of the encrypted images. During training, the discriminator is trained using the encrypted picture and a notable loss function, which will be called the original loss function henceforth [19]. In order to compare the loss functions acquired during discriminator training with the encrypted data, this original loss function is utilized.

Not only that, but it also shows the generator how much it needs to improve its performance through training. We use the discrepancies in the losses as a starting point for measuring additional loss functions. As demonstrated in Figure 4, the secured encrypted image is further strengthened in security by feeding it into the generator. This generator can be the same that was trained with the original loss function or a different one that uses a new loss function acquired while training with the encrypted image. The conventional algorithm is then used to implement this enhancement. In the intentions to improve the security efficiency, the discriminator strives to outperform the generator by producing better encrypted and secured data. This accomplishes the task of translating the input visual data from the target domain into the desired format. The G sets up the first convolutional stage to encode and compress the images [20]. Several characteristics and losses are produced during this stage, which will be used in the forthcoming transformation. The different qualities and content are provided by combining 9 leftover blocks with identical layouts.

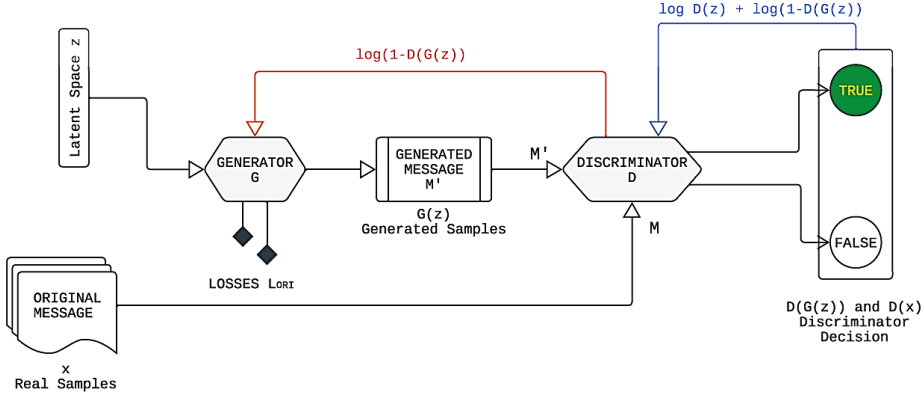


Figure 3. Training the discriminator with the original encrypted images

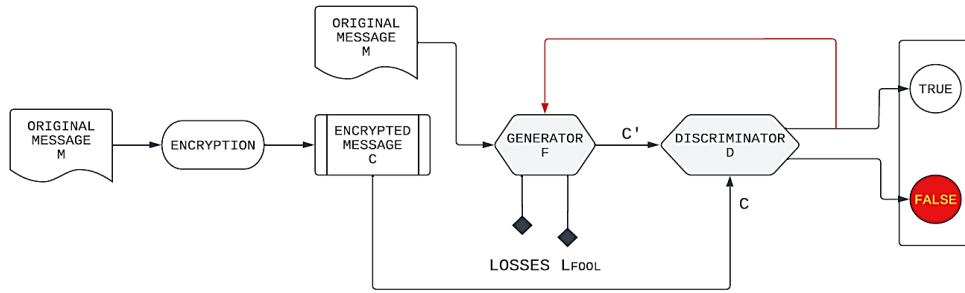


Figure 4. Training the discriminator with the losses

Reconstructing the output image requires a number of components, including two up-convolution blocks and the stride accurately applied. The final step is to export all predictions using a 7×7 convolutional kernel. Making the change from source to target domain images Y , accomplishes this task as per the loss functions mentioned in (3) and (4) [10]. The two mappings, $G: X \rightarrow Y$ and $F: Y \rightarrow X$, are included in the proposed model. In order to fool the discriminator, mapping function G must first determine this process [21].

$$L_G = \min_G (E_{x \sim p_{data(x)}} \log (1-D (G(x)))) \quad (3)$$

$$L_{RC} = E_{x \sim p_{data(x)}} \|Y - X\|_1 \quad (4)$$

4. EXPERIMENTAL SIMULATION AND MODEL PERFORMANCE ANALYSIS

4.1. Discriminator and generator loss plot

The loss curves for the discriminator and generator are appearing to be steep at the beginning of the learning process for the GAN in Figure 5. But as training continues, the generator's loss goes down, which means it gets better at producing images and tricks the discriminator. Because of this, the discriminator's loss remains constant up until it reaches a minimum. We see a reversal in the generator's loss around the 150th epoch [22]. It may also indicate that the training has reached its limit [23], and hence saturated in learning.

