Iraqi Journal of Information and Communications Technology(**IJICT**)
Vol. 7, Issue 2, August 2024

www.ijict.edu.iq

ISSN:2222-758X
e-ISSN: 2789-7362

GANS FOR IMAGE SECURITY APPLICATIONS: A LITERATURE REVIEW

Mays Y. Mhawi [1], **Hikmat N. Abdullah** [2], **Axel Sikora**[3]
[1,2] Department of Information and Communications Engineering,College of information Engineering ,Al-Nahrain University, Jadriya, Baghdad, Iraq.
[3] University of Applied Sciences, Offenburg, Germany.
mais.yousif@coie-nahrain.edu.iq[1], hikmat.abdullah@nahrainuniv.edu.iq[2]
axel.sikora@hs-offenburg.de[3]
Corresponding Author: **Axel Sikora**

Received:01/08/2024; Revised:25/08/2024; Accepted:29/08/2024
DOI:**10.31987/ijict.7.2.296**

***Abstract*- Generative Adversarial Networks (GANs) have earned significant attention in various domains due to their generative model's compelling ability to generate realistic examples probably drawn from sample distribution. Image security indicates the process of protecting digital images from unauthorized access, modification, or distribution. This requires a guarantee of image privacy, integrity, and authenticity to prohibit them from being exploited by malicious attacks. GANs can also be utilized for improving image security by exploiting its generation ability in encryption, steganography, and privacy-preserving tech-niques. This paper reviews GANs-based image security techniques providing a systematic overview of current literature and comparing the role of GANs in image encryption, image steganography, and priva-cy preserving from multiple dimensions. Additionally, it outlines future research directions to further explore the potential of GANs in addressing privacy and image security concerns.**

***keywords:* Generative Adversarial Networks, Machine Learning, Image Security, Image Encryption, Fake Images.**

I. Introduction

Generative adversarial networks (GANs) were introduced as a potent class of generative models and have become a prominent subject in artificial intelligence in recent years [1]. GANs are unsupervised learning algorithms that construct two neural networks competing in a zero-sum game with each other. While the objectives of GANs network vary, the general goal is to generate data samples P_g that are similar to the data distribution P_{data}. GANs are extensively used in image and video processing and have achieved magnificent improvements in the last few years. In the GANs framework shown in Fig.1, there are two connected networks: Generator (G) and Discriminator (D). The generator generates an image started from random noise and presents it to the discriminator which is a binary classifier that assigns a label as real or fake. The discriminator's output probability indicates how far / close of generated image (fake) is from the real image which is used to improve the generator by accordingly updating the weights of the generator. By refining the generator, the discriminator needs to improve itself during the next training phase, so it cannot uniquely depend on current features any-more. Consequently, both networks continue to improve each other until the generator produces images that are indistinguishable from real images. The generator and discriminator neural networks are denoted by the following two functions, $G(z)$ and $D(x)$ respectively. The overall value function $V(G,D)$, which encompasses both Discriminator loss $L^{(D)}$ and Generator loss $L^{(G)}$, is defined as [2]:

$$\min_G \max_D V(G,D) = \mathbb{E}_{x\sim p_{\text{data}}(x)}[\log D(x)] + \mathbb{E}_{z\sim p_z(z)}[\log(1 - D(G(z)))] \quad (1)$$

Where D is trained to maximize the probability of assigning $x \sim p_{\text{data}}$ with label 1 and $x \sim p_{\text{g}}$ with label 0 whereas G is trained to minimize the probability of producing samples classified as fake $(\log(1 - D(G(z))))$. The main idea in the training process of GAN is that G completely depends on the features D has learned. D is always leading, after it gleans a feature, this will also be passed on to G. Only just when the discriminator allows, the generator can become good [2].

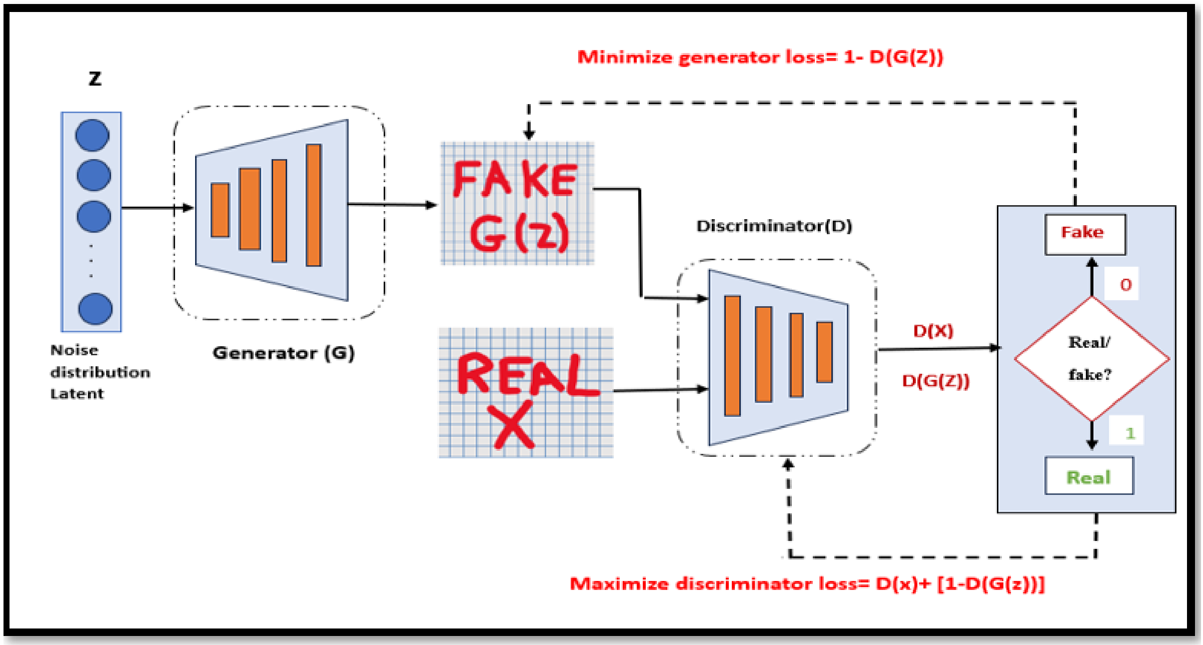
Minimize generator loss= 1- D(G(Z))
Z
Noise distribution Latent
Generator (G)
FAKE G(z)
REAL X
Discriminator(D)
D(X)
D(G(Z))
Fake
0
Real/ fake?
1
Real
Maximize discriminator loss= D(x)+ [1-D(G(z))]

Figure 1: GANs framework.

