International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

A novel approach for Secure IoT Architecture Using Deep Learning-Based Image Steganography and Multi-Factor Authentication-A Review

Sharath Babu CG
Research Scholar, Assistant Professor
Department of Computer Science and Engineering,
SSIT, Sri Siddhartha Academy of Higher Education,
Karnataka, Tumkur 572105
Email: sharathbabucg@ssit.edu.in

Dr. Komala K
Associate Professor
Department of Electronics and Communication Engineering,
SSIT, Sri Siddhartha Academy of Higher Education,
Karnataka, Tumkur 572105
Email: komalak@ssit.edu.in

***Abstract* - IoT systems employ image steganography more to reliably transmit data between devices since they care a lot about privacy and data quality. Two old ways that don't work in real life and don't stop modern steganography techniques are Least Significant Bit (LSB) encoding and alterations in the frequency domain. In this scenario, deep learning has proven useful. Two new technologies, autoencoders and generative adversarial networks (GANs), make it easier to identify and generate private, personalized tunes. These tools might also help you make more room for texts. But new systems have problems like technological overfitting, long wait times on multiple lines, and having to pick between data and security all the time. Steganalysis has come a long way over the years. It began with simple algorithms, but now deep learning systems use the Visually Robust Image Steganography (VRIS) model, DCT-based steganography, and transform-domain approaches. This article looks at the problems that come with common approaches and how JPEG compression, noise, and shape changes affect them. The study's purpose is to learn more about these new methods that combine content-adaptive embedding, convolutional neural networks, and adversarial training to make the photos harder to recognize and better. Use HILL or WOW to look for something. Use J-Uniward or UERD to alter something. The study's purpose is to find ways to improve and simplify steganography for everyone who uses it in the future. This will assist keep communication networks safe that need more than one type of ID.**

Keywords: Image Steganography, Deep Learning, Generative Adversarial Networks, IoT Security, Multi-Factor Authentication.

I. INTRODUCTION

Sharing private information properly is more crucial than ever as IoT devices and digital communication become more prevalent. "Steganography" is a method that works well with a lot of various types of coding in this case. Steganography is a better approach to keep hidden messages safe. Digital photos are used a lot in communication networks these days, and it's easy to hide them in other files. This is why picture steganography is becoming more widespread. In contrast, picture steganography only works properly when three things happen. It's not easy to keep something from being seen by people and computers, make sure it can handle a lot of weight, and make it hard for people to make mistakes when talking to each other. These aims are hard, which means that a lot of new steganography work needs to be done. The very hard math that goes into making safe steganographic systems today primarily comes from deep learning.

A. Image Steganography Using Deep Learning

Image steganography is very important for keeping data private while it is being sent in today's digital environment. It adds extra information to photos to keep them from being seen by other people. People can talk to each other in private and quiet here when safety isn't possible or necessary. This feature makes sure that no one can see your conversations. Image

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

steganography is used by a lot of digital watermarking tools to assist users secure their rights and make sure that content is legitimate. Encoding in the Least Significant Bit (LSB) and modifications in the frequency domain are ancient methods that are usually simple to spot and not robust enough to stop today's powerful signal-processing attacks. Steganography, like math, can help with security issues that are continually evolving. This means that individuals have been trying to find more difficult and beneficial solutions to fix problems with steganography security. Picture steganography has improved a lot since deep learning became more popular. This led to people finding more useful, better, and more effective covert techniques [3]. Two tools that have taught to encode and decode functions at the same time are auto encoders and generative adversarial networks (GANs).

Methods based on GANs use the generator-discriminator game to make stage pictures look more lifelike and harder to figure out. Autoencoders make little hidden models, that let you add things quickly and make sure they are correct [4]. These deep learning techniques help you get better at writing secret notes. Some of these problems are preserving enough data, dealing with modifications to photographs, and making files smaller. There will still be a significant, genuine problem if you accomplish these things. You could call this "mechanical overfitting." A lot of systems still employ an encoder-decoder chain that doesn't make sense. This method makes the secret code and its copy look practically the same. The shared feature generator actually works better with training data since it gets used to it. If the software or information doesn't work this way, it could be slower. But a lot of pipelines only witness a small part of the data transfer process. This is because they only operate well with one type of distortion model [5] or a little bit of noise, such Gaussian noise. So, they don't work as well when more particular types of problems are applied, such as JPEG quantization, impulse noise, complicated sensor noise, blur, geometric warps, weather-like faults, and random erase. The suggested model won't work on this data set since it's too small. Its training method is too focused on channels, and it has one encoder-decoder path that is linked to a small perturbation model [6]. This is why the most advanced models in real life usually can't do both scene accuracy and secrecy when they are capturing, compressing, and transferring data.