4.2. Information entropy

For many images processing tasks, information entropy is the go-to metric for measuring how unpredictable a noise map is. The entropy value, $H(m)$, can be determined [24] using (5). This approach outperforms the algorithms in [25]–[27] in terms of entropy, and the encrypted image's pixel distribution.

$$H(m) = - \sum_{i=0}^{2^N-1} p(m_i) \log_2 p(m_i) \quad (5)$$

N represents the grey level, and $p(m_i)$ denotes the likelihood of m_i . The optimal entropy [16] for a 256-grayscale cipher-image is 8, implying the data is unknown. As a result, an information entropy close to 8 is typical for highly secure encrypted images. The entropy of the generated encryption image is in Table 1.

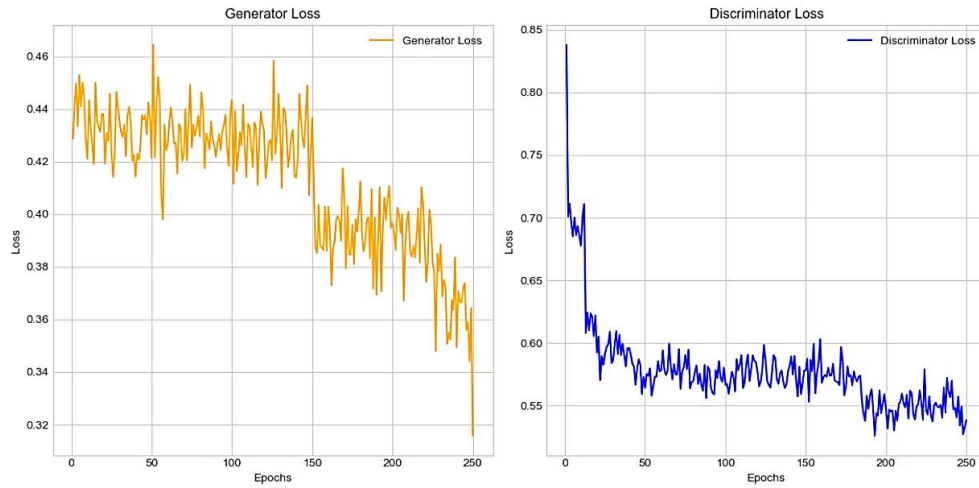


Figure 5. The loss curves of the generator and discriminator after training

Table 1. Entropy information of encryption

	Image_1	Image_2	Image_3	[25]	[26]	[27]
Entropy	7.9954	7.9978	7.9958	7.9912	7.9972	7.9973

4.3. Robustness against cropping and noise

With the intentions of assessing the resilience of the cipher-images against cropping attacks, portions measuring 128×128 and 64×64 are removed. The original image, the encrypted image, 128×128 cut in the encrypted image, and the decrypted image of image_1 and the original image, the encrypted image, 64×64 cut in the encrypted image, and the decrypted image of image_2 is shown in Figure 6, respectively. Because of this, our approach is resistant to attacks of this nature. Tables 2 and 3, include findings for histogram, neighbouring pixel correlation, peak signal-to-noise ratio (PSNR), all of which confirm this claim.

