Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Gamma Statistic Kakutani Fixed Point and Equilibrium Generative Adversarial Network Based Secure Steganography

Gahan A V*, Geetha D Devanagavi
*School of Electronics and Communication Engineering, REVA University, Bengaluru, 560064, India, E-mail: gahanbit@gmail.com, https://orcid.org/0000-0003-2252-5302
School of Computing and Information Technology, REVA University, Bengaluru, 560064, India, E-mail: dgeetha@reva.edu.in, https://orcid.org/0000-0002-7788-5615

ARTICLE INFO

Received: 18 Dec 2024
Revised: 10 Feb 2025
Accepted: 28 Feb 2025

ABSTRACT

Images have been frequently utilized as ideal conditions for hiding information through the employment of steganography algorithms. The information for hiding ranges between documents digitization, other secret image where hidden data is said to be embedded without the intervention of human. Until now, an abundance of steganography algorithms are found in the state of the art works, as well as steganalysis techniques, dedicated to hidden information detection in files. Present day Steganography algorithms depend on machine learning (ML) and deep learning (DL) for embedding as much as secret text image as probable as reducing visual changes in given input image (i.e., cover image) with improved accuracy. However, the embedding rate and bit error rate was focused minimally. Following this direction, this article endeavors to exemplify that a Generative Adversarial Network (GAN) can be utilized to enhance the potentiality of spatial domain steganalysis method and to position secret text message information with minimal image alteration (i.e., improving the embedding rate and bit error rate) significantly. In this work a method called, Gamma Statistic Kakutani Fixed-point and Equilibrium Generative Adversarial Network-based (GSKF-EGAN) secure steganography is proposed. First, a Gamma Statistic Histogram Equalization-based Preprocessing model is designed by fine tuning gamma coefficient and equalization for both cover image and secret text image to circumvent high peak and ensure optimal illumination simultaneously. Second, Kakutani Fixed-point and Equilibrium Generative Adversarial Network-based Steganography model is design with the processed images as input. Here by employing the Kakutani Fixed-point ensures significant embedding rate during the embedding process and by using Strategic Equilibrium for validation ensures minimum distortion or bit error rate during the extraction process. Also experimental results reveal that retrieved secret message data generated by GSKF-EGAN method with minimum distortion or bit error rate, therefore enhancing retrieved image quality with higher embedding rate than those generated by conventional image Steganography techniques.

Keywords: Image Steganography, Gamma Statistic, Histogram Equalization, Machine Learning, Deep Learning, Kakutani Fixed-point, Equilibrium Generative Adversarial Network.

INTRODUCTION

Over the past few decades, quite a few materials and methods have been designed for information hiding and preserve communication channels in a secure manner. Upon comparison with the cryptography, that concerns to materials and methods where the message is altered with the purpose of making it in indiscernible for undesirable readers, steganography is art of producing data unseen to keep away from being identified through third party. To attain extreme safeguard of a provided data piece, both cryptography and steganography are employed in coexistence, embedding an encrypted messaged to image employing steganographic algorithm.

Support Vector Machine (SVM) and Integer Wavelet Transform (IWT) was proposed in [1].Here, initially, SVM was utilized in is employed primary to segregate RoI from No-Represent in medical image. Following which IWT was appertained with the purpose of embedding secret information inside the non area of interest portion of medical cover image. In addition, circular array as well as shared secret key were applied with objective of improving the robustness in a significant manner. With this type of design resulted in the improvement of PSNR with higher rate of structural similarity and finally minimizing the bit error rate extensively. However, the embedding rate involved in steganography process was not focused. Hitherto, an abundance of steganography techniques are designed in the literature simultaneously with steganalysis techniques, with the idea of detecting hidden information.

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Moreover, contemporary steganography methods depend on CNN to embed as much information as probableas reducing visual transposes in image. With this objective, Generative Adversarial Networks and Genetic Algorithm were designed in [2] to enhance the potentiality of spatial domain steganalysis as well as enclose secret information by nominal image changes. By means of this integrated method resulted in the improvement of true positive rate and accuracy with minimal true negative rate simultaneously.

Despite improvement in terms of accuracy and true negative rate, the bit error rate involved in spatial domain steganalysis was not focused. To address the above said issues, in this work a method called, Gamma Statistic Kakutani Fixed-point and Equilibrium Generative Adversarial Network-based (GSKF-EGAN) secure steganography is proposed.

1.1 Contributing remarks

The contributions of the work include the following:

- A novel Gamma Statistic Histogram Equalization-based Preprocessing model is defined based on gamma coefficient that ingeniously controls high peak from transposing the course of action of histogram statistic. This model in turn improves the contrast and enhances the illumination in a simultaneous manner and engineering magnificent execution in refining both cover image and secret text message with high peak in histogram.
- To propose and implement Kakutani Fixed-point and Equilibrium Generative Adversarial Network-based Steganography algorithm for stego image generation, therefore enhancing visual quality of recuperated image with minimum distortion
- Employ of Kakutani Fixed-point and Equilibrium functions for cover image generation minimizes degradation of image quality from conventional steganography methods, SVM and Integer Wavelet Transform and Generative Adversarial Networks and Genetic Algorithm.
- The performance is evaluated via immense simulations based on BOSSBase v1.0.1 dataset natural image brain MRI image dataset. Compared with Support Vector Machine and Integer Wavelet Transform [1] and Generative Adversarial Networks and Genetic Algorithm [2], our Gamma Statistic Kakutani Fixed-point and Equilibrium Generative Adversarial Network-based (GSKF-EGAN) secure steganography method is comparatively better in embedding quality (i.e., embedding rate , bit error rate), recovered visual quality (i.e., PSNR, SSIM) respectively.

1.2 Organization of the work

The organization of the paper is given as follows. Section 2 presents the secure steganography method review of related literature. Section 3 provides the proposedGamma Statistic Kakutani Fixed-point and Equilibrium Generative Adversarial Network-based (GSKF-EGAN) secure steganography work in detail. The elaborate experimental results and discussionsare detailed in Section 4. The paper concludes in Section 5.

Related works

As emergence of Natural Language Processing (NLP) to research discipline, linguistic Steganography has replaced further categories of Steganography. In [3] the positive features of natural language processing based Markov chain method for generating auto generative cover text was proposed in [3]. To not only ensure information security but also to improve the embedding rateRNN model was pursuedthroughLSTM neural network. Nevertheless, crucial reviews have been heightened concerning the security and privacy aspects.

Deep learning was applied in [4] that improved steganography in ad hoc system by reducing message detection rates significantly. Steganography excels other methods of data security from possible menaces. Steganography is an insurgence where prevailing information compression, data postulation and cryptography evolutions are combined to converge necessitate for data protection over the Internet.

A detailed study and critical analyses by comparing prevailing cover steganography methods were investigated and also valuable results were identified in [5]. The application of image steganography is not only restricted to natural and still images but also are said to be extended in medical domain in which medical data privacy and security account for a paramount matter in question. Also, the medical data confidentiality can be attained by means of encryption and data hiding algorithms. More over with the evolution of quantum computers based on mathematical modeling the data is said to be hacked.