This paper has collected the latest works and has organized them according to the specific use of GANs in security applications. The contribution of this review paper lies in its comprehensive synthesis of existing research on utilizing GANs for image security. By examining key topics such as image encryption, steganography, and privacy preservation. It offers valuable insights into the current trends, advantages, effectiveness, and limitations in this domain. Through its systematic organization and analysis, it also provides a solid foundation for guiding future research directions and establishing a coherent knowledge base in this rapidly evolving field. The remainder of this paper is structured as follows: Section II introduces the recently existing works according to the different roles of GANs. Section III discusses the advantages and limitations of existing methods and suggests directions for future work. Finally, section IV presents the review conclusions.

II. ROLE OF GANs IN FUNDAMENTAL SECURITY TECHNIQUES

Recently, there has been a growth in digital communication and a necessity for exchanging a lot of private and sensitive information in cyberspace. Image is one of the important resources for using information in many fields such as medical image processing, military applications, and others. The use of these images over the internet will not be secure. Therefore, there is a need for image security because these applications need to control and oversight access to images and provide the means to verify the integrity of images. GANs are widely used in the field of image security and can demonstrate noteworthy performance improvements. Security is a principal task for all the network environments which means an illegal party with prior knowledge cannot learn exact information in plain image through cipher images. Therefore, Security is the major task for any system to maintain confidentiality, integrity, and image authenticity [3]. Specifically, these studies fall into the role of GAN in three domains:(1) efficient image encryption (2) image steganography (3) privacy pre-serving of images.

The role of GANs for efficient image encryption includes GANs for key generation and GANs-based style transfer for image encryption. In these missions, the main role of GANs is that of data generation, the purpose of which is to generate data with distribution similar to the real data required by the target system. In image steganography, due to the adversarial nature between the generator and discriminator of GANs which is similar to the game between steganalyser and steganographer, GANs can be introduced in hiding strategies such as cover modification, cover selection, and cover synthesis. Image privacy issues have become a serious problem due to GANs's ability to generate realistic images and ensure the protection of private details, GANs have paved the way for solving privacy issues such as face anonymization, synthetic content generation (GANs-based content), and image transformation to visually protected domain.

A. *GANs for efficient image encryption*

According to the available literature, GANs were used for image encryption in two different ways. The first way was for secret key generation while the second was for style transformation. Table I summarizes Comparative Roles of GANs in Image Encryption.

TABLE I
Comparative Roles of GANs in Image Encryption.

Aspect	Purpose	Mechanism	Key features
GANs-based secret key generation	- To generate private keys for image encryption.	- A generator is used to create secret keys and a discriminator is to validate their security.	- High dimensional space for key generation. - Randomness ensures unpredictability.
GANs-based style transformation	- Cycle GAN is utilized to transfer the image from its original domain into the target domain. - Training network parameters are considered as secret keys for encryption / decryption.	- The encryption network G is used to encrypt the original input image. - The decryption network F is used for restoring the encrypted image to the original one. - The discriminator D is mainly designed to improve the performance of the encryption network.	- Enables reversible transformations for decryption. - Enable encryption between unpaired domains. - Cycle GAN improves the quality of decrypted images using cycle consistency loss.

1. GANs-based secret key generation In terms of an image encryption scheme, the generation of random keys is critical in the cryptosystem. Fig.2 shows how GANs can be used as learning networks trained to generate encryption keys with best-expected performance as designed. Researchers below exploit the optimum use of GANs to securely and automatically generate secret keys with sufficient key space and strong sensitivity used for image encryption. Ding et. al. [4] introduced a new approach called Deep KeyGen, which used deep learning (DL) to generate a private key. The key generation network, based on GANs, learned how to transform an initial image into the private key which could then be used for encrypting and decrypting of images. Experimental results and security analysis on generated key and encrypted image demonstrated that the stream cipher generated by GANs had high randomness, one-time bad, large key space, and high sensitivity. It also showed robustness against different at-tacks. Despite, this work's optimistic results, it also came with the shortcoming of increasing the computation time of key generation. Therefore, it is essential to balance the tradeoff between security and efficiency of private key generation. Man et. al. [5] introduced learning random number generators for image encryption using Least Squares GAN (LSGAN) trained on six chaotic systems with different dimensions. A scrambling method and a converge diffusion algorithm were proposed to improve the security of encrypted images. The experimental results showed that LSGAN could generate random numbers that could pass all randomness tests to improve the security of encrypted images. Nevertheless, the proposed work still needs to be further im-proved related to key sensitivity by strengthening the relationship between plain text image and generated key. K. L. Neela et. al. [6] presented a Blockchain Chaotic Deep GAN Encryption Scheme that aimed to securely store and protect large medical image reports in the cloud. The confusion and a diffusion process after producing the secret key using GANs were done. Security analysis showed that the proposed scheme had a large key space, pseudo randomness, and high sensitivity. This scheme also provided good encryption performance related to differential analysis, statistical analysis, and similarity analysis. In the encryption phase, XOR is the only method used for image encryption. However, this may not offer a sufficient level of security, especially against advanced cryptographic attacks because of its simplicity and vulnerability to attacks.