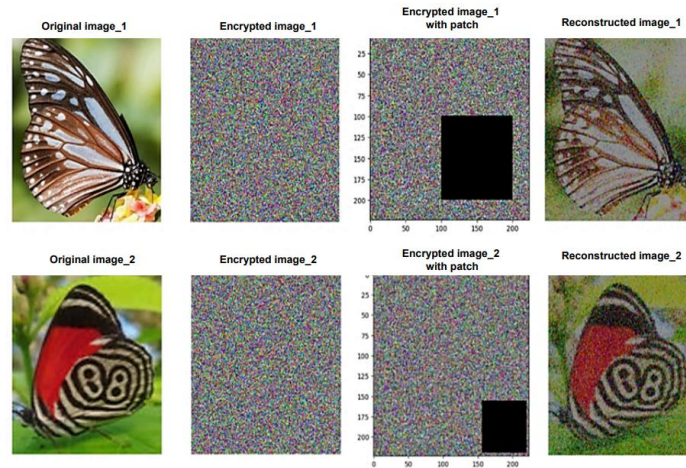
Figure 6. The original image_1, encrypted image_1, 128×128 cut in the encrypted image_1, and decrypted result, respectively. Original image_2, encrypted image_2, 64×64 cut in the encrypted image_2, and decrypted result, respectively

Table 2. Correlation coefficient of encrypted images

	Image_1	Image_2	Image_3	[28]	[29]	[30]
Horizontal	7.9977	7.9905	7.9929	7.9972	7.9933	7.9912
Vertical	0.0016	-0.0099	0.00288	-0.00209	0.0093	0.00964
Vertical	-0.0168	0.0059	0.01963	-0.1618	0.0159	0.01963
Diagonal	-0.0010	-0.0002	0.0225	0.0178	0.0097	0.01963

Table 3. Mean square error (MSE) and PSNR of encrypted images

	Image_1	Image_2	Image_3	[31]	[27]	[32]
MSE	8802.5	8485.5	7005.5	-	-	6885.83
SNR	8.8755	8.5962	9.5674	28.8	8.548	0.18

4.4. Histogram analysis

The histogram of an image encryption technique is a crucial indicator of its effectiveness. It may demonstrate the distribution pattern of image pixels by depicting the number of pixels that correspond to each grey level and the frequency at which each grey level appears. The consistent pattern observed in the pixels of the plain shots is not present in the cipher images. Figures 7(a) to 7(c) show the histogram analysis of the original image_1, encrypted image_1, and decrypted image_1, respectively. Figures 7(d) to 7(f) show the histogram analysis of the original image_2, encrypted image_2, and decrypted image_2, respectively. Figures 7(g) to 7(i) show the histogram analysis of the original image_3, encrypted image_3, and decrypted image_3, respectively. This suggests that the attacker is incapable of using any statistically significant data acquired from the cipher-image to specifically target the method.