In [6], a novel method for medical image steganography technique. With this type of design resulted not only in the improvement of PSNR but also improving the payload capacity in an efficient manner. Presently, the most eminent method to image steganography to implant payload as reducing an adequately defined distortion.Practitioner's objective here remains in designing a mechanism to attain a method by enhanced empirical statistical detectability.

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Distortion design method based on universal wavelet was proposed for embedding in a random domain in [7].As far as digital communication environment is concerned, securitizing the information is imperative. Three crucial specifications utilized in design procedure of steganography algorithm are fidelity, security as well as payload. Nevertheless, distinct algorithms are executed in information hiding.

In [8], anew steganography method depend on agent technology was presented. Here secure communication was designed based on the steganography framework.Yet another data security mechanism employing learning management system was designed in [9]. In spite of the indestructible existence of color images for communication, several research works have been designed for grayscale Steganography images. However, in [10], a steganographic method involving spatial color images based on associations as well as divergences among color channels was presented. With this the embedding capacity was said to be improved extensively.

With the evolution and advancement of technology, data has highly vulnerable to mishandling as well as exploitation. This resulted in inception of information hiding based on steganography and extraction via steganalysis. In [11] Blind steganalysis method was employed by abstraction of ML embodied into it.

Yet another information hiding method employing semi supervised algorithm focusing on the bit error rate and success rate was designed in [12]. Statistical imaging model was proposed in [13] with second order statistics was focused to address the issues concerning secured embedding capacity.

Steganography detectors constructed with aid of deep CNN have vehemently entrenched one another as comparatively better to the preceding detection prototype classifiers on the basis of rich media methods. Nevertheless, prevailing network architectures still contains constrained convolutional kernels that compromises the accuracy rate significantly.

In [14], a deep residual architecture was presented for reducing utilization of heuristics that enhanced the detection accuracy significantly review of deep learning techniques combining information hiding technology was investigated in [15]. In contemporary literature concerning steganalysis, it perceived which a deeper network is desired for minimum tone noise detection images.

Nevertheless, a deep learning model called, Fractal Network was designed in [16-18] on the basis of self-similarity and expanded profound and extensive by sustaining an equilibrium between shallowness and breadth utilizing a recurrent transformation of an elementary building block. In [18-20], the hypothesis of fractal network was used for steganography detection.

Steganographic methods are schemes are frequently outlined in a method with the purpose of preserving steganalytic characteristics. Owing to the reason that most of the steganalytic methods utilize a classifier based on ML, it is appropriate or practical to involve countering steganalysis, nevertheless, simply employing perturbations on stego images may result in the data extraction failure and generate introduce unpredicted noises.

In [21-23], a steganographic method employing adversarial embedding that attains the objective of stego message hiding with minimum distortion was presented. In this manner better security was said to be achieved. Despite improvement observed in terms of both security and distortion, the complexity involved in the design was not focused. To address on this issue, a channel-wise convolution model was employed in [24] to address on the complexity related issues. A steganography framework employing a distortion function was designed in [25]. Here, first, generator with the aid of U-Net architecture translated cover image to embedding probability map, following which double-tank function was employed in approximating optimal embedding and finally utilizing CNN by several high pass filters as discriminator. With this type of design adversarial training time was reduced considerably.

Motivated by the above mentioned works, in this paper, a Gamma Statistic Kakutani Fixed-point and Equilibrium Generative Adversarial Network-based (GSKF-EGAN) secure steganography method is introduced.

Gamma Statistic Kakutani Fixed-point and Equilibrium Generative Adversarial Network-based Secure Steganography

Through evolution of computer as well as communication technology, extensive amounts of images are hoard and transmitted via internet. The process of retaining certain sensitive images, like, sensitive medical images from accessed by third parties has paramount bifurcate of data security. To address on this aspect, a probable way remains in hiding the secret images in carrier image so which visual contents do not change. In this manner, only authorized users extract data of secret image and referred to image steganography.

Upon comparison with the conventional Steganography method, steganographic algorithm based on deep learning perceives spontaneous image hiding and extraction where there requires no necessitate for human interference.

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Distinctive features can be extracted by fine tuning parameter information that in turn extensively enhances the significance of image steganography. The flow chart of the proposed Gamma Statistic Kakutani Fixed-point and Equilibrium Generative Adversarial Network-based Secure Steganography method is shown in figure 1.

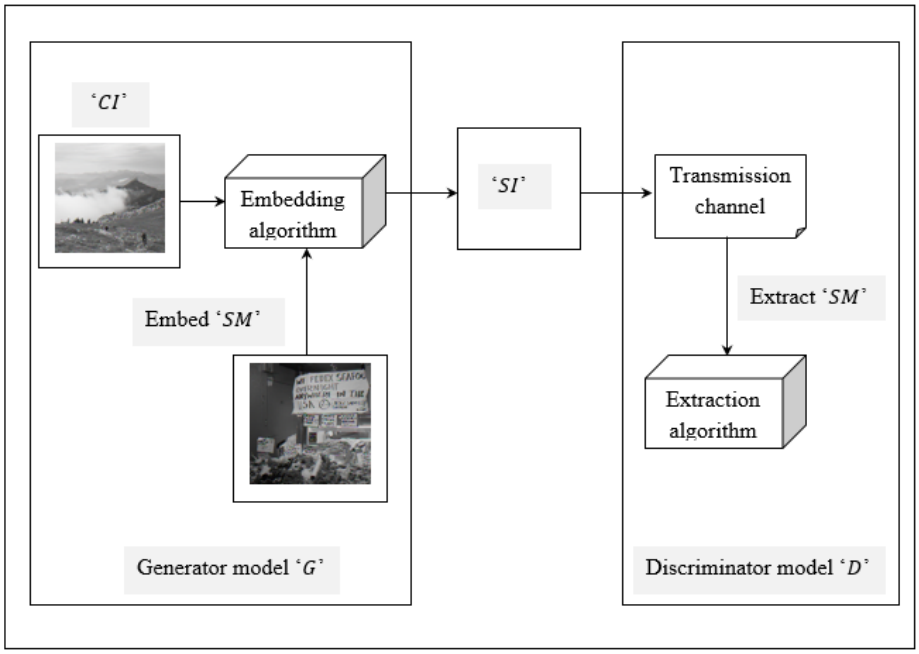

Figure 1: Structure of Gamma Statistic Kakutani Fixed-point and Equilibrium Generative Adversarial Network-based Secure Steganography

As illustrated in the above figure, there are preprocessing, embedding '*Embed*' via the generator model '*G*' and extracting '*Extract*' via the discriminator model '*D*'. Initially, preprocessing network normalizes secret image while extracting essential features via Gamma Statistic Histogram Equalization-based Preprocessing model. Next, the Kakutani Fixed-point and Equilibrium Generative Adversarial Network embedding algorithm '*EmbedAlg*' embeds the secret text or secret message '*SM*' and cover image '*CI*' to generate a stego image '*SI*'. Finally, extracting algorithm Kakutani Fixed-point and Equilibrium Generative Adversarial Network (i.e., the inverse process)'*ExtractAlg*' extracts the secret image via a transmission channel.