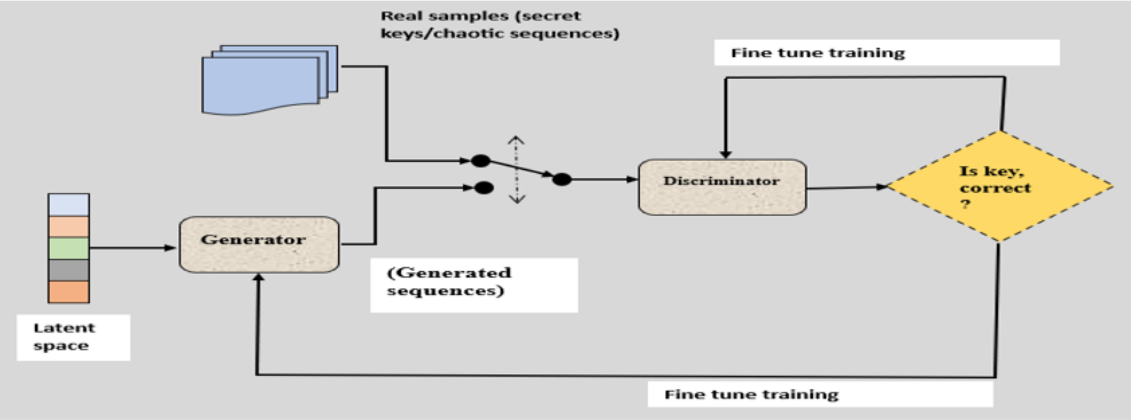

Figure 2: Block diagram of random number generation scheme based on GANs.

Singh et. al. [7] proposed a robust image encryption scheme that used cryptography to protect digital imag-es during transfer with encryption keys generated from GANs trained on the Logistic Maps. The encryption scheme performed operations at the bit level and byte level to increase the difficulty of image decryption. Due to the use of GANs, the generated key passed the NIST test suite, chi-square test, and runs test. This scheme also offered promising resistance against potential attacks. Despite this, it was essential to conduct a more complete analysis of time cost in terms of key generation, image encryption, and decryption process. Fang et. al. [8] developed an algorithm for block image encryption. By the combination of GANs and a hyperchaotic system, a key stream with high randomness and high complexity was obtained. A new block image encryption algorithm was constructed by using a neural network operation mechanism and improved generalized Feistel structure. The security of this algorithm was analyzed quantitatively and qualitatively. The experimental analy-sis demonstrated that the proposed algorithm had a large key space, high robustness, and high key sensitivity. Nevertheless, the combination of GANs and chaotic systems needed to be prepared in advance which would take time. Therefore, the algorithm still needs to be further improved to enhance the network efficiency and meet the needs of practical applications. Singh et. al. [9] proposed a GAN-based encryption method for secur-ing digital images. For image encryption, a random sequence generator using GANs with multiple chaotic sys-tems (cross-coupled logistic and HÃ©non map) was generated. After that, the encrypted image was down-sampled and sent to the receiver which is reconstructed by a customized super-resolution network (CSRNet). This scheme achieved lower time costs and good reconstruction performance. Furthermore, this work resisted differential attacks and brute force attacks with high sensitivity to encryption keys.

Kumar et. al. [10] presented a novel medical image encryption and compression method. GAN-based DeepKeyGen architecture was utilized to generate a fake image used as an initial key. Henon map and hash-based equation were used to further improve the security of the initial key image generated by GAN. To encrypt and compress the original medical image, Henon map, Mersenne Twister (MT), XOR-based algorithm, and DHC were used before being sent to the receiver. Different performance metrics such as key space, key sensitivity, statistical analysis, similarity analysis and differential analysis were performed. Despite an encryption time may not be considered excessive, it still needs an improvement in this scenario, especially in real-time applications or high-speed encryption is required. Zhang et. al. [11] proposed color image encryption scheme-based GANs. In this work, GANs were trained on the hyperchaotic Chen system for producing a key image related to the original plain text image. Depending on the produced key image, the image was encrypted in three steps: pixel-level substitution, scrambling, and diffusion. The performance analysis of the proposed system showed robustness against different attacks. The GANs could significantly expand key space, randomness, and sensitivity. It was essential to conduct a more complete analysis of time cost in terms of key generation, image encryption, and decryption process. Table II summarizes the encryption schemes based on GANs for key generation with their performance analysis.

2. GANs-based style transformation Due to properties of deep learning such as its nonlinear structure and ability to learn [12], many researchers put their effort into the combination of deep learning with image encryption based on image style transfer as shown in Fig.3. The different approaches to image encryption, that adopted GANs as learning networks, have been categorized as follows:

a. Image encryption/ decryption using cycle GAN In recent, deep-learning-based image encryption techniques have gained extensive attention due to their great potential in dealing with issues of conventional encryption. In image encryption/decryption networks based on deep learning, the network of cycle GANs is extensively adopted as a learning

TABLE II
Key generation GAN-based image encryption schemes.