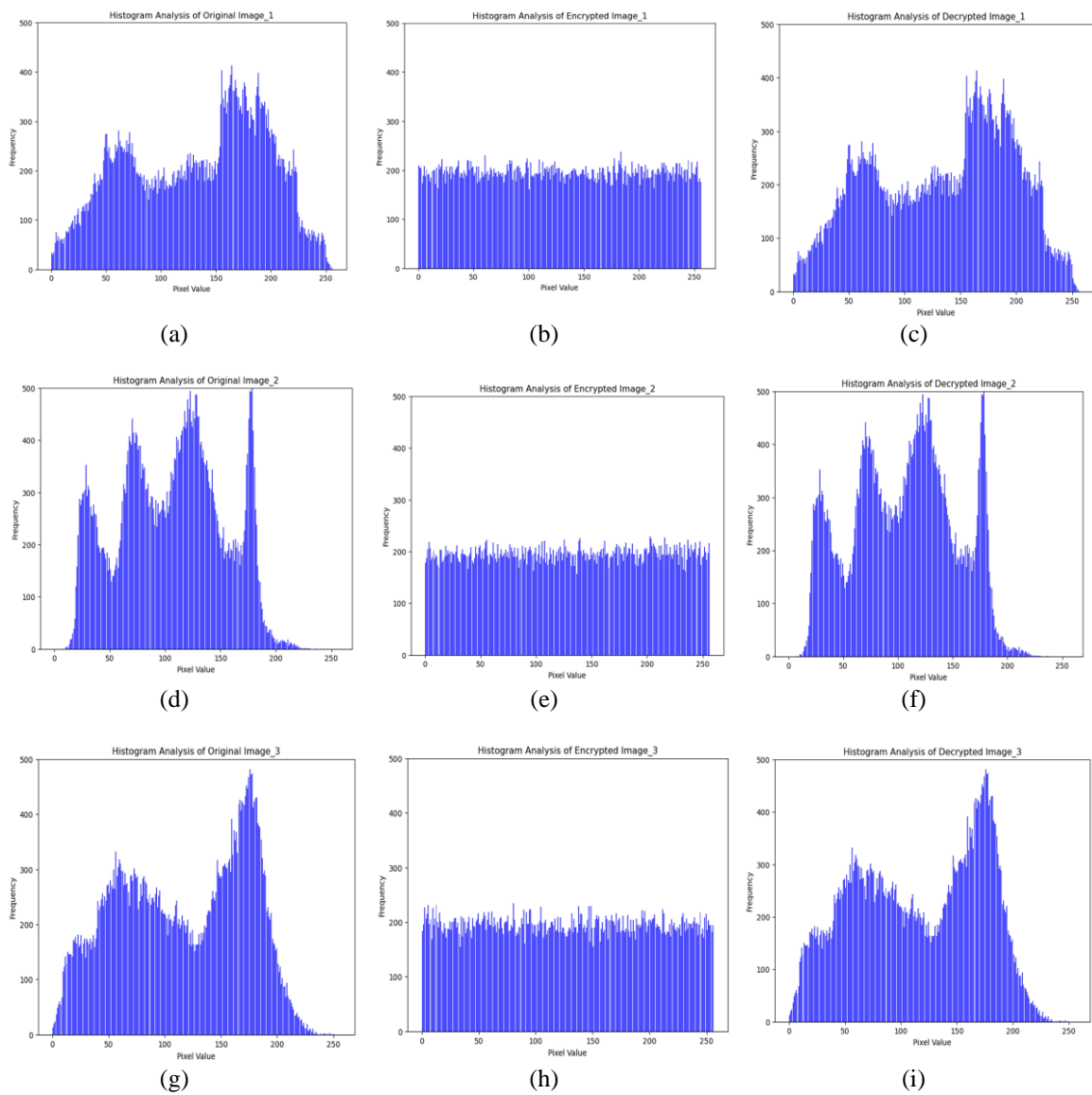


Figure 7. Histogram analysis: (a) original image_1, (b) encrypted image_1, (c) decrypted image_1, (d) original image_2, (e) encrypted image_2, (f) decrypted image_2, (g) original image_3, (h) encrypted image_3 and (i) decrypted image_3

4.5. Adjacent pixels correlation

Table 2 shows how dependent or similar neighbouring pixels in the encrypted picture are on one another. Diffusion effects are more pronounced and regularity is diminished when correlation coefficients are lower. For this investigation, geographic statistics or correlation coefficients has be utilised. The horizontal correlation plot of the original images_1, encrypted image_1, and decrypted image_1 are shown in Figures 8(a) to 8(c), respectively, the vertical correlation plot of the original images_2, encrypted image_2, and decrypted image_2 are shown in Figures 8(d) to 8(f), respectively and the diagnol correlation plot of the original images_3, encrypted image_3, and decrypted image_3 are shown in Figures 8(g) to 8(i), respectively.

