**A Novel Hybrid**

**Image Steganography Technique**

**By**

**Manash Das 16**

**Mriganka Manna 43**

**Gitiparna Paul 50**

**Souhit Paul 51**

**Under the esteemed guidance of**

**Abhijit Sarkar**

A project synopsis submitted for the partial fulfilment of

Bachelor of Technology in the

**Department of Computer Science and Engineering**

**St. Thomas’ College of Engineering and Technology**

**Affiliated to**

**Maulana Abul Kalam Azad University of Technology, West Bengal**

**St. Thomas’ College of Engineering and Technology**

**Department of Computer Science and Engineering**

**Declaration**

We declare that this written submission represents our ideas in our own words and we have adequately cited and referenced the original sources. We also declare that we have adhered to all the principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in our submission. We understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

**Gitiparna Paul Manash Das Mriganka Manna Souhit Paul**

Roll: 50 Roll: 16 Roll: 43 Roll: 51

Contents

1. [Pre-amble I](#_Toc187753444)

[**1.1 Vision and Mission** I](#_Toc187753445)

[**1.2 Program Outcome (PO) and Program Specific Outcome (PSO)** I](#_Toc187753446)

[**1.3 PO and PSO mapping with justification** III](#_Toc187753447)

1. [Abstract 1](#_Toc187753448)
2. [Introduction 1](#_Toc187753449)

[**3.1 Problem Statement** 1](#_Toc187753450)

[**3.2 Objective** 1](#_Toc187753451)

[**3.3 Literature Survey** 1](#_Toc187753452)

**[3.4 Brief Discussion on Problem](#_Toc187753453)** [3](#_Toc187753453)

[**3.5 Organization/Planning** 3](#_Toc187753454)

1. [Concepts and Problem Analysis 5](#_Toc187753455)
2. [Conclusion 9](#_Toc187753456)
3. [References 10](#_Toc187753457)

**1. Pre-amble**

**1.1 Vision and Mission**

**1.1.1 Vision of the Institute**

To evolve as an industry oriented, research-based Institution for creative solutions in various engineering domains, with an ultimate objective of meeting technological challenges faced by the Nation and the Society.

**1.1.2 Mission of the Institute**

1. To enhance the quality of engineering education and delivery through accessible, comprehensive and research-oriented teaching-learning-assessment processes in the state-of-art environment.
2. To create opportunities for students and faculty members to acquire professional knowledge and develop managerial, entrepreneurial and social attitudes with highly ethical and moral values.
3. To satisfy the ever-changing needs of the nation with respect to evolution and absorption of sustainable and environment friendly technologies for effective creation of knowledge-based society in the global era.

**1.1.3 Vision of the Computer Science and Engineering Department**

To continually improve upon the teaching-learning processes and research with a goal to develop quality technical manpower with sound academic and practical experience, who can respond to challenges and changes happening dynamically in Computer Science and Engineering.

**1.1.4 Mission of the Computer Science and Engineering Department**

1. To inspire the students to work with latest tools and to make them industry ready.
2. To impart research based technical knowledge.
3. To groom the department as a learning centre to inculcate advanced technologies in Computer Science and Engineering with social and environmental awareness.

**1.2 Program Outcome (PO) and Program Specific Outcome (PSO)**

**1.2.1 Program Outcome (PO)**

**PO1: Engineering knowledge:** Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.

**PO2: Problem analysis:** Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

**PO3: Design/development of solutions:** Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.

**PO4: Conduct investigations of complex problems:** Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

**PO5: Modern tool usage:** Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modelling to complex engineering activities with an understanding of the limitations.