1.3 Dataset description

BOSSBase v1.0.1 dataset is used for performing simulation purpose. The dataset consists of 10,000 grey as well as white images by pixel values ranging between '*0*' and '*255*' and overall image size of '256×256' pixels. Natural images present in this dataset are considered as cover image '*CI*' and the text images present in this dataset are considered as secret message or secret image '*SM*'. Once dataset has provoked, it has been disjoined to arbitrary training as well as test sets. All of these training and testing sets is organized through set of cover images and their associated stego images. Training and testing set comprise 60% of training images (6000) and 40% of the testing set images (4000) respectively.

1.4 GAN Image Steganography System Model

Generative Adversarial Network based image Steganography employed in our work is featured by being incompetent to produce sample images as near as possible to target samples. By employing Game theory GAN includes a Generator model 'G' and a Discriminator model 'D' separately. Here, Generator model 'G' metamorphoses the arbitrary noise that follows the preceding allocation to generated samples, so which distribution of generated sample that executes as near as possible to the real data and on the other hand, the Discriminator model '*D*' decide whether the input simulation samples are real or generated samples. Finally, Generative Adversarial Network based image Steganography is summarized as a MinMax game theory where Discriminator model '*D*' tries to maximize probability of accurately differentiating between real and generated samples whereas the Generator model maximize the probability which Discriminator model 'D' does not differentiate generated samples. Then, system model for designing image Steganography based on GAN is formulated as given below.

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

$$\min_{G}\max_{D} f(D,G) = E_{CI\sim ProbCI}(CI)[\log D(CI)] + E_{\epsilon\sim Prob\epsilon}(\epsilon)\left[\log\left(1 - D\left(G(\epsilon)\right)\right)\right] \quad (1)$$

From the above equation (1), '$G(\epsilon)$' denotes the Generator model 'G' generated sample or the cover image 'CI' based on the input arbitrary noise 'ϵ'. Also '$D(CI)$' denotes probability which Discriminator model 'D' ascertains the sample 'CI' is real sample cover image or not.

1.5 Gamma Statistic Histogram Equalization-based Preprocessing model

Owing to the reason that secret message has embedded with cover image of image processing; stego image processing generation method requires to trained initially. Generation method employs Gamma Statistic Histogram Equalization for initial training process. Prior to the training of generation method, Gamma Statistic Histogram Equalization is executed on the original cover image 'CI' and secret image text 'SM' to model dual processed image sets. Following which dual processed image sets utilized for designing secure steganography model. Figure 2 shows the structure of Gamma Statistic Histogram Equalization-based Preprocessing model.

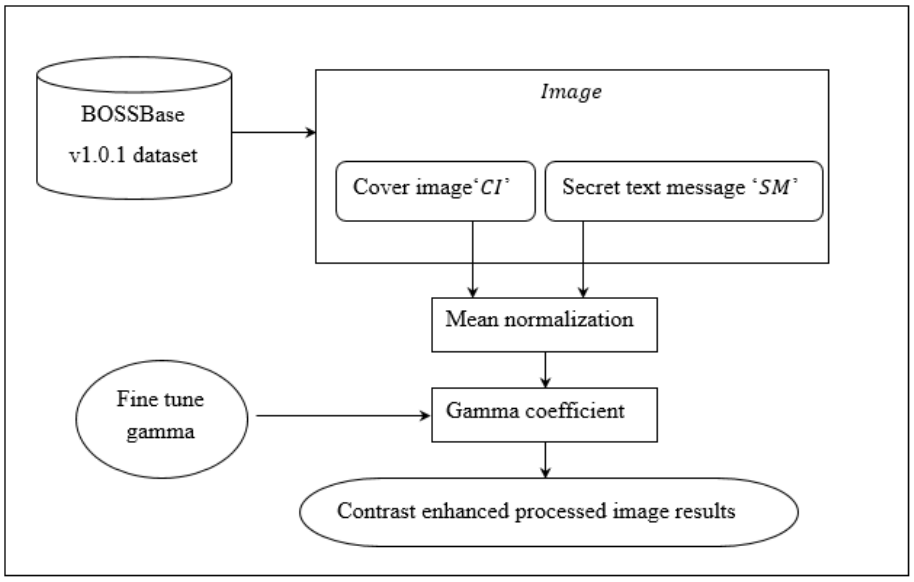

Figure 2: Structure of Gamma Statistic Histogram Equalization-based Preprocessing

As shown in the above figure, with the raw images obtained as input from BOSSBase v1.0.1 dataset are subjected to normalization and fine tuning of gamma coefficient is performed to generate final processed results for further processing. To systematically take different types of detail information into consideration, cover image and secret image text are normalized discretely. Mean normalization is conducted on cover image and secret image text to guarantee images discharges rational dispersal with mean 'o' and standard deviation of '1' respectively as given below.

$$NCI = \frac{CI - \mu(CI)}{\sigma(CI)} \quad (2)$$

$$NSM = \frac{SM - \mu(SM)}{\sigma(SM)} \quad (3)$$

From the above equations (2) and (3), 'CI' and 'SM' represents the sample cover image and sample secret text image, '$\mu(CI)$' and '$\sigma(CI)$' are mean and standard deviation of the corresponding images respectively. Following which to enhance texture, Gamma Statistical function is applied with the purpose of enhancing the illumination placement and this is mathematically stated separately for the normalized cover and secret text message as given below.

$$GNCI = Gamma\big(NCI(p,q)\big) = \begin{cases} \left(\frac{NCI(p,q)}{Max(NCI)}\right)^{\gamma_i} * Max(NCI), NCI(p,q) \geq o \\ \left(\frac{NCI(p,q)}{Min(NCI)}\right)^{\gamma_i} * Min(NCI), NCI(p,q) < o \end{cases} \quad (4)$$

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

$$GNSM = Gamma\big(NSM(p,q)\big) = \begin{cases} \left(\frac{NSM(r,s)}{Max(NSM)}\right)^{\gamma_j} * Max(NSM), NSM(r,s) \geq o \\ \left(\frac{NSM(r,s)}{Min(NSM)}\right)^{\gamma_j} * Min(NSM), NSM(r,s) < o \end{cases} \quad (5)$$

From the above equations (4) and (5) 'NCI', 'NSM' stands for the normalized cover images and normalized secret text messages with '$NCI(p,q)$' and '$NSM(r,s)$' representing certain pixel information accordingly. Finally, the fine tuned gamma coefficient results are modeled as given below.

$$\gamma_i = \delta\big(1 - NCI(p,q)\big) \quad (6)$$

$$\gamma_j = \delta\big(1 - NSM(r,s)\big) \quad (7)$$

From the above equations (6) and (7), the fine tuned gamma coefficient value lies between 'o' and '1' that in turn makes the magnitude of intensification insignificant over low prevalence portion and significant over high prevalence potion that can efficiently circumvent noise magnification by maintaining low prevalence portion respectively. The pseudo code representation of Gamma Statistic Histogram Equalization-based Preprocessing is given below.