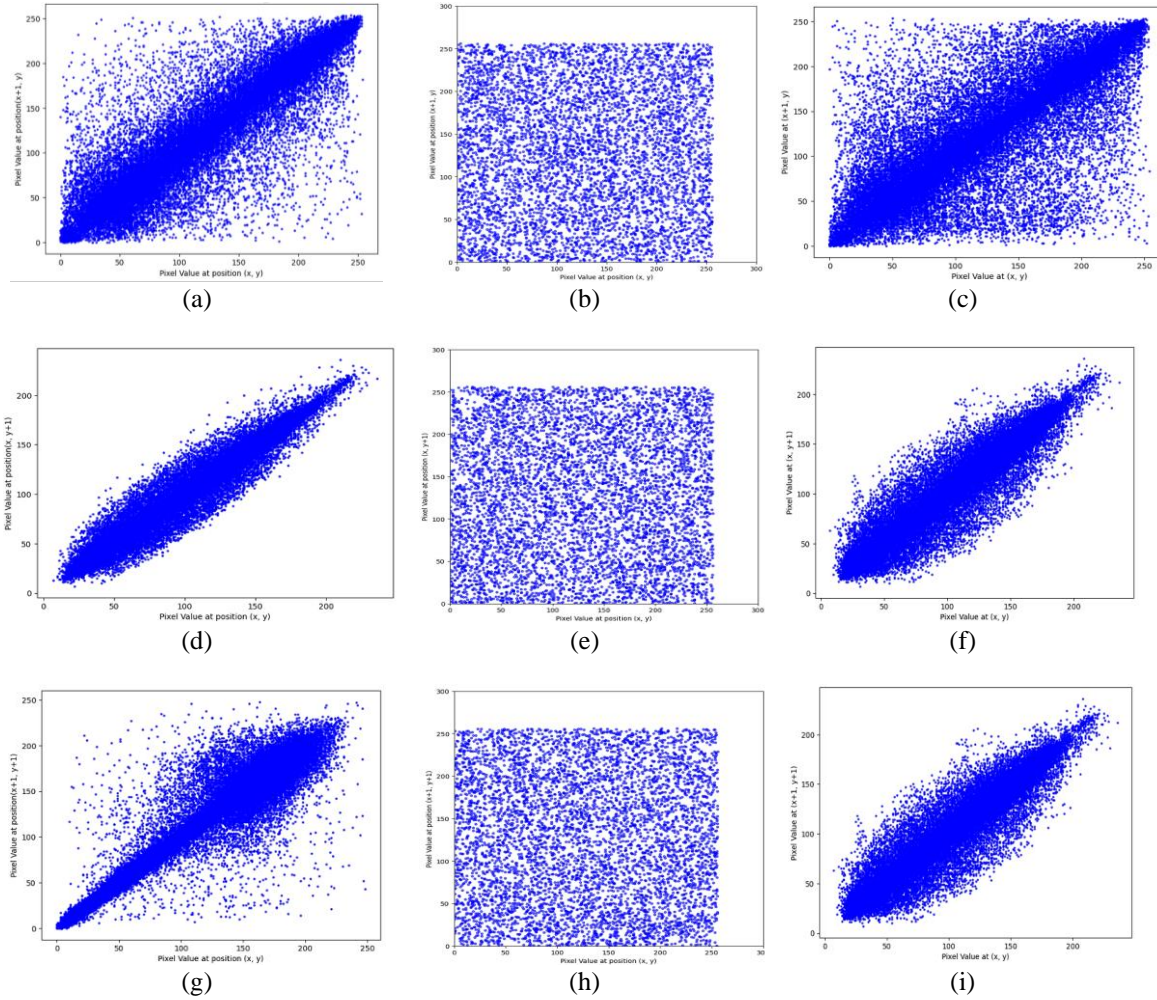


Figure 8. Horizontal correlation of: (a) original image_1, (b) encrypted image_1, (c) decrypted image_1.

Vertical correlation: (d) original image_2, (e) encrypted image_2, (f) decrypted image_2. Diagonal correlation: (g) original image_3, (h) encrypted image_3, and (i) decrypted image_3 [31]–[34]

4.6. Peak signal-to-noise ratio

By contrasting the encrypted image with the original plain image, we can determine the PSNR. More disparities and higher randomness are indicated by a lower PSNR. The MSE between the plain and cipher pictures is frequently used to calculate PSNR. MSE in (6), is a metric used to compare plain-image and cipher-image differences.

$$MSE = \frac{\sum_i \sum_j (P(i,j) - C(i,j))^2}{T} \times 100\% \quad (6)$$

The number of pixels in an encrypted picture is represented by T , here. A greater number for MSE indicates that the image's encryption effect is powerful, as the disparity between the encrypted and original image is bigger. A PSNR is the ratio of the plain picture to the cipher image. One way to think about PSNR is in (7). The maximum pixel value of the plain-image is represented by max. The lower the PSNR, more random

the encrypted image should be, and hence the objective of an effective encryption method [28]. For comparison, we look at [29]–[31] and see the cipher-image MSE and PSNR values in Table 3.