**PO6: The engineer and society:** Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

**PO7: Environment and sustainability:** Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

**PO8: Ethics:** Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.

**PO9: Individual and team work:** Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

**PO10: Communication:** Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.

**PO11: Project management and finance:** Demonstrate knowledge and understanding of the engineering and management principles and apply these to one’s own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

**PO12: Life-long learning:** Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

**1.3 PO and PSO mapping with justification**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 | PO8 | PO9 | PO10 | PO11 | PO12 | PSO1 | PSO2 | PSO3 |
| 3 | 3 | 3 | 3 | 3 | 2 | 2 | 3 | 2 | 3 | 2 | 3 | 3 | 3 | 3 |

**PO1: Engineering Knowledge**

The project applies knowledge of mathematics (e.g., chaotic maps, Reed Solomon codes), computer science, and neural network architectures like DenseNet to solve complex steganography problems. It demonstrates how advanced engineering knowledge can develop solutions to secure data embedding and extraction.

**PO2: Problem Analysis**

The team analyzed challenges like adversarial attacks, compression artifacts, and robustness of steganographic systems, using research methods to design a system resistant to these issues. Problem analysis helped identify key solutions like chaotic mapping and error correction using Reed Solomon encoding.

**PO3: Design/Development of Solutions**

The design of encoder-decoder neural networks for embedding and extracting secret messages, combined with chaotic mapping and error-correction techniques, addresses specific needs of robustness and imperceptibility. The team’s iterative improvements further showcase their focus on robust system design.

**PO4: Conduct Investigations of Complex Problems**

Extensive testing, including simulations of adversarial and compression challenges, is carried out to validate system robustness. The iterative process of redesigning neural networks and adjusting parameters demonstrates an investigative approach to system optimization.

**PO5: Modern Tool Usage**

The project leverages tools like convolutional neural networks (CNNs), programming frameworks, and data compression techniques. Use of advanced steganography evaluation tools like StegExpose underlines proficiency in modern engineering tools.

**PO6: The Engineer and Society**

This system ensures secure communication for personal and organizational needs, addressing concerns like privacy and data protection. The project considers societal implications of secure data embedding.

**PO7: Environment and Sustainability**

By minimizing bandwidth consumption through efficient data embedding and compression-resistant techniques, the project indirectly supports sustainable communication practices in constrained network environments.

**PO8: Ethics**

Ethical principles are adhered to by ensuring responsible data use and protecting intellectual property through secure and robust design choices.

**PO9: Individual and Team Work**

The project demonstrates effective collaboration, with each team member contributing to distinct components like chaotic mapping, neural network architecture, and error correction. Combined efforts ensure a comprehensive solution.

**PO10: Communication**

The documentation, including a well-structured report and detailed visualizations, facilitates clear communication of the project’s findings and methodologies to peers and evaluators.

**PO11: Project Management and Finance**

Project timelines, alternative strategies for failures, and clear planning for future improvements reflect sound project management skills. Budgeting efforts for computing resources are implied.

**PO12: Life-long Learning**

The project emphasizes the team’s adaptability to emerging technologies like dense networks and chaotic maps, ensuring continuous improvement in their knowledge of steganography and neural networks.

**PSO1: Industry Readiness**

The use of advanced neural network designs and robust steganographic techniques prepares students for industry challenges in secure communication and data protection.

**PSO2: Research and Development**

By integrating concepts like chaotic mapping and Reed Solomon codes, the project pushes the boundaries of existing steganography techniques, showcasing research-driven innovation.

**PSO3: Practical Implementation**

Testing the system with real-world scenarios, such as social media compression, ensures practical applicability and usability of the developed technique.

**Abstract**

Traditional image-based steganography techniques have faced the challenges of low steganographic capacity, loss of data due to transmission compression or decoding based difficulties and various forms of attacks against possibly data bearing images like crop attack and intentionally induced compression. We have proposed a network closely resembling a Fully Convolutional Dense Network, along with a Reed Solomon based encoding technique to fight compression related artefacts, and a prominent use of Chaotic Mapping technique to make interpolation-based extraction difficult. First, the secret image is embedded with the secret message, which is first passed through a Reed Solomon Encoder. Next this secret image is divided into smaller equally sized pieces and reordered using a chaotic map, and then it is embedded into the cover image using the neural network. On the receiver side, the embedded cover image is sent through the decoder network, which extracts the secret image, the pieces are reordered using the Chaotic Mapping technique used previously and the embedded data is passed through the Reed Solomon decoder to retrieve the secret message.