Input: Dataset 'DS', Cover Image '$CI = \{CI_1, CI_2, \dots, CI_m\}$', Secret text Message '$SM = \{SM_1, SM_2, \dots, SM_n\}$'
Output: noise improved processed cover image and secret text message
1: **Initialize** 'm', 'n', '$\delta = 0$ *to* 1' 2: **Begin** 3: **For** each Dataset 'DS' with Cover Image 'CI' and Secret Message 'SM' 4: Evaluate mean normalization for cover images as given in (2) 5: Evaluate mean normalization for secret text images as given in (3) 6: Apply gamma coefficient to the normalized cover images as given in (4) 7: Apply gamma coefficient to the normalized secret text images as given in (5) 8: Fine tune gamma coefficient results as given in (6) and (7) 9: **Return** processed results '$GNCI$', '$GNSM$' 10: **End for** 11: **End**

Algorithm 1: Gamma Statistic Histogram Equalization-based Preprocessing

As given in the above algorithm with the purpose of enhancing the image enhancement quality results via PSNR, a gamma coefficient is applied to the generated statistic histogram for the corresponding input cover image as well as secret text message. With this objective first, mean normalization function is used to cover image and secret text message. Following which normalized cover images and secret text message are subjected to gamma coefficient function. Finally, fine tuning is performed to return the processed results by reducing high peak and controlling over enhancement.

1.6 Kakutani Fixed-point and Equilibrium Generative Adversarial Network-based Steganography model

Over the decades, the ever accelerating evolutions of communication technology permitted the free transferring and sensitive information sharing over the complicated internet network. In the recent years, secured communication between users or parties is ensured via mathematical models accelerated steganographic algorithms. Nevertheless, most of the traditional steganographic algorithms experience high embedding while determining the best position for hiding secret message text in the host channel with minimal bit error rate. This limitation is surpassed in our work by introducing the Generative Adversarial Network (GAN) based steganographic algorithm, where the GAN employs a distributed representation to store the learning knowledge via generator user 'GU' and discriminator user 'DU' respectively. This in turn by introducing the back propagation function via Kakutani Fixed-point that in turn warrants the existence of a fixed-point only if the quadrant conditions are satisfied. As a result secured image Steganography process is said to be ensured. Here, the discriminator process (i.e., embedding) is performed using the convolutional operation via discriminator user 'DU' and in a similar manner, the generator process (i.e., extraction) is performed using the deconvolutional operation via generator user 'GU'. Figure 3 shows the structure of Kakutani Fixed-point and Equilibrium Generative Adversarial Network-based Steganography model.

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

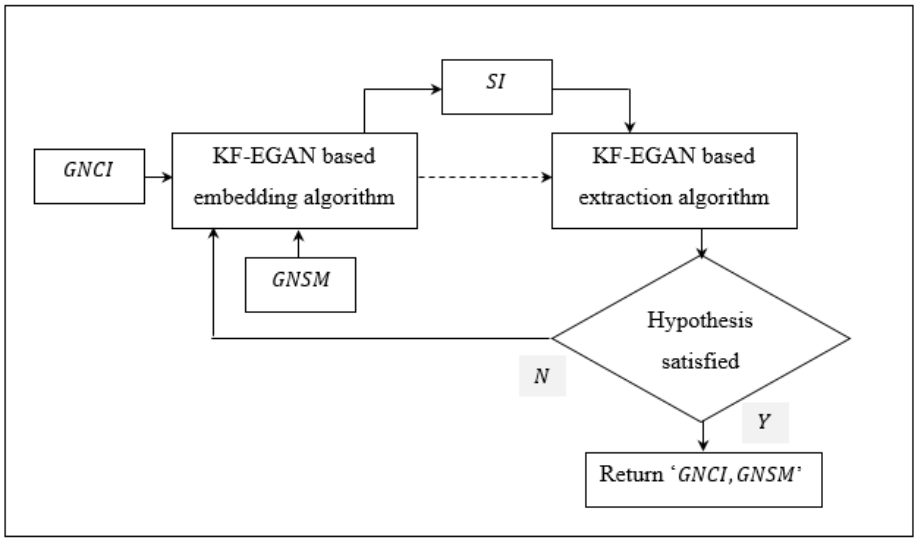

Figure 3: Structure of Kakutani Fixed-point and Equilibrium Generative Adversarial Network-based Steganography model

As shown in the above figure, let us consider a secure probability steg space 'α, β_{ref}' with the involvement of two players or users. Here, the dual players, discriminator user 'DU' (i.e., the sender) sends cover image 'CI' as well as the secret text message 'SM' via convolution process whereas the generator user 'GU' can either be the intended recipient user or malicious user. Here the task remains in sending the stego images to the intended recipient user with higher rate of security. Here the generator user 'GU' strategy set is '$Prob(\alpha)$', whereas the discriminator user 'DU' strategy set is '$\beta_{DU}: \alpha \rightarrow Prob[0,1]$'. Then, the Generative Adversarial Network-based game theory in our work with the objective function formulated as given below.

$$Objfun(\beta_{GU}, \mu_{DU}[GNCI, GNSM]) = E_{p\sim\beta_{ref}, q\sim\beta_{DU}}(p)[\log q] + E_{p\sim\beta_{GU}, q\sim\beta_{DU}}(p)[\log(1-q)] \quad (8)$$

From the above equation (8) objective function '$Objfun(\beta_{GU}, \mu_{DU})$' is formulated based on the secure probability steg space and strategy set of generator user 'GU' and discriminator user 'DU' respectively. Following which the formulation of objective function is mathematically represented as given below.

$$GU \rightarrow Max\big(Objfun(\beta_{GU}, \mu_{DU}[GNCI, GNSM])\big) \quad (9)$$

$$SI = DU \rightarrow Min\big(Objfunv(\beta_{GU}, \mu_{DU}[GNCI, GNSM])\big) \quad (10)$$

From the above equations (9) and (10), the generator user 'GU' objective remains in maximizing the objective (i.e., maximizing the stego image to be given to the intended user) whereas the discriminator user 'DU' objective remains in minimizing the objective (i.e., minimizing the stego image to be given to the malicious user). Then, according to the Kakutani Fixed point, the extraction formulates are designed wherein only upon the satisfaction of three conditions given below.

$$\beta'_{GU} \in \arg\max_{\beta_{GU}}\big(Objfun(\beta_{GU}, \mu_{DU}[GNCI, GNSM])\big), \beta'_{DU} \in \arg\min_{\beta_{DU}} objfun\big(\beta^{q}_{GU}, \beta_{DU}\big) \quad (11)$$

$$\beta'_{DU} \in \arg\max_{\beta_{DU}}\big(Objfun(\beta_{GU}, \beta_{DU}[GNCI, GNSM])\big), \beta'_{GU} \in \arg\min_{\beta_{GU}} objfun\big(\beta_{GU}, \beta'_{DU}\big) \quad (12)$$

From the above equation (11), the condition is satisfied from the fact that the argmax function is simplex and hence compact. In a similar manner, from the above equation (12), the condition is satisfied by way of argmax function supporting sending of cover image and secret text message to the intended recipient. Finally, to prove the existence of the best equilibrium using Kakutani Fixed point is mathematically stated as given below.

$$KN_i(DU_{-i}) = \arg\max_{DU_i} PO_i(DU_i, DU_{-i}) \quad (13)$$

From the above equation (13), the condition is said to be satisfied as a result of mixed strategies with maximum payoffs 'PO_i', therefore ensuring data security in a smooth fashion. The pseudo code representation of Kakutani Fixed-point and Equilibrium Generative Adversarial Network-based Steganography to ensure smooth and secure embedding and extraction process is given below.