$$PSNR = 10 \log_{10} \left(\frac{I_{max}^2}{MSE} \right) \quad (7)$$

4.7. Differential attack

The resistance to differential attacks can be determined by analysing how the cipher image changes in response to small changes to the plain image. We make use of metrics like number of pixels change rate (NPCR) [26] and unified average changing intensity (UACI) [15]. The attack aims to deduce the link between the plain image and its cipher image by comparing the two encrypted images. The NPCR and the UACI are two measures that are used to assess differential attacks. Here are the ideal values for the cipher-image's UACI and NPCR: 33.4653% and 99.6093%, respectively [32]–[35]. Both the calculations are presented in Table 4.

Table 4. UACI and NPCR performances

	Image_1	Image_2	Image_3	[33]	[34]	[35]
NPCR	99.450	99.666	99.652	99.62	99.72	99.62
UACI	32.855	33.523	33.268	33.53	33.45	33.42

5. CONCLUSION

This work creatively presents CryptoGAN, a modified GAN for image encryption. The encryption samples are achieved by utilising the GAN model's strong learning capability. The encrypted image generation system suggested in this paper is shown to be capable of providing solid assurances for image security for a large number of images through efficiency test, entropy, and histogram analysis. This goes a long way towards expanding the new frontier of image security research, as this is a less commonly accepted approach. GAN architecture is changed and revamped to increase the robustness of encrypted images. The scheme has an average entropy of 7.9972, according to the experimental data. Differential, cut, and noise attacks constitute the additional methods used to validate the scheme's defence against attacks. We intend to enhance the current model and address its weaknesses in the future, with the goal of achieving greater accuracy in both encryption and decryption.




REFERENCES

- [1] W. Cao, Y. Mao, and Y. Zhou, "Designing a 2D infinite collapse map for image encryption," *Signal Processing*, vol. 171, Jun. 2020, doi: 10.1016/j.sigpro.2020.107457.
- [2] X.-Y. Wang and Z.-M. Li, "A color image encryption algorithm based on hopfield chaotic neural network," *Optics and Lasers in Engineering*, vol. 115, pp. 107–118, Apr. 2019, doi: 10.1016/j.optlaseng.2018.11.010.
- [3] A. A. Abdulla, H. Sellahewa, and S. A. Jassim, "Improving embedding efficiency for digital steganography by exploiting similarities between secret and cover images," *Multimedia Tools and Applications*, vol. 78, no. 13, pp. 17799–17823, Jul. 2019, doi: 10.1007/s11042-019-7166-7.
- [4] Q. Li *et al.*, "A novel grayscale image steganography scheme based on chaos encryption and generative adversarial networks," *IEEE Access*, vol. 8, pp. 168166–168176, 2020, doi: 10.1109/ACCESS.2020.3021103.
- [5] A. Yahya, "Introduction to steganography," in *Steganography Techniques for Digital Images*, Cham: Springer, 2019, pp. 1–7.
- [6] B. Yang, M. Schumaker, and W. Funk, "DCT based reversible watermarking technique for medical images with improved quality of watermarked image," *Journal of Critical Reviews*, vol. 7, no. 5, Sep. 2020, doi: 10.31838/jcr.07.05.255.
- [7] R. Zhang, S. Dong, and J. Liu, "Invisible steganography via generative adversarial networks," *Multimedia Tools and Applications*, vol. 78, no. 7, pp. 8559–8575, Apr. 2019, doi: 10.1007/s11042-018-6951-z.
- [8] R. Zahmoul and M. Zaied, "Toward new family beta maps for chaotic image encryption," in *2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, Oct. 2016, pp. 4052–4057, doi: 10.1109/SMC.2016.7844867.
- [9] A. Arab, M. J. Rostami, and B. Ghavami, "An image encryption method based on chaos system and AES algorithm," *The Journal of Supercomputing*, vol. 75, no. 10, pp. 6663–6682, Oct. 2019, doi: 10.1007/s11227-019-02878-7.
- [10] I. Goodfellow *et al.*, "Generative adversarial networks," *ACM*, vol. 63, no. 11, pp. 139–144, Oct. 2020, doi: 10.1145/3422622.
- [11] Y. Zhang, R. Jia, H. Pei, W. Wang, B. Li, and D. Song, "The secret revealer: generative model-inversion attacks against deep neural networks," in *2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, Jun. 2020, pp. 250–258, doi: 10.1109/CVPR42600.2020.00033.
- [12] M. N. Minaidi, C. Papaioannou, and A. Potamianos, "Self-attention based generative adversarial networks for unsupervised video summarization," in *2023 31st European Signal Processing Conference (EUSIPCO)*, Sep. 2023, pp. 571–575, doi: 10.23919/EUSIPCO58844.2023.10289808.
- [13] T. Miyato and M. Koyama, "Generative adversarial network (GAN)," in *Computer Vision*, Cham: Springer, 2021, pp. 508–513.
- [14] R. Zhang, P. Isola, A. A. Efros, E. Shechtman, and O. Wang, "The unreasonable effectiveness of deep features as a perceptual metric," in *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition*, Jun. 2018, pp. 586–595, doi: 10.1109/CVPR.2018.00068.
- [15] W. Sirichotedumrong, T. Maekawa, Y. Kinoshita, and H. Kiya, "Privacy-preserving deep neural networks with pixel-based image encryption considering data augmentation in the encrypted domain," in *2019 IEEE International Conference on Image Processing (ICIP)*, Sep. 2019, pp. 674–678, doi: 10.1109/ICIP.2019.8804201.
- [16] M. Li, D. Lu, Y. Xiang, Y. Zhang, and H. Ren, "Cryptanalysis and improvement in a chaotic image cipher using two-round permutation and diffusion," *Nonlinear Dynamics*, vol. 96, no. 1, pp. 31–47, Apr. 2019, doi: 10.1007/s11071-019-04771-7.