Ref. No.	**Tools & approaches**	**Analysis of encryption keys**	**Performance analysis of image encryption scheme**	**Time cost analysis**
[4]	GAN is used to generate a private key for image encryption.	-Key space -One time pad -Entropy, Histogram analysis -Sensitivity analysis (NPCR, UACI)	-Statistical analysis (entropy, histogram,correlation) -Similarity analysis (MSE, SSIM) -Differential analysis (NPCR, UACI)	-key generation time
[5]	Key generated by LSGAN for image encryption.	-statistical analysis of key (Entropy, histogram) -Randomness analysis (NIST) -Key space	-Statistical analysis (entropy, histogram, correlation) -Similarity analysis (PSNR, MSE) -Differential analysis (NPCR, UACI) - Robustness analysis against (noise, cropping)	-Key generation time -Encryption time - Decryption time
[6]	Deep GAN produces keys utilized as input to encrypt medical images.	-key space -Entropy, histogram analysis -sensitivity analysis (UACI, NPCR)	Similarity analysis (MSE, SSIM) -Statistical analysis (normalized correlation) -Differential analysis (NPCR, UACI)	- Encryption time - Decryption time
[7]	Key generated by GAN trained on logistic map.	-key space -NIST SP 800-22 -Chi-square test (CST) -Run test (RT)	- visual analysis (visual inspection) -Statistical analysis (correlation coefficients, histogram analysis) -quantitative analysis (MSE, PSNR, SSIM, entropy, BER) - Differential analysis (UACI, NPCR) - Robustness analysis	N/A
[8]	New block image encryption algorithm based on new hyperchaotic system and GAN is proposed	- key space -key sensitivity	- Statistical analysis (histogram, variance,local & global entropies, correlation analysis, gray-level co-occurrence matrix) - Robustness analysis (against noise& cropping, cryptographic attack) -Differential analysis (NPCR, UACI)	Execution time
[9]	GAN trained on combination of Logistics and a Henon map for secret key generation	-key space -key sensitivity	-Statistical analysis (entropy, histogram, correlation, chi-square test) -Differential analysis (NPCR, UACI)	-Encryption time -Decryption time
[10]	Novel model based on GAN and chaotic for image encryption	-key space -key sensitivity	tatistical analysis (entropy, histogram, correlation) - Similarity analysis (PSNR, -Differential analysis (NPCR) - Robustness analysis (against noise/occlusion)	Encryption time
[11]	GAN is used to generate key image trained on hyperchaotic Chen system	-Key space, Entropy, NIST -Sensitivity analysis UACI)	-Statistical analysis (histogram, entropy, Correlation) - Robustness analysis (against against cropping)	N/A

network where parameters obtained after the training network are considered secret keys for encryption and decryption. Style transfer methodology based on cycle GAN consists of an encryption network that is converted into a target domain which is regarded as a hidden factor to realize encryption and becomes ciphertext images, a decryption network that is used to recover the original one, and a discriminator network is used to confirm the generated image similar to the target or not and penalizes the encryption/decryption network accordingly. The works below exploit cycle GAN for image encryption schemes in the medical field. Ding et. al. [13] exploited the image-to-image transformation field to design a novel medical image encryption and decryption network (DeepEDN). Cycle GAN was utilized as the main learning network to transfer the image from its original domain into the target domain. The encryption network consisted of a generator network(G) and a discriminator network(D). On the other hand, the decryption procedure by decryption network (F) was the inverse of the encryption process that was used to reconstruct the original image. In this work, a Region of Interest (ROI)-mining network was used to extract interested regions from the encrypted image. In DeepEDN, private keys of encryption were the parameters of the generator network, while the parameters of reconstruction were used as the private keys for decryption. Security analysis of this work demonstrated a high-security level with good efficiency. Panwar et. al. [14] developed an efficient image encryption/decryption system based on deep learning. This system was designed based on the cycle-GAN network for medical applications which consisted of the encryption network (a feature encoder, a transformation module, and a feature decoder), discriminator network, and decryption network. The loss function employed structural similarity index metrics (SSIM) to train the encryption/decryption network that helped to generate a cipher image similar to the target cipher image and recovered an image similar to the original image concerning contrast, luminance, and structure. The extensive results of the proposed model demonstrated high-security resistance and high-quality recovered images with large key space due to a large number of training parameters.

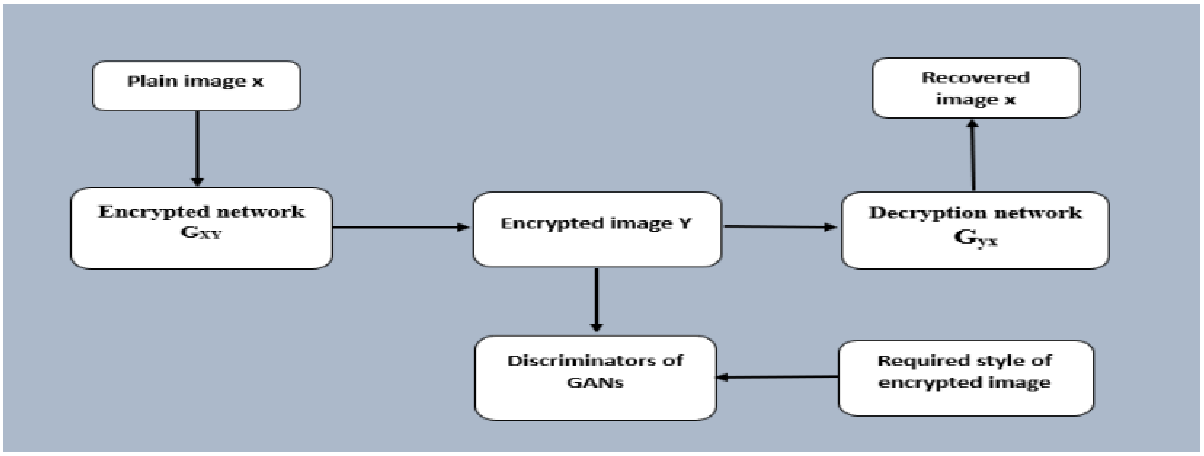

Figure 3: GAN-based style transfer for image encryption.