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Input: Dataset 'DS', Cover Image '$CI = \{CI_1, CI_2, \dots, CI_m\}$', Secret text Message '$SM = \{SM_1, SM_2, \dots, SM_n\}$', generator user '$GU = GU_1, GU_2, \dots, GU_u$', discriminator user '$DU = DU_1, DU_2, \dots, DU_v$'
Output: robust and secure steganography
1: **Initialize** 'm', 'n', processed results '$GNCI$', '$GNSM$', generator user 'GU', discriminator user 'DU', 'u', 'v' 2: **Initialize** secure probability steg space 'α, β_{ref}', test image 'TI' 3: **Begin** 4: **Foreach** Dataset 'DS' with Cover Image 'CI', Secret Message 'SM' and processed results '$GNCI$', '$GNSM$' **//Embedding (*EmbedAlg*)** 5: Formulate Kakutani Fixed point-based objective function as given in (8) 6: Generate min max function validation as given in (9) and (10) 7: Generate stego image 'SI' 8: **Return stego image** 'SI' **//Extraction (*ExtractAlg*)** 9: **For** each stego image 'SI' 10: Formulate the theorems according to three conditions as given in (11), (12) and (13) and extract secret message and stego image 'SI' 11: Subject test image 'SI' to three conditions as given in (11), (12) and (13) 12: **If** '$SI = CI$' 13: **Then** stego image and cover image are same 14: Establish secure communication between users 15: Return secret text message to the intended user '$GNSM$' 16: **End if** 17: **If** '$SI <> CI$' 18: **Then** stego image and cover image are different 19: Proceed with other set of users 20: **End if** 21: **End for** 22: **End for** 23: **End**

Algorithm 2: Kakutani Fixed-point and Equilibrium Generative Adversarial Network-based Steganography

As given in the above algorithm, with the processed cover and secret text images obtained as input, both the images are subjected to embedding process using Kakutani Fixed-point via Generative Adversarial Network. Here, with the aid of Kakutani Fixed-point theorem, only upon satisfying three conditions, condition validity is ensured, therefore reducing the bit error rate involved in image Steganography significantly. Moreover to improve embedding rate strategic equilibrium or three conditions are introduced via Generative Adversarial Network that in turn improves the embedding rate in an extensive manner. Hence, by improving the embedding rate, Structural Similarity Index (SSIM) is improved, i.e., enhancing the similarity between cover image and stego images.

Simulation setup

It gives an extensive explanation of experimental analysis performed on Gamma Statistic Kakutani Fixed-point and Equilibrium Generative Adversarial Network-based (GSKF-EGAN) secure Steganography method using BOSSBase v1.0.1 dataset (https://dde.binghamton.edu/download/). Dataset contains overall of 10,000 with training and testing set include 60% of training images (6000) and 40% of the testing set images (4000) respectively. 4000 images are employed as training possessing various size. Experimentation has been carried out by MATLAB R2023a .Here, we examine performance of the proposed GSKF-EGAN secure Steganography technique that is

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

estimated by Peak Signal to Noise Ratio (PSNR), Bit Error Rate (BER) and Embedding Rate (bpp) and SSIM respectively.

Analysis of embedding quality

To measure embedding quality of Gamma Statistic Kakutani Fixed-point and Equilibrium Generative Adversarial Network-based (GSKF-EGAN) secure Steganography method and provide a detailed analysis by comparing it with the existing methods, Support Vector Machine and Integer Wavelet Transform [1] and Generative Adversarial Networks and Genetic Algorithm [2], embedding rate and bit error rate are validated. To ensure fair comparison similar image sizes are employed for both the GSKF-EGAN method and existing methods, Support Vector Machine and Integer Wavelet Transform[1] and Generative Adversarial Networks and Genetic Algorithm[2] respectively.

1.6.1 Embedding rate

It measures ratio between entire number of bits embedded in cover image as well as total number of pixels in cover image and is measured in bits per pixel (bpp). In addition, the embedding rate measures the amount of data that we can hide in cover image in addition to the secret message data employing a reversible data hiding mechanism. Hence, it represented by 'ER' is referred highest payload of stego image and mathematically stated given below.

$$ER = \frac{PL}{(2*i-1)*(2*j-1)} \tag{14}$$

In equation (14), the embedding rate 'ER' is estimated on the basis of 'PL', total number of secret message bits in addition to secret message data embedded in processed cover image and '$i * j$' indicates cover image original size whereas '$(2 * i - 1) * (2 * j - 1)$' represents the processed cover image with respect to actual cover image size and '$PL = 0.05$'.Table 1 provides the investigation of GSKF-EGAN method by Support Vector Machine and Integer Wavelet Transform [1] and Generative Adversarial Networks and Genetic Algorithm [2] with reference to embedding rate value attained for ten distinct cover images based on values substituting in equation (14) respectively.

Table 1: Tabulation of embedding rate using GSKF-EGAN, Support Vector Machine and Integer Wavelet Transform [1] and Generative Adversarial Networks and Genetic Algorithm [2]

Sample images (KB)	Embedding rate (bpp)		
	GSKF-EGAN	Support Vector Machine and Integer Wavelet Transform [1]	Generative Adversarial Networks and Genetic Algorithm [2]
77	3.69	3.03	2.47
77.6	5.25	4.95	4.45
83	6.45	5.65	5.10
82.4	7.10	6.85	6.65
89.5	5.95	5.65	5.45
103	6.65	6.25	6.10
87	7.25	6.85	6.55
93	8.35	7.95	7.35
96	8.95	8.15	7.95
106	9.45	8.95	8.10