- [17] X. Chen, H. Ma, P. Ji, H. Liu, and Y. Liu, "Based on GAN generating chaotic sequence," *Cyber Security. CNCERT 2020. Communications in Computer and Information Science*, 2020, pp. 37–49, doi: 10.1007/978-981-33-4922-3_4.
- [18] M. Singh, N. Baranwal, K. N. Singh, and A. K. Singh, "Using GAN-based encryption to secure digital images with reconstruction through customized super resolution network," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 3977–3984, Feb. 2024, doi: 10.1109/TCE.2023.3285626.
- [19] D. Zhao *et al.*, "High-security and low-complexity OCDM transmission scheme based on GAN enhanced chaotic encryption," *Optics Express*, vol. 30, no. 19, Sep. 2022, doi: 10.1364/OE.465522.
- [20] R. A. Hallman, "Poster EveGAN," in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, Nov. 2022, pp. 3355–3357, doi: 10.1145/3548606.3563493.
- [21] J. Purswani, R. Rajagopal, R. Khandelwal, and A. Singh, "Chaos theory on generative adversarial networks for encryption and decryption of data," *Advances in Bioinformatics, Multimedia, and Electronics Circuits and Signals*, 2020, pp. 251–260, doi: 10.1007/978-981-15-0339-9_20.
- [22] R. Xu, J. B. D. Joshi, and C. Li, "CryptoNN: training neural networks over encrypted data," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, Jul. 2019, pp. 1199–1209, doi: 10.1109/ICDCS.2019.00121.
- [23] T. Chuman, K. Kurihara, and H. Kiya, "On the security of block scrambling-based ETC systems against jigsaw puzzle solver attacks," in *2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Mar. 2017, pp. 2157–2161, doi: 10.1109/ICASSP.2017.7952538.
- [24] S. Singh, Y.-S. Jeong, and J. H. Park, "A survey on cloud computing security: issues, threats, and solutions," *Journal of Network and Computer Applications*, vol. 75, pp. 200–222, Nov. 2016, doi: 10.1016/j.jnca.2016.09.002.
- [25] X. Zhang, "Application of knowledge distillation in generative adversarial networks," in *2023 3rd Asia-Pacific Conference on Communications Technology and Computer Science (ACCTCS)*, Feb. 2023, pp. 65–71, doi: 10.1109/ACCTCS58815.2023.00014.
- [26] B. F. -Vajargah, "Image encryption based on permutation and substitution using clifford chaotic system and logistic map," *Journal of Computers*, pp. 309–326, 2018, doi: 10.17706/jcp.13.3.309-326.
- [27] S. Farwa, N. Muhammad, N. Bibi, S. A. Haider, S. R. Naqvi, and S. Anjum, "Retracted: fresnelet approach for image encryption in the algebraic frame," *Applied Mathematics and Computation*, vol. 334, pp. 343–355, Oct. 2018, doi: 10.1016/j.amc.2018.03.105.
- [28] A. A. A. El-Latif and X. Niu, "A hybrid chaotic system and cyclic elliptic curve for image encryption," *AEU - International Journal of Electronics and Communications*, vol. 67, no. 2, pp. 136–143, Feb. 2013, doi: 10.1016/j.aeue.2012.07.004.