b. Visually meaningful image encryption using cycle GAN In a visually meaningful image encryption scheme (VMIE), the plain text image is encrypted and embedded into a cover image to achieve both content and visual protection. Recently, a visual image encryption scheme integrated with deep learning has been used for protection content and visual security using GAN which enables image translation from the ciphertext domain into the plain text domain without needing to embed the secret image in any carrier image as in the traditional (VMIE). The researchers below exploit GAN to visualize the encryption of images with high reconstruction quality. Liu et al. [15] presented a learning visual image encryption scheme based on cycle GAN and compressive sensing (CS). This work aimed to protect content security as well as focused on ensuring visual security. The sparse image was compressed by CS and then this compressed image was permuted and diffused to obtain ciphertext using the Henon map. Finally, cycle GAN was used to obtain visually meaningful encrypted images. This encryption scheme showed improvement in time efficiency and reconstruction quality.

c. Thumbnail-preserving encryption using cycle GAN (TPE-GAN) Thumbnail-preserving encryption (TPE) was proposed as a way to balance the privacy and usability of images. In TPE, the cipher image is similar to a low-resolution form of the plain image, in which a legal user with prior knowledge can preview the content of the original image with rough visual information, while the illegal user can only access vague version, thus protecting the image privacy [16]. Chai et. al. [16] proposed thumbnail-preserving encryption based on cycle GAN (TPE-GAN) which was used to simulate randomized unary encoding (RUE) to make a balance between the quality of the encrypted image and the usability of the cipher image. TPE-GAN consisted of two steps: cycle GAN-based encryption network and decryption network with a key in which binary string was used as key instead of using decryption network parameters to facilitate encrypted image sharing. Table III summarizes the encryption schemes based on GANs for style transfer with their performance analysis.

TABLE III
Style transfer GAN-based image encryption schemes.

Ref. No.	**Tools & approaches**	**Analysis of secret keys**	**Performance analysis of image encryption scheme**	**Quality of recovered image**	**Time cost analysis**
[13]	Medical image encryption /decryption using cycle GAN	-key space -key randomness -key sensitivity	-Histogram analysis - Entropy analysis -security analysis under different adversary models -security analysis under different attack models	-PSNR -SSIM	Speed of encryption & decryption process
[14]	Medical image encryption /decryption using cycle GAN	-key space -key sensitivity	-Histogram analysis - -Information entropy -Correlation analysis	PSNR	N/A
[15]	Visual image encryption using cycle GAN	-key space -key sensitivity	- Ciphertext security analysis (entropy, histogram, correlation) - Decryption quality analysis (PSNR, SSIM) -Differential attack analysis (NPCR, UACI) -Noise attack analysis	-PSNR -SSIM	-Encryption time -Decryption time -Total time
[16]	Thumbnail consistency loss to improve visual usability of cipher image using cycle GAN	-key space -key sensitivity	SSIM loss to improve the quality of decrypted images	SSIM	N/A

B. *GANs for Image Steganography*

Image steganography is a technique used to embed secret information in a cover image to generate a stego image in such a way that the hidden data is not visible to the human eyes [17]. Steganography can be characterized by three sides that are related to each other: security, capacity, and robustness [18]. GANs provide an opportunity for merging Deep Learning and image steganography due to the adversarial nature between the generator and discriminator [19]. Researchers below exploit the potential capability of introducing GANs into image steganography models to expand embedding capacity and improve the security and stego image quality performance. Qi et. al. [20] proposed a novel image steganography scheme that hid an encrypted image into a grayscale cover image to solve the problem of color distortion in the color image. Chaotic encryption technology was used to encrypt the secret image solving the problem of secret information loss. This encrypted image was then merged with the cover image by a convolutional neural network (CNN) to produce a stego image. In this work, GAN was used to generate a more realistic steg image and there was no evident appearance difference between the cover image and stego image. From the experimental results and analysis, this approach preserved high embedding capacity with advantageous high values of steg image quality measures. Zhangjie et. al. [19] presented a secure steganography model for hiding secret images via GAN called HIGAN. It consisted of three sub-networks: the encoder network which hid a secret color image into a color cover image with the same size. Decoder network where the secret image was extracted. The discriminator network was used as a steganalysis model. The adversarial training between the encoder-decoder network and discriminator network was used to improve the security of steganographic images. The extensive result of this work achieved high visual quality steganographic images with strong security. Yuan et. al. [17] inspired a novel image steganography scheme called ADF-IS (Attack and Deep Fusion for Image Steganography). In the proposed scheme, the secret information was embedded in the cover image for high security without compromising imperceptibility. Four modules were used to achieve that: The attack module conducted by UAN (universal adversarial network) to enhance the security of image steganography, the Encoder module was adopted as the generator for imperceptible embedding with high payload, the Decoder module to recover embedded information and Critic module was designed for adversarial training. Experimental results verified that this scheme achieved better performance in security due to the advantageous use of universal adversarial perturbations. Peng et. al. [21] presented medical image adaptive steganography with a generative adversarial network named MedSteGAN. In this work, the generator network was reconstructed using the U-shaped architecture and used multiple convolutions with different kernel sizes to improve feature extraction capability. To improve stego image quality, the loss function was optimized by incorporating visual quality loss based on multi-scale structural similarity index metric (MS-SSIM) and the high-frequency MSE loss. Experimental results showed that MedSteGAN outperformed other steganographic methods in the security-quality domain. Wang et. al. [22] proposed novel GAN-based steganography to improve security performance by learning better embedding probability maps. A novel attention mechanism was introduced into U-Net architecture that made the generator focused on texture-rich regions of input images. Moreover, dual-stream input consisting of a cover image and an enhanced image, was introduced to improve the generatorâs ability to learn structural features from input images. In order to simplify information flow between different layers, different skip connection was used to connect feature maps between the contraction path and expansion path, maintaining structural information and details of images. Extensive experimental results showed that this approach learned better-embedding probability maps and improved security performance against various steganalysis attacks. At the same time, the computational efficiency of this work needs to be further improved. Table IV summarizes the encryption schemes based on GANs for image steganography.

TABLE IV
GAN-based image steganography schemes.