**3. Introduction**

In the digital realm, where data flows endlessly and prying eyes lurk in the shadows, the need for secure communication has never been greater. Imagine passing a secret note hidden within an ordinary photograph—completely invisible to anyone but the intended recipient. This is the essence of image steganography, a fascinating technique that conceals sensitive information within images, blending security with creativity. As cyber threats grow and privacy becomes a prized commodity, such methods offer a lifeline for safeguarding confidential data, ensuring that the message not only reaches its destination but does so unnoticed.

**3.1 Problem Statement**

Our problem statement revolves around developing a novel context aware steganography approach to enhance stealth & robustness of hidden data by adapting to the context of host media. This involves dynamically adjusting embedding processed based on content of carrier, ensuring imperceptibility.

**3.2 Objective**

The objectives of our problem statement involve the following:

1. The technique should be context aware.
2. Enhanced stealth i.e., should be less perceivable to human eyes, and also to steganalysis tools.
3. Robust to transmission artefacts like compression.
4. Extracted secret data should be error-free if possible, or with minimum error.

**3.3 Literature Survey**

The growing field of secure information embedding and biometric authentication has seen innovative methods emerge, with significant contributions from generative models, chaos theory, and advanced encryption techniques. One noteworthy approach is the integration of cancellable iris biometrics with steganography for IoT authentication systems, which conceals user keys within cover images. This method, although slightly increasing error rates, provides robust protection against unauthorized access [1].

Similarly, generative adversarial networks (GANs) have revolutionized steganographic techniques. A notable example is the use of cardan grilles and DCGANs to create steganographic images through pixel value modification, ensuring secure and realistic image generation [2]. Following Kerckhoffs’ Principle, another GAN-based method ensures message retrieval is only possible when both the cover image and the extraction key are present, adding a crucial layer of security [3]. Further advancing GAN applications, WGAN-GP has been employed to simultaneously train a generator and an extractor, streamlining the embedding process and improving retrieval accuracy [4]. Expanding on these concepts, the use of multiple feature maps in GANs has improved distortion measurement, leading to better security and imperceptibility in steganographic techniques [5].

In cloud environments, multimodal biometric systems have been developed to combine biometric encryption with identity-based methods. One such system uses graph theory and chaotic logistic mapping to secure templates while integrating modules for identification, user authentication, and verification. This approach achieves high security, low error rates, and reduced processing times [6]. In the domain of biometric template security, the combination of Twofish and 3DES cryptographic algorithms with LSB steganography demonstrates a balance between security and minimal impact on cover image quality. This approach is particularly effective for iris template embedding [7].

Expanding the capabilities of GANs, coverless steganography has been introduced to eliminate risks posed by steganalysis tools, achieving high payload capacity while preserving cover image security [8]. Advanced frameworks like UMC-GAN further enhance steganographic security by incorporating nested U-shape generators and linear-clipped embedding simulators. These design innovations significantly improve embedding efficiency and overall security performance [9]. Similarly, GAN-based techniques utilizing adversarial attacks, such as ADF-IS, offer robust protection by achieving high payload embedding and imperceptibility against adversarial interference [10]. Neural style transfer (NST) introduces a creative dimension to steganography by embedding secret images within stylized cover images and enabling precise extraction via destyling GANs. This method excels in visual quality, payload capacity, and resistance to steganalysis [11].

In the realm of privacy-preserving biometric authentication, cloud-based systems have been developed that embed fingerprints within iris images using DWT and DLCM. These systems achieve high PSNR and low MSE, although their visual quality may require further optimization [12]. Addressing e-passport security, multimodal biometrics incorporating iris, fingerprint, and face recognition employ fuzzy vault encoding to ensure fraud prevention. This strategy links biometric templates with secure data decoding through stego-images and auxiliary files [13].