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

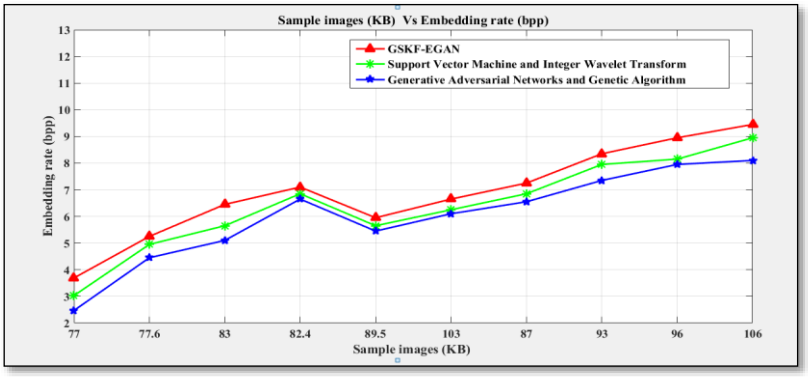

Figure 4: Sample images versus embedding rate

Figure 4 given above illustrates embedding rate graphical representation by varying image sizes ranging between 77KB to 106KB. In Figure 4 it is clearly seen obviously GSKF-EGAN achieved embedding rate of 3.69bits/pixel for testing image sizing of 77KB that is finest than the conventional methods, 3.03KB [1] and 2.47KB [2]. All other compared methods, [1], [2] had comparatively lesser embedding rate when juxtaposed with the GSKF-EGAN method for every varying test images. In addition, visual nature of stego images acquired through GSKF-EGAN method is normal when compared to [1] and [2].Moreover, the GSKF-EGAN method significantly safeguards every requisite info of natural image as well as generated fine tuned stego images by applying Gamma Statistic Histogram Equalization-based Preprocessing model. Along these lines, it is significantly concluded that the GSKF-EGAN method imparted eminent embedding rate for natural images as compared techniques did not. Therefore upon comparison the embedding rate was better by GSKF-EGAN method by 8% and 17% than the [1] , [2].

1.6.2 Bit Error Rate

Embedding rate is measured to validate the proposed method. It is represented as below.

$$BER = \frac{1}{mn}\left[\sum_{i=1}^{m}\sum_{j=1}^{n} CI_o(i,j) \oplus CI_e(i,j)\right] * 100 \qquad (15)$$

From the above equation (15), the bit error rate 'BER' is valued taking into consideration original cover image '$CI_o(i,j)$' and extracted cover image '$CI_e(i,j)$' with '(m,n)' representing dimensions. The resultant bit error rate value measured using the above equation from the selected 10 distinct cover image samples are given in table 2. One of the significant feature i.e., bit error rate was not identified to be homogeneous for all the ten sample cover images but relative analysis inferred lesser bit error rate using GSKF-EGAN upon comparison with the Support Vector Machine and Integer Wavelet Transform [1] and Generative Adversarial Networks and Genetic Algorithm[2].

Table 2: Tabulation of bit error rate using GSKF-EGAN, Support Vector Machine and Integer Wavelet Transform [1] and Generative Adversarial Networks and Genetic Algorithm [2]

Sample images	Bit error rate		
	GSKF-EGAN	Support Vector Machine and Integer Wavelet Transform [1]	Generative Adversarial Networks and Genetic Algorithm [2]
4000	0.0565	0.0623	0.0654
8000	0.0396	0.0556	0.0506
12000	0.0546	0.0636	0.0696
16000	0.0396	0.0466	0.0496
20000	0.0626	0.0696	0.0746
24000	0.0496	0.0686	0.0736
28000	0.0275	0.0306	0.0446
32000	0.0686	0.0846	0.0986
36000	0.0526	0.0646	0.0606
40000	0.04	0.05	0.06

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

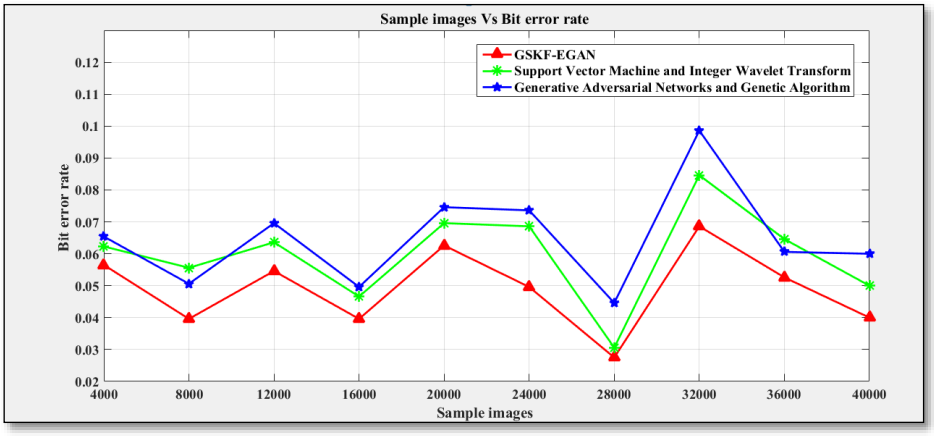

Figure 5: Sample images versus bit error rate

Figure 5 given above illustrates figurative characterization of bit error rate considered for differing images. Secure Steganography method is concerned, efficiency of the method can be analyzed at with closer to 0 value (i.e., bit error rate) ensuring advantageous and vice versa. From the above figure, it is inferred that, bit error rate by proposed GSKF-EGAN technique was found to be closer to 0 than upon comparison with the existing methods, [1] and [2]. The reason was owing to the application of back propagation function via Kakutani Fixed-point where three conditions were employed for validating and only upon successful validation, further processing was ensured. This in turn reduced the bit error rate during the recovery and extraction process. As a outcome, bit error rate by GSKF-EGAN technique was found to be comparatively lesser than [1] and [2] by 17% and 24% respectively.

1.7 Analysis of extraction quality

In this section to measure visual quality of recovered image PSNR and SSIM are discussed. Also to ensure fair comparison both the performance metrics are validated using the proposed GSKF-EGAN method and existing methods [1], [2] with the aid of table and graphical representations.

1.7.1 PSNR

Performance of GSKF-EGAN method has validated in several image quality metrics like PSNR, SSIM. It is mathematically formulated as given below.

$$PSNR(dB) = 10log_{10}\frac{255^2}{MSE} \tag{16}$$

From the above equation (16), the resultant value of '$PSNR$' is obtained based on mean square error and is evaluated below.

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}[C(i,j) - S(i,j)]^2 \tag{17}$$

From the above equation (17), the resultant mean square error 'MSE' value is arrived at on basis of difference pixel values between the cover image pixels '$CI(i,j)$' and stego image pixels '$SI(i,j)$'. Table 3 tabulates validation results of GSKF-EGAN method with Support Vector Machine and Integer Wavelet Transform [1] and Generative Adversarial Networks and Genetic Algorithm [2] for all ten distinct cover images respectively.