Ref. No.	Tools & approaches	Security Analysis	Stego Image Quality	Computational efficiency
[20]	Chaos encryption and GAN to improve image steganography	-Payload capacity	-PSNR -SSIM	N/A
[19]	HIGAN for secure image hiding	-Detection accuracy	-PSNR -SSIM	N/A
[17]	Enhancing security of GAN-based image steganography via UAI and pixel-wise deep fusion	-Payload -Detection accuracy	-PSNR -SSIM PSNR-HVS PSNR-HVSm	N/A
[21]	Medical image steganography with GAN named MedSteGAN	-Detection error rate	-PSNR -SSIM	N/A
[22]	Novel GAN based image steganography	-Average detection accuracy	N/A	Training time

C. *Image Privacy Preserving using GANs*

Privacy-preserving using GANs is a rapidly progressive field at the intersection between privacy protection and deep learning. GANs have paved the way for innovative techniques to solve privacy problems in various applications such as face anonymization, Synthetic content generation (GAN-based content), and image transformation to visually protected domains and thus generate visually protected images. Fig.4 shows the model of the image privacy-preserving method using GAN-based content generation. Researchers below exploit the potential capability of GAN and develop an effective way to compromise between privacy protection and image utility.

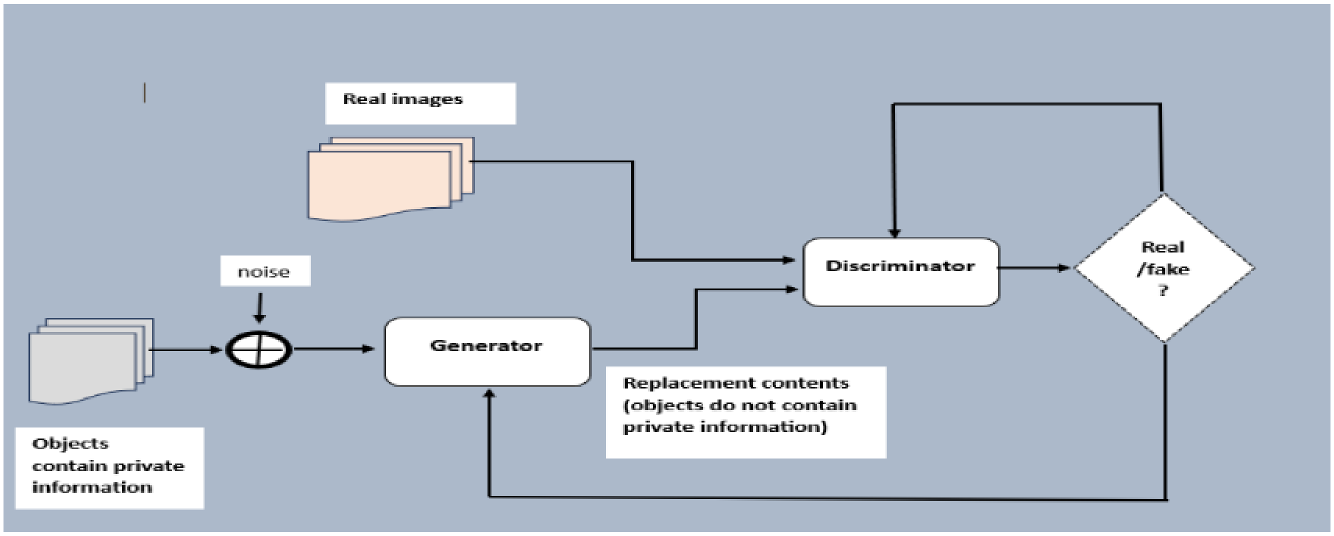

Figure 4: Image privacy-preserving method using GAN-based content generation.

Yu et. al. [23] used the synthetic content generated by GAN to protect the sensitive personal content of images in IoMT devices. The framework consisted of three stages to achieve the goal of image privacy preservation: Convolutional Neural Network (CNN) networks were used to detect various objects in images and classify them as private or public. Then GAN-based content generation was used where style GAN could generate content that was not much different from real images (De-Identification). After de-identified content had been generated by GAN, the generated content was replaced with the original private object images. Privacy protection and image utility metrics demonstrated that the scheme protected privacy while preserving image utility by using the combination of GAN with differential privacy (DP). Chen et. al. [24] proposed a face anonymization model based on GAN while preserving the utility of images. There were three parts in this work: Detection module (for attribute labels extraction of both the original images and the protected images), Fake image creation module using DCGAN, and Image transformation module (for matching attributes in the original image with the fake images). The results demonstrated that the proposed scheme achieved balancing the need for privacy-preserving and image utility. Warit et. al. [25] utilized Cycle-consistent adversarial networks (Cycle GAN) to produce visually protected images for privacy-preserving image classification. From the experimental results, the proposed scheme demonstrated its ability not only to maintain high classification accuracy of DNN but also to have high resistance against attacks by using a transformation network for the protection of training and testing images in DNN. Mahmoud et. al. [26] proposed an intelligent anonymity platform using the Conditional Identity Anonymization Generative Adversarial Network (CIAGAN) model. Their models suggested a new swapping face strategy, benefited from the decoder and encoder architecture, and used adversarial training. CIAGAN proved its ability to generate anonymous face images with important attributes to the difficult recognition of specific objects. Table V summarizes the encryption schemes based on GANs for privacy-preserving.

TABLE V
GAN-based privacy preserving schemes.