Chaos theory has also been harnessed to enhance security mechanisms. For instance, a novel 3D chaotic map, derived from sine and cosine functions, facilitates image encryption with a large key space and heightened unpredictability, improving resistance to unauthorized decryption [14]. In parallel, graph theory and chaotic logistic mapping have been combined to secure biometric authentication. This integration ensures dynamic and cancellable biometric templates, providing strong resistance to brute-force and multimedia attacks [15].

Finally, addressing limitations in traditional steganography, techniques like FC-DenseNet overcome challenges such as gradient issues and limited capacity. These methods achieve high-quality reconstruction and significantly enhance steganographic capacity [16]. The robust adaptive steganography method GMAS builds upon dither modulation by utilizing asymmetric distortion and expanded embedding domains, resulting in enhanced security and resilience against compression [17].

**3.4 Brief Discussion on Problem**

For our method, we have adopted a neural network which is similar to [16], albeit a smaller one. Seeing the original paper, we were motivated to not treat the secret image as the data, but consider it as a carrier image as well. The actual data will be hidden inside this secret image which will be embedded. A smaller network is very easier to train and modify, while giving us the flexibility to work with a cover and secret image of any size.

To tackle the problem of adversarial attacks, we have divided the secret image into smaller parts and used chaotic mapping to scramble the order of the parts, thus requiring the original network as well the key of the chaotic map to actually retrieve the embedded secret.

Additionally, to protect our data against compression, we have used a Reed Solomon encoder with a custom (N, K) value, to add some redundancy and error protection.

**3.5 Organization/Planning**

To ensure the project is completed and successful, we have setup the following schedule with consecutive steps, along with planned alternatives if certain objectives are failed to be met:

1. Build and test the vanilla neural network from [16] – *Done*
2. Test the neural network with changed parameters to improve performance – *Ongoing*
3. Test the neural network against compression – *Ongoing*
   1. If failed – Redesign both encoder and decoder network with new techniques like in [17]
4. Build Chaotic Map implementation – *Ongoing*
5. Scramble and unscramble secret image using chaotic map - *Ongoing*
6. Build Reed Solomon Encoder (insert citation??) – *Done*
7. Embed Data into secret image using Reed Solomon – *Ongoing*
8. Test neural network with embedded data – *Yet to do*
   1. If unsatisfactory – redesign network with reduced colour channels to reduce net payload and increase network stability
9. Test neural network against: - *Yet to do*
   1. Other image data sets
   2. Other papers
   3. Steganalysis tools like StegExpose (insert citation)
   4. Real world (social media) applications

**4. Concepts and Problem Analysis**

**The Neural Network**

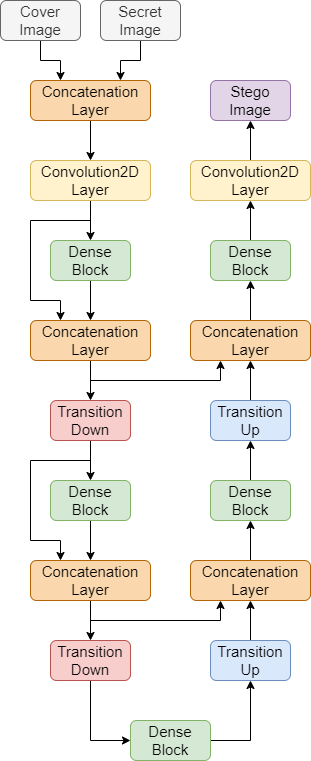
The deep neural network which has been designed for this project takes inspiration from the original paper [16]. We, however have scaled downed the network to a much shorter size, which we believe will make both training and deployment more efficient. The neural network uses concepts from the FC-DenseNet [18] architecture and the U-Net [19] architecture.

Figure 1 The Encoder Architecture

FC-DenseNet a deep learning architecture designed for semantic segmentation. It extends the DenseNet framework by integrating fully convolutional principles, making it suitable for pixel-level predictions. FC-DenseNet is composed of dense blocks, where each layer connects to all previous layers in the block, promoting feature reuse and efficient gradient flow. Transition down layers reduce the spatial dimensions, while transition up layers use transposed convolutions for up-sampling and restoring spatial resolution. Skip connections integrate features from earlier layers for precise segmentation. This architecture is highly memory-efficient, robust against vanishing gradients, and excels in handling complex datasets with detailed segmentation needs.