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 3: Tabulation of PSNR using GSKF-EGAN, Support Vector Machine and Integer Wavelet Transform [1] and Generative Adversarial Networks and Genetic Algorithm [2]

Sample images (KB)	PSNR (dB)		
	GSKF-EGAN	Support Vector Machine and Integer Wavelet Transform [1]	Generative Adversarial Networks and Genetic Algorithm [2]
77	30.14	26.62	21.18
77.6	25.25	23.65	22.10
83	32.55	30.45	29.45
82.4	29.45	28.55	27.55
89.5	33.65	31.25	30.65
103	32.95	30.55	29.10
87	23.55	21.45	20.65
93	37.65	35.65	33.55
96	31.10	29.65	28.45
106	30.25	28.35	27.10

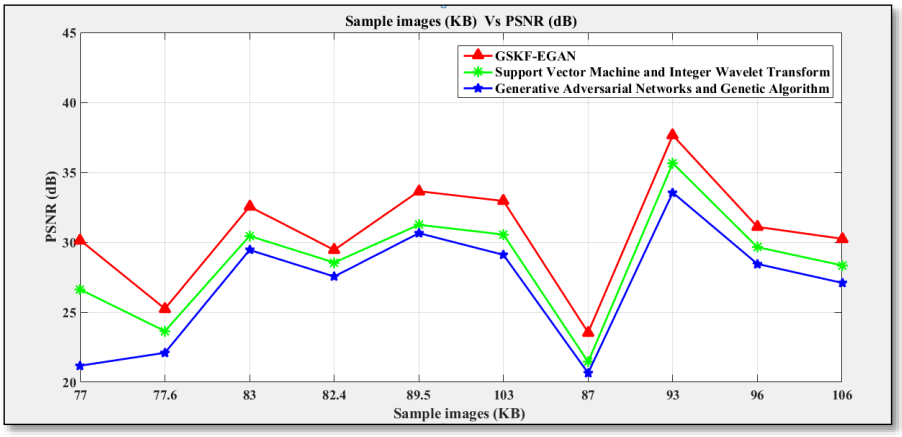

Figure 6: Sample images versus PSNR

Figure 6 illustrate study of PSNR values acquired through GSKF-EGAN and Support Vector Machine and Integer Wavelet Transform [1], Generative Adversarial Networks and Genetic Algorithm [2] on differing image sizes. It might be discerned magnificently from the above figure that the GSKF-EGAN method imparted permissible Gaussian normalized cover image and stego image even at maximum image sizes, but every other compared ones [1] and [2] in perspective on their minimized embedding rates might possibly not work at maximum image sizes. Exceptional or unprecedented execution of GSKF-EGAN method on every sample test images of distinct sizes is chalked up to its eventuality to supervise minimum intensity pixels, by guaranteeing both images discharges rational dispersal with mean '*o*' and standard deviation of '*1*' using Gamma Statistical function with the objective of improving illumination placement prior to data embedding. But, in conventional methods, they essentially discarded these divergences as well as distinguish them as non-embeddable cases. It enhancing PSNR with GSKF-EGAN method by 7% and 14% than the [1],[2].

1.7.2 SSIM

Finally, '*SSIM*' is measured using three distinct terms, i.e., luminance, contrast and structure and is stated as given below.

$$SSIM\ (i,j) = \frac{(2\mu_i\mu_j+C_1)(2\sigma_{ij}+C_2)}{(\mu^2 i+\mu^2 j+C_1)(\sigma^2 i+\sigma^2 j+C_2)} \quad (18)$$

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

From the above equation (18), the SSIM is evaluated taking into considerations the mean values '$\mu_i\mu_j, \mu^2 i, \mu^2 j$', standard deviation '$\sigma^2 i, \sigma^2 j$' and cross variance '$\sigma_{ij}$' for sample cover images 'i, j' respectively. To measure the similarity level, the Structural Similarity Index (SSIM) is taken into consideration as distinct performance metrics to estimate the similarity level. The SSIM validates the association of similarity among stego image and original cover image. 'SSIM' value lies among '-1' and '$+1$', here '$+1$' associates to identical images whereas '-1' associates to different or distinct images. Finally, SSIM results obtained when substituted in equation (18) are listed below.

Table 4: Tabulation of SIIM using GSKF-EGAN, Support Vector Machine and Integer Wavelet Transform [1] and Generative Adversarial Networks and Genetic Algorithm [2]

Sample images (KB)	SSIM (dB)		
	GSKF-EGAN	Support Vector Machine and Integer Wavelet Transform [1]	Generative Adversarial Networks and Genetic Algorithm [2]
77	0.864	0.724	0.704
77.6	0.844	0.704	0.674
83	0.814	0.674	0.634
82.4	0.804	0.644	0.614
89.5	0.834	0.704	0.674
103	0.844	0.724	0.704
87	0.864	0.774	0.734
93	0.814	0.754	0.724
96	0.879	0.78	0.744
106	0.874	0.804	0.789

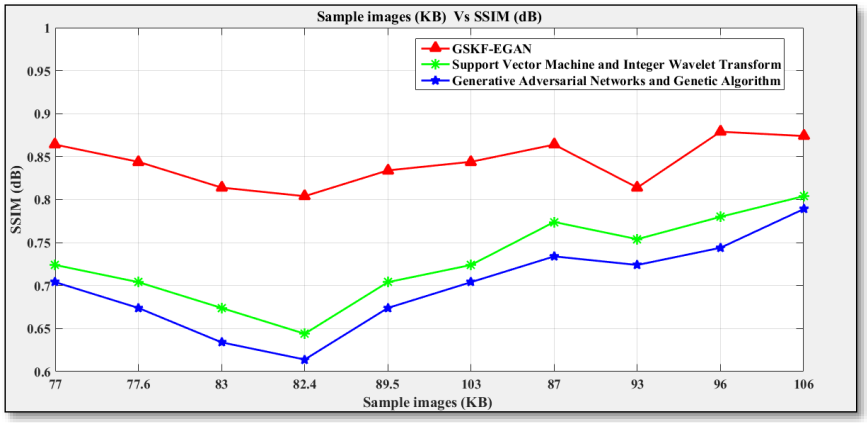

Figure 7: Sample images versus SSIM

Finally, figure 7 shows graphical illustration of SSIM for 10 differing images of distinct sizes. Due to reason that natural images are used for image hiding, their SSIM have been estimated for evaluation of the method. The SSIM value has been measured for obtaining the values of similarity of existing methods [1], [2] with respect to the proposed image employed for analysis. Dominance of proposed method in case of natural cover images is owing to the reason that the application of three hypothesis theorem via best equilibrium using Kakutani Fixed point function .cover images are maximum. As reason, natural cover images of superior importance are hidden with another secret text message to circumvent it for privacy uses. Through this SSIM value using GSKF-EGAN was by 16% and 21% than the [1] ,[2] respectively.

Conclusion

A novel steganographic technique called, Gamma Statistic Kakutani Fixed-point and Equilibrium Generative Adversarial Network-based (GSKF-EGAN) which is embedding secret text message in process of histogram equalization as well as statistical processing during trained histogram equalization inception model and statistical inception model. Between them, image processing inception methods generate contrast enhanced processed images during gamma coefficient, after that, the stego images are generated from gamma coefficient mapped through secret text message during image processing. To undergo this process, Kakutani Fixed-point and Equilibrium

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Generative Adversarial Network-based Steganography is applied separately by the discriminator and generator for embedding and extraction separately. To confirm security of steganographic method designed in this paper, we employ current conventional secure Steganography method to identify processed stego images generated. Experimental outcomes manifested that steganographic technique has improved security performance to resist recognition by conventional methods.