Ref. No.	**Privacy-preserving approaches using GAN**	**Evaluations metrics**	
		Privacy Protection Metrics	**Image utility metrics**
[23]	Synthetic content generation by GAN	-Distance between original image and protected image -Confidence score	-L_0: The number of changed pixels -L_2: Euclidean distance between original image image and protected image -ALD_P: The average L distance between the images -SSIM: Similarity between original image and protected image -Dhash: The degree of modification
[24]	Face anonymization using GAN	Euclidean distance between original image and final protected image	Accuracy
[25]	Image transformation using GAN to generated visually protected image	SSIM (lower value mean lower visual information)	Accuracy
[26]	Face anonymization using GAN	-FID -Precision -Recall -F1-score	-PSNR -SSIM

III. ANALYSIS AND FUTURE TRENDS

Today in the digital era, image security is a critical concern. In this context, this paper focuses on exploring the use of GANs for the image security field and highlights the different applications of GANs that have been developed. It is imperative to understand the capabilities and limitations of GANs in this field which can smooth the way for new advancements in protecting and securing digital images in several domains. Table VI presents a relatively comprehensive analysis of GANs in image security techniques. This analysis can provide researchers with a comprehensive idea of the methods to be used in further studies. GAN-based image security techniques are still in the early stage of development which presents many research opportunities. Most of these come from the algorithm training itself. In image encryption/decryption networks based on GAN, possible research directions are a modification in the architecture of GANs models to enhance the performance of the security system, as well as how to identify the best loss functions to get a good quality of encrypted images and recovered images that capture full details, especially in medical image field. The experiments showed that providing additional information can improve security performance. For example, in image steganography [22], the generator may adopt dual stream to improve its ability to learn more accurate embedding probability maps making the structure of the model more complex and the training time is increased. Therefore, future research should explore an efficient approach to obtain better embedding probability maps while keeping training time within acceptable range. In [27], GANs can also be used to solve the inverse kinematics (IK) problem of 3DOF redundant robot arm.

IV. CONCLUSION

GANs are one of the evolution directions in fields of image security which provide a new way to resolve many security issues related to image encryption, image steganography, and image privacy preservation where GANs have shown their effectiveness in these techniques, exhibit their capabilities to enhance the overall security of images. In GANs approaches for key generation (Table II), the statistical analysis of keys along with NIST randomness tests, consistently demonstrated that GANs are a powerful technique to generate keys with high security. Furthermore, key space analysis emphasizes GANs's ability-based methods to generate keys within a sufficiently large and complex space. These findings substantially indicate that GANs show a promising approach for key generation securely and efficiently. In Table III, the style transfer approaches show the versatility of GANs in image encryption, allowing for flexible and visually appealing transformations without compromising security. These results highlight the strong cryptographic properties of encryption keys, which are the network parameters, making them resistant against attacks. The analysis of encryption quality utilizing metrics like [PSNR, SSIM, NPCR, and UACI], demonstrates that GAN-based image encryption offers a high level of security and preserves decrypted image quality, especially in applications where fidelity is paramount. Table IV looked into GANs in image steganography applications, examining their impact on stego image quality, security analysis (such as Payload and Detection accuracy), and computational efficiency (training time). GANs exhibit an encouraging approach to embedding information within images while preserving both visual quality and security, making them a good alternative to traditional steganographic methods.

GANs have opened new ways for advanced approaches to address privacy concerns across various applications, including

TABLE VI
Analysis of reviewed papers.

Security Technique	Roles of GANs	Advantages	Limitations
Image encryption	-Generate encryption key	-Expand key space, key randomness, key sensitivity -strong robustness against security attacks	- Increasing computation time of key generation Large storage overhead
	-Cycle GAN based image encryption	-It resists plaintext attacks due to nonlinearity introduced through deep learning -Increase sensitivity to the key change - High quality of recovered image	- The use of only network parameters as secret key for encryption and decryption has a large storage overhead which not conductive to image sharing
	GAN based Visual meaningful image encryption	-Cycle GAN enables image translation from ciphertext domain to plaintext domain -Protecting data security and ensuring visual security at the same time -The secret image is not embedded in any carrier image, so it can effectively resist steganalysis	-time efficiency need to be improved -large storage overhead due to large number of parameters in training network
	- Thumbnail preserving encryption based on GAN	- Use cycle GAN to balance image privacy and usability and improve encryption efficiency -Thumbnail consistency loss and ssim loss are used to improve visual usability of cipher image and quality of decrypted image	-Encryption network correspond to only one target domain
Image steganograph	-GAN is adopted to generate more realistic stego image -GAN is used to enhance automatic learning of embedding cost	-improve stego image quality -high embedding capacity -high security against various steganalysis attacks -hiding the details of secret image perfectly by using skip connection	Time consuming compared with those of conventional steganography work
Image privacy preserving	-Protect sensitive content in images with synthetic content generated by GANs (de-identify with GAN-based content) - GANs-based face anonymization (generate facial image while preserving important attributes) - image transformation to visually protected domain using GANs	-maximum usability of original image while preserving privacy -robustness against attacks -high image quality and uniformity	Efficiency and scalability need to be improved

face anonymization, synthetic content generation (GAN-based content), and image transformation into visually protected domains, ultimately resulting in the creation of secure images. Table V demonstrates the effectiveness of image utility metrics and privacy-preserving metrics has demonstrated their capability in resolving privacy preservation challenges. However, GAN-based image security is still in its preliminary stages, and the optimization of the training process needs to be further explored. Due to its capabilities in generating realistic data, GANs may be extensively used in security applications in the future. To improve the performance of GANs-based security, further exploitation of GANs capabilities, paving the way for future advancements in these areas.

Funding

None

ACKNOWLEDGEMENT

The author would like to thank the reviewers for their valuable contribution in the publication of this paper.