B. Steganographic approach for enhanced data security

You can counter steganography with steganalysis. The major purpose is to locate secret information and maybe stop people from chatting to each other in private. "Steganalysis" is a name for a strategy to keep yourself safe from risks that are hard to see. Figure 1 shows two fundamental reasons why steganography should be used: and utilizing languages to keep messages secret

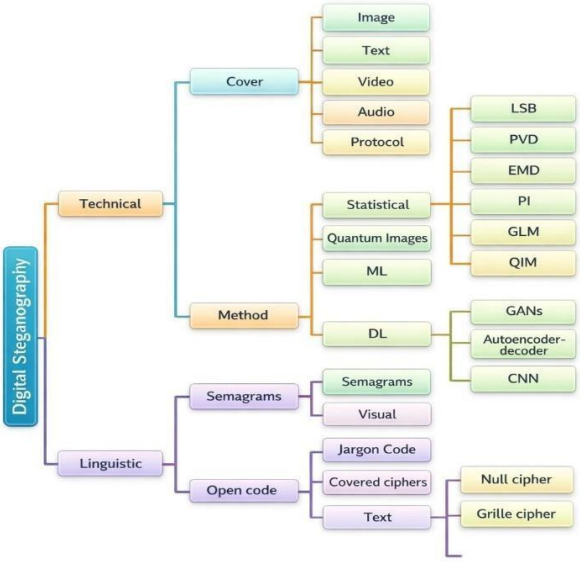

FIGURE 1: TAXONOMY OF STEGANOGRAPHY.

The digital world is increasing quickly, so we need to protect our data from hackers and make sure that touch is safe. Because of this, a number of technological solutions have been suggested to improve matters. Some of them are stenography, watermarking, and coding. Every plan has its good and bad points. Cryptography makes sure that data is safe, hidden, and easy to get to. Cryptography is a means to keep information from getting lost while it's being sent. Steganography is a way to hide information in text, movies, music, photographs, and other types of media. Watermarking is a very special type of steganography that is used to secure and keep track of intellectual property. Steganography have one unique benefit over both cryptography and watermarking [8]. When you use steganography to hide data, the media it is hidden in

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

looks a lot like the media it is concealed on. Deep learning (DL) is a novel and interesting technique to keep what you know secret. It can store and retrieve information in methods that are less likely to be discovered [9]. The "Related work" section has short summaries of other works that are similar to this one. As steganography gets better, deep learning approaches will undoubtedly become quite crucial for the field's future progress. But the most important thing is to make tools that are useful, work effectively, and don't get in the way.

Even with all these advancements, steganography methods are still facing a lot of challenges. These methods modify the cover material a lot, which makes them a little less good at disguising steganography [10]. LSB steganography and other simple methods of disguising messages are easy to employ, but they don't always function effectively against other approaches. Deep learning methods that are newer are safer, but they make the system harder to use and fit too many times. Also, a lot of older layouts don't have a lot of space, so you can't hide a lot of information unless you change the cover photo a lot. Most of the methods we use today also have trouble finding a balance between hiding data and making sure it is strong enough to keep it safe from harm or changes while it is being sent. The goal of this study is to figure out what went wrong in previous experiments. For ideal compression, Huffman encoding will be used. For speedy data entry, LSB will be used; and for safety, deep learning is used. This is a strategy to obscure information called "stacked steganography."

Many individuals still use LSB encoding and other older methods to hide data since they are easy and work well. Still, these strategies aren't quite right in a lot of essential aspects [11]. For instance, hacking LSB encoding is rather easy. There are two techniques to accomplish steganography, and you can use either one to do this. Deep learning is especially helpful when steganographic systems have problems [12]. Convolutional neural networks (CNNs) and encoder-decoder designs are examples of deep learning models that make things better by modifying the data. This is not the same as deep learning techniques that adapt to and mimic the statistical characteristics of the cover media.

C. Challenges

Here are five big issues with using deep learning-based picture steganography in IoT systems:

1. Mechanistic Overfitting and Limited Generalization

Most steganographic systems that use deep learning currently use only one encoder-decoder chain that doesn't understand anything. It also believes there are numerous methods to communicate and transmit confidential messages. When the payload or channel conditions are different from those during training, the shared feature collector looks at the training data that happen the most often. This makes things less efficient. This framework is very complex, which makes things a lot more difficult. In a lot of IoT contexts, it doesn't perform properly.

2. Robustness Against Diverse Channel Perturbations

A lot of ways to hide information work better if you make a few tiny tweaks. Most of the time, these merely contain one distortion model or some Gaussian noise. JPEG quantization, impulse noise