References

[1] ParthaChowdhuri, Pabitra Pal, Tapas Si, "A novel steganographic technique for medical image using SVM and IWT", Multimedia Tools and Applications, Springer, Dec 2024 [Support Vector Machine and Integer Wavelet Transform]
[2] Alejandro Martín, Alfonso Hernández, MoutazAlazab, Jason Jung, David Camacho, "Evolving Generative Adversarial Networks to improve image Steganography", Expert Systems With Applications, Elsevier, Mar 2024 [Generative Adversarial Networks and Genetic Algorithm]
[3] R. Gurunath, Ahmed H. Alahmadi, DebabrataSamanda, Mohammad Zubair Khan, Abdulrahman Alahmadi, "A Novel Approach for Linguistic Steganography Evaluation Based on Artificial Neural Networks", IEEE Access, Sep 2021
[4] Ahmed A. Mawgoud, Mohamed Hamed N. Taha, Amr Abu-Talleb and AmiraKotb, "A deep learning based steganography integration framework for ad-hoc cloud computing data security augmentation using the V-BOINC system", Journal of Cloud Computing: Advances, Systems and Applications, Springer, Oct 2022
[5] ShahidRahman, Jamal Uddin, Muhammad Zakarya, HameedHussain, Ayaz Ali Khan, Aftab Ahmed, Muhammad Haleem, "A Comprehensive Study of Digital Image Steganographic Techniques", IEEE Access, Jan 2023
[6] BassemAbd-El-Atty, "A robust medical image steganography approach based on particle swarm optimization algorithm and quantum walks", Neural Computing and Applications, Springer, Feb 2023
[7] VojtechHolub, Jessica Fridrich and Tomas Denemark, "Universal distortion function for steganography in an arbitrary domain", EURASIP Journal on Information Security 2, Springer, Feb 2021
[8] FatmahAbdulrahmanBaothman and Budoor Salem Edhah, "Toward agent-based LSB image steganography system", Journal of Intelligent Systems, De Gruyter, Sep 2021
[9] Paramita Chatterjee, Rajesh Bose, Subhasish Banerjee, Sandip Roy, "Enhancing Data Security of Cloud Based LMS", Wireless Personal Communications, Springer, Mar 2023
[10] Yaofei Wang, Weiming Zhang, Weixiang Li, Xinzhi Yu, Nenghai Yu, "Non-Additive Cost Functions for Color Image Steganography Based on Inter-Channel Correlations and Differences", IEEE Transactions on Information Forensics and Security, Mar 2019
[11] Deepa D. Shankar, Adresya Suresh Azhakath, "Random embedded calibrated statistical blind steganalysis using cross validated support vector machine and support vector machine with particle swarm optimization", Scientific Reports, Feb 2023
[12] Al-HussienSeddik, Mohammed Salah, GamalBehery and Ahmed El-Harby, " Information Hiding Using Coverless Steganography System Based on Image Generation", Scientific Journal for Damietta Faculty of Science , Oct 2022
[13] LinjieGuo, JiangqunNiWenkangSu,Chengpei Tang, and Yun-Qing Shi, "Using Statistical Image Model for JPEG Steganography: Uniform Embedding Revisited", IEEE Transactions on Information Forensics and Security, VOL. 10, NO. 12, DECEMBER 2015
[14] Mehdi Boroumand, Student Member, IEEE, Mo Chen, Member, IEEE, and Jessica Fridrich, "Deep Residual Network for Steganalysis of Digital Images", Transactions on Information Forensics and Security, Mar 2018
[15] Pan Yang, Minqing Zhang, Riming Wu, Yunxuan Su and KaiyangGuo, "Hiding Image within Image Based on Deep Learning", Pattern Recognition and Data Mining, Nov 2022
[16] BrijeshSingh,Arijit Sur, and PinakiMitra, "Steganalysis of Digital Images Using Deep Fractal Network", IEEE Transactions on Computational Social Systems, Vol. 8, No. 3, June 2021
[17] Jian Ye, Jiangqun Ni, Yang Yi, "Deep Learning Hierarchical Representations for Image Steganalysis", Transactions on Information Forensics and Security, Mar 2016
[18] Weixuan Tang, Bin Li, Shunquan Tan, Mauro Barni, and Jiwu Huang, "CNN-based Adversarial Embedding for Image Steganography", IEEE Transactions on Information Forensics and Security, Jul 2018
[19] JishenZeng, Shunquan Tan, GuangqingLiu,Bin Li, and Jiwu Huang, Fellow, "WISERNet: Wider Separate-then-reunion Network for Steganalysis of Color Images", IEEE Transactions on Information Forensics and Security, Oct 2018
[20] Jianhua Yang, DanyangRuan, Jiwu Huang, Xiangui Kang, Yun-Qing Shi, "An Embedding Cost Learning Framework Using GAN", IEEE Transactions on Information Forensics and Security, Feb 2019.

Research Article

[21] Hira Nazir, Imran SawarBajwa, SaimaAbdullah, RafaqutKazmi, Muhammad Samiullah, "A Color Image Encryption Scheme CombiningHyperchaos and Genetic Codes", IEEE Access, Feb 2022
[22] Aiman Jan, Shabir A. Parah, MuzamilHussan, Bilal A. Malik, "Double layer security using crypto-stego techniques: a comprehensiveReview", Health and Technology, Springer, Oct 2021
[23] S. N. V. J. Devi Kosuru, Anita Pradhani, K. Abdul Basith, ReshmaSona, GandharbaSwain, "Digital Image Steganography With ErrorCorrection on Extracted Data", IEEE Access, Aug 2023
[24] Mohammed NaifAlatawi, "A Hybrid Cryptography and LogiXGBoost Model for Intelligent and Privacy Protection in Wireless Body Sensor Networks (WBSNS)", International Journal of Computer Networks and Applications, Apr 2023
[25] WidAkeelAwadh, Ali Salah Alasady, AlaaKhalafHamoud, "Hybrid information security system via combination of compression, cryptography, and image steganography", International Journal of Electrical and Computer Engineering, Dec 2022

BIOGRAPHIES OF AUTHORS

Gahan A V, Research Scholar, School of Electronics and Communication Engineering, REVA UNIVERSITY. Currently working as Assistant Professor in Department of Electronics and Communication Engineering, Bangalore Institute of Technology with teaching experience of 9 years. His research interest includes, Computer Communication Networking, Cryptography, Artificial Intelligence and Machine Learning. Completed Bachelor's in Electronics and Communication Engineering & Master of Technology in Digital Communication and Networking from Visvesvaraya Technological Institute. He can be contacted at email: gahanbit@gmail.com

Dr. Geetha D Devanagavi is currently working as Professor in REVA UNIVERSITY. She has 29 years of teaching experience. Her research interest includes wireless sensor networks, cryptography, communication, machine learning, artificially intelligence. She has good number of publications in reputed journals. She has published 40 papers in peer reviewed national and international journals. She has guided 6 Ph.D. Scholars. She has been listed in Marquis' Who Who's in the world (2014 Edition), USA. She has Scopus h-index 7 and 259 citations. She can be contacted at email: dgeetha@reva.edu.in