CONFLICTS OF INTEREST

The author declares no conflict of interest

REFERENCES

[1] W. Zheng, K. Wang, and F.-Y. Wang, "GAN-Based Key Secret-Sharing Scheme in Blockchain," in IEEE Transactions on Cybernetics, vol. 51, no. 1, pp. 393-404, Jan. 2021.
[2] C. Hogenboom, "Generation of synthetic Financial time-series with Generative adversarial network,â Research Master thesis, College of Eng. and Sc, Maastricht Univ.,2020.
[3] Madhu B., Ganga Holi, and Srikanta Murthy K., "An Overview of Image Security Techniques," International Journal of Computer Applications, vol. 154, no. 6, 2016.
[4] Y. Ding, F. Tan, Z. Qin, M. Cao, K. -K. R. Choo and Z. Qin, "DeepKeyGen: A Deep Learning-Based Stream Cipher Generator for Medical Image Encryption and Decryption," in IEEE Transactions on Neural Networks and Learning Systems, vol. 33, no. 9, pp. 4915-4929, Sept. 2022.
[5] Z. Man, J. Li, X. Di, et al., "A novel image encryption algorithm based on least squares generative adversarial network random number generator," Multimedia Tools Appl, vol. 80, pp. 27445-27469, 2021.
[6] K. Neela and V. Kavitha, "Blockchain based Chaotic Deep GAN Encryption scheme for securing medical images in a cloud environment," Applied Intelligence, vol. 53, pp. 1-15, 2022.
[7] O. Singh, S. Dhall, A. Malik, and S. Gupta, "A robust and secure immensely random GAN based image encryption mechanism," Multimedia Tools Appl, vol. 82, 2022.
[8] P. Fang, H. Liu, C. Wu, and M. Liu, "A block image encryption algorithm based on a hyperchaotic system and generative adversarial networks," Multimedia Tools Appl, vol. 81, 2022.
[9] 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," in IEEE Transactions on Consumer Electronics, vol. 70, no. 1, pp. 3977-3984, Feb. 2024.
[10] P. Kumar, M. Rahman, S. Namasudra, et al., "Enhancing Security of Medical Images Using Deep Learning, Chaotic Map, and Hash Table," Mobile Netw Appl, 2023.
[11] Zhang, R., Kang, X., Lu, Q. et al. "A plaintext-related image encryption scheme based on key generation using generative adversarial networks". Multimedia Tools Appl (2024).
[12] Panwar, Kirtee Kukreja, Sonal Singh, Akansha Singh, Krishna. (2023). "Towards Deep Learning for Efficient Image Encryption". Procedia Computer Science. 218. 644-650. 10.1016/j.procs.2023.01.046.
[13] Yi Ding, Guozheng Wu, Dajiang Chen, et al., "DeepEDN: A Deep-Learning-Based Image Encryption and Decryption Network for Internet of Medical Things," in IEEE Internet of Things Journal, vol. 8, no. 3, pp. 1504-1518, 1 Feb.1, 2021.
[14] K. Panwar, A. Singh, S. Kukreja, K. K. Singh, N. Shakhovska, and A. Boichuk, "Encipher GAN: "An End-to-End Color Image Encryption System Using a Deep Generative Model," Systems, vol. 11, no. 1, p. 36, 2023.
[15] Liu, Z., Xue, R. Visual image encryption based on compressed sensing and Cycle-GAN. Vis Comput 40, 5857â5870 (2024).
[16] X. Chai, Y. Wang, X. Chen, Z. Gan, and Y. Zhang, "TPE-GAN: Thumbnail Preserving Encryption Based on GAN With Key," IEEE Signal Processing Letters, vol. 29, pp. 972-976, 2022.
[17] C. Yuan, H. Wang, P. He, et al., "GAN-based image steganography for enhancing security via adversarial attack and pixel-wise deep fusion," Multimed Tools Appl, vol. 81, pp. 6681â6701, 2022.
[18] Hikmat N. Abdullah, Sura F. Yousif, Alejandro A. Valenzuela, "Efficient Steganography Scheme for Color Images Based on Wavelets and Chaotic Maps", Iraqi Journal of Information and Communication Technology (IJICT), Iraq, ISSN 2222-758X, Vol.2, Issue 4, pp.1-10, December 2019.
[19] Z. Fu, F. Wang, and X. Cheng, "The secure steganography for hiding images via GAN," J Image Video Proc., vol. 46, 2020.
[20] Qi Li; Xingyuan Wang; Xiaoyu Wang et al., "A Novel Grayscale Image Steganography Scheme Based on Chaos Encryption and Generative Adversarial Networks," in IEEE Access, vol. 8, pp. 168166-168176, 2020.
[21] Y. Peng, C. Fu, Y. Zheng, et al., "Medical steganography: Enhanced security and image quality, and new S-Q assessment", Signal Processing, Volume 223, 2024,109546, ISSN 0165-1684.
[22] D. Wang et al., "GAN-based adaptive cost learning for enhanced image steganography security", Expert Systems with Applications, Volume 249, Part A, 2024, 123471, ISSN 0957-4174.
[23] Yu J, Xue H, Liu B, et al., "GAN-Based Differential Private Image Privacy Protection Framework for the Internet of Multimedia Things". Sensors. 2021; 21(1):58.
[24] Zhenfei Chen, Tianqing Zhu, Ping Xiong et al., "Privacy preservation for image data: A GAN-based method", International Journal of Intelligent Systems, 36, 2021.
[25] W. Sirichotedumrong and H. Kiya, "A GAN-Based Image Transformation Scheme for Privacy-Preserving Deep Neural Networks," in 2020 28th European Signal Processing Conference (EUSIPCO), 2020, pp. 745-749.
[26] M. A. Al-Khasawneh and M. Mahmoud, "Safeguarding Identities with GAN-based Face Anonymization", Eng. Technol. Appl. Sci. Res., vol. 14, no. 4, pp. 15581â15589, Aug. 2024.
[27] H. Z.Khaleel and A. J. Humaidi, "Towards accuracy improvement in solution of inverse kinematic problem in redundant robot: A comparative analysis". International Review of Applied Sciences and Engineering, 15(2), 242-251,2024.