U-Net a convolutional neural network designed specifically for semantic segmentation. It features a symmetric encoder-decoder architecture. The encoder path extracts features using convolutional layers and reduces spatial dimensions through max pooling, capturing context and high-level semantics. The bottleneck layer connects the encoder and decoder, processing the most abstract features. The decoder path restores spatial resolution through transposed convolutions and integrates detailed spatial information via skip connections, which link corresponding layers in the encoder and decoder. U-Net is lightweight, highly effective with limited training data, and capable of producing accurate segmentation maps.

Figure 1 shows the architecture of our encoder network. The neural network takes in two 16x16x3 blocks, one is the cover image while the other is a secret image.

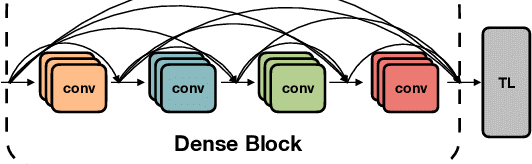
The encoder network consists of 121 layers, 15 connections and 389.4 k parameters. In terms of layers, the network has 5 dense blocks, 2 transition up and down blocks respectively, and 4 skip connections. Each dense block in turn consists of a 4 sets of batch normalization layer, relu regularization layer, a 3x3 2d convolutional layer with 12 filters and a dropout layer. This being a dense block architecture, every set receives the inputs of every preceding set. Figure 2 show how each set of layer receives the input and output of the previous layers. The transition up block is made of a single 3x3 2d transpose convolutional layer, while the transition down block consists of a batch normalization layer, a relu regularization layer, a 1x1 convolution layer, a dropout layer and a 2x2 max pooling layer.

Figure 2 A single dense block

The encoder network is trained using the loss formula:

where c is the original cover, c’ is the generated cover, β is a hyper parameter and ν is the error of the decoder.

The Decoder network has a much simpler linear architecture. It has 17 layers, 16 connections and 742.6 k parameters. In terms of layers, it has 5 sets of 3x3 2d convolution layer, batch normalization layer and relu regularization layer, followed by a final 3x3 2d convolution layer with an output of 16x16x3 layer, which is the extracted secret image. The input is a single 16x16x3 stego-image.

The Decoder network is trained using the loss formula:

where s is the original secret image and s’ is the extracted secret image.

**4.1 Chaotic Map**

A chaotic map is a cryptosystem that generates nonlinear and sophisticated random sequences for encrypting original data. First introduced in cryptography in 1989, chaotic maps utilize nonlinear iterative functions to produce chaotic sequences, which exhibit sensitivity to initial conditions and control parameters. These control parameters act as secret keys in cryptographic systems, enhancing security. The unpredictable nature of chaotic maps makes them ideal for applications such as secure communication, random number generation, and image encryption.

In our project, we will be using Logistic Sine Mapping, which combines the logistic map and the sine function to create more complex chaotic behaviour. Its formula is:  
Here, r is the control parameter, and is the current state. The sine function amplifies non-linearity, producing intricate patterns and increasing unpredictability. Logistic sine maps are particularly suited for cryptographic applications, as their output is highly dependent on control parameters, providing an added layer of security.

This r value will be required both at the time of encoding and decoding, and will act like a key. The scrambling order of the smaller 16x16 blocks of the secret image will be determined with this function. This will result in a more secure embedding, and protect the data from interpolative adversarial techniques.