- [29] H. Yang, K.-W. Wong, X. Liao, W. Zhang, and P. Wei, "A fast image encryption and authentication scheme based on chaotic maps," *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, no. 11, pp. 3507–3517, Nov. 2010, doi: 10.1016/j.cnsns.2010.01.004.
- [30] S. A. Gebereselassie and B. K. Roy, "Secure image encryption algorithm based on two-level diffusion and hybrid chaotic maps," in *2023 IEEE Silchar Subsection Conference (SILCON)*, Nov. 2023, pp. 1–6, doi: 10.1109/SILCON59133.2023.10404972.
- [31] X. Li and X. Li, "A novel block image encryption algorithm based on DNA dynamic encoding and chaotic system," in *2019 IEEE 4th International Conference on Signal and Image Processing (ICSIP)*, Jul. 2019, pp. 901–906, doi: 10.1109/SIPROCESS.2019.8868638.
- [32] X. Wang, X. Zhu, and Y. Zhang, "An image encryption algorithm based on Josephus traversing and mixed chaotic map," *IEEE Access*, vol. 6, pp. 23733–23746, 2018, doi: 10.1109/ACCESS.2018.2805847.
- [33] C. W. -Bin and Z. Xin, "Image encryption algorithm based on Henon chaotic system," in *2009 International Conference on Image Analysis and Signal Processing*, 2009, pp. 94–97, doi: 10.1109/IASP.2009.5054653.
- [34] L. Xu, X. Gou, Z. Li, and J. Li, "A novel chaotic image encryption algorithm using block scrambling and dynamic index-based diffusion," *Optics and Lasers in Engineering*, vol. 91, pp. 41–52, Apr. 2017, doi: 10.1016/j.optlaseng.2016.10.012.
- [35] X. Wu, B. Zhu, Y. Hu, and Y. Ran, "A novel colour image encryption scheme using rectangular transform-enhanced chaotic tent maps," *IEEE Access*, pp. 1–1, 2017, doi: 10.1109/ACCESS.2017.2692043.

BIOGRAPHIES OF AUTHORS



Ranjith Bhat    earned his Masters of Technology from Nitte University in 2011, India. He earned a Bachelor of Engineering from Visvesvaraya Technological University (VTU), Belagavi, India. He is an Assistant Professor at NMAM Institute of Technology, NITTE (Deemed to be University), Department of Robotics and Artificial Engineering. Also, a Bengaluru-based JAIN university Research Scholar. Artificial intelligence, machine learning, deep learning, and network security are his research areas. He can be contacted at email: ranjithbhat@gmail.com or ranjith.bhat@nitte.edu.in



Raghu Nanjundegowda    earned his Ph.D. from JAIN University, Bengaluru. He received a 2011 Masters of Technology from Nitte University, India. Visvesvaraya Technological University (VTU), Belagavi, India, awarded him a Bachelor of Engineering. In Bengaluru, India, he is an Associate Professor in the Electrical and Electronics Engineering Department of JAIN University. His research areas include artificial intelligence, machine learning, and deep learning. He can be contacted at email: raghu1987n@gmail.com or n.raghu@jainuniversity.ac.in.