**4.2 Reed Solomon Encoding**

To face the problem of neural network related losses and also compression related losses, we have used a Reed Solomon encoder to ensure protection against data loss. More specifically – we will be using a (240, 144) RS encoder and decoder. Since we cannot directly hide the secret data into the cover image as the neural network is convolutional in nature, we will be modifying the bits in the secret image in the following way –

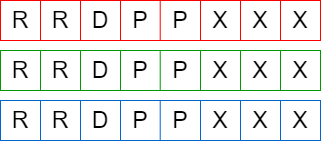
1. First, we divide the original 16x16x3 block into two 8x16x3 blocks.
2. For each of the 8x16x3 block, we initialize the (240, 144) RS encoder/decoder with the symbols having 8 bits each.
3. Again, we divide the 8x16x3 block into 16 4x2x3 blocks, where we define our required symbols:
   1. R – Reserved bits, extracted directly from the secret image to preserve context

Figure 3 Bit usage in RGB channels of one pixel

* 1. D – Data bits, where we embed our data
  2. P – Parity bits, for recovery against data loss
  3. X – Don’t care/ignored bits

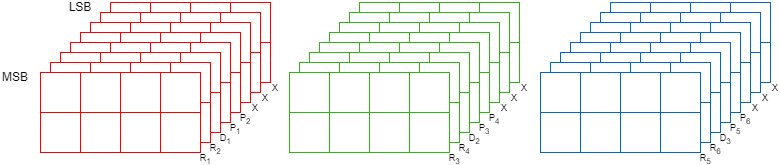
1. In a single 4x2x3 block, we have 6 Reserved symbols, 3 Data symbols and 6 Parity symbols. Each symbol will have 1 bit from every channel i.e., first Reserved symbol will have 1 bit from Red channel of every pixel, second Reserved symbol will have 1 bit from Red channel of every pixel and so on. The assignment will occur from the most significant bit of the pixels, as we have observed that bit errors mostly occur in the least significant bits of the colour channels.

Figure 4 How the symbols for RS encoding are embedded

1. We first extract all the Reserved bits from the 16 4x2x3 blocks and convert them into 96(=16x6) Reserved symbols. Next we get 48(=16x3) Data symbols worth of data and feed them into the RS encoder to generate the 96(=16x6) Parity symbols.
2. Now we embed the Data symbols and the Parity symbols into the secret image, which is now ready to be the input of our neural network.
3. On the decoding cycle, we simply extract all the Reserved, Data and Parity symbols from the decoded secret image and feed them into the RS decoder to get the original data error free, after first discarding the reserved symbols.

Since we have a (240,144) Reed Solomon encoder, we can correct a maximum of 48(= [240-144]/2) symbol errors in an 8x16x3 block i.e., 96 symbol errors for the entire 16x16x3 block, which should be more than enough. Again, we have opted for RS encoder as we expect to get burst errors (if any at all) from the decoding process, which will affect not only a particular pixel, but also its neighbours. Spreading the symbols to have data bits from different pixels help mitigate the burst error by containing it within a single symbol. The unaffected symbols can carry the data safely.

**5. Conclusion**

The findings from our literature review strongly indicate that methods incorporating neural network-based embedding techniques consistently demonstrate superior embedding ratios and enhanced robustness. However, these advantages come at the expense of higher computational requirements and increased architectural complexity. Despite these challenges, we believe that this represents the most appropriate and forward-thinking direction for the field. By achieving higher embedding ratios, future researchers will have the potential to implement more sophisticated and resilient error detection and correction techniques, addressing current limitations in the area of image-based steganography.

The current situation of our projects reflects a very positive outcome regarding the project’s success. We are currently putting the network under thorough tests, both to figure out its limits and solidify the hyper parameters. The avenues of a more error free data transmission by employing Reed Solomon encoding and Chaotic map scrambling are under development. If any problems are faced, we will employ methods from the already explored literature, and strengthen them further.

Another essential step is to test these methods on more diverse datasets and optimize computational efficiency. This would allow for the practical application of steganography in environments with limited resources, while still maintaining high performance. Expanding modalities to include multimedia formats and refining techniques for error correction codes and robustness against image processing operations will also play a vital role in ensuring that these methods remain effective in a rapidly evolving digital landscape.

**References**

|  |  |
| --- | --- |
| [1] | O. Ronneberger, P. Fischer and T. Brox, “U-Net: Convolutional Networks for Biomedical Image Segmentation,” arXiv, 2015. |
| [2] | S. Jégou, M. Drozdzal, D. Vazquez, A. Romero and Y. Bengio, “The One Hundred Layers Tiramisu: Fully Convolutional DenseNets for Semantic Segmentation,” Montreal, 2016. |
| [3] | Wencheng Yang , Song Wang , Jiankun Hu , Ahmed Ibrahim, Guanglou Zheng , Marcelo Jose Macedo , Michael N. Johnston and Craig Valli, “A Cancelable Iris- and Steganography-Based User Authentication System for the Internet of Things,” MDPI, 2019. |
| [4] | Zhuo Zhang, Jia Liu, Yan Ke, Yu Lei, Jun Li and Minqi, “Generative Steganography by Sampling,” IEEE, 2019. |
| [5] | ke, Y., Zhang, Mq., Liu and J. et al., “Generative steganography with Kerckhoffs’ principle.,” Springer, 2019. |
| [6] | Jun LI, Ke Niu, Liwei Liao, Lijie Wang, Jia Liu and Yu Lei & Minqing Zhang, “A Generative Steganography Method Based on WGAN-GP,” Springer Nature, 2020. |
| [7] | Abikoye, O.C., Ojo, U.A., Awotunde and J.B. et al, “A safe and secured iris template using steganography and cryptography.,” Springer, 2020. |
| [8] | Jiaohua Qin , Jing Wang , Yun Tan, Huajun Huang , Xuyu Xiang and Zhibin He, “Coverless Image Steganography Based on Generative Adversarial Network,” MDPI, 2020. |
| [9] | H. Wu, F. Li, X. Zhang, K. Wu, H. Wang, Y. Shi, H. J. Kim and A. Piva, “GAN-Based Steganography with the Concatenation of Multiple Feature Maps,” Springer, 2020. |
| [10] | X. Duan, L. Nao, G. Mengxiao, D. Yue, Z. Xie and Y. Ma, “High-Capacity Image Steganography Based on Improved FC-DenseNet,” IEEE Access, 2020. |
| [11] | X. Duan, L. Nao, G. Mengxiao, D. Yue, Z. Xie and Y. Ma, “High-Capacity Image Steganography Based on Improved FC-DenseNet,” IEEE Access, 2020. |
| [12] | H. Fu, X. Zhao and X. He, “Improving Anticompression Robustness of JPEG Adaptive Steganography Based on Robustness Measurement and DCT Block Selection,” John Wiley & Sons, Ltd, 2021. |
| [13] | Yuan, C., Wang, H. and P. et al., “GAN-based image steganography for enhancing security via adversarial attack and pixel-wise deep fusion.,” Springer, 2022. |
| [14] | Zhao, Wang, S. and J., “A stable GAN for image steganography with multi-order feature fusion.,” Springer, 2022. |
| [15] | D. Prabhu, S. Vijay Bhanu and S. Suthir, “Privacy preserving steganography based biometric authentication system for cloud computing environment,” Elsevier, 2022. |
| [16] | Garg, M., Ubhi, J.S. & Aggarwal and A.K., “ Neural style transfer for image steganography and destylization with supervised image to image translation.,” Springer, 2023. |
| [17] | Amina, Y., Bekkouche, T., Daachi and M.E.H. et al., “A novel trigonometric 3D chaotic map and its application in a double permutation-diffusion image encryption,” Springer, 2024. |
| [18] | Jasmine, R.M., J. & Geetha and M.R., “An efficient secure cryptosystem using improved identity based encryption with multimodal biometric authentication and authorization in cloud environments.,” Springer, 2024. |
| [19] | Vian S. Al-Doori, Mohammed Abdul Jaleel Maktoof, Abdulqader Faris Abdulqader, Serhii Lienkov, Alejandro Nicolás-Sánchez, Francisco J. Castro-Toledo, Md Thouhedul Alam Tonoy, Namita Munjal, Ridam Aditya Sinha and Ariyan Paul, “Incorporating iris, fingerprint and face biometric for fraud prevention in e-passports using fuzzy vault,” IET, 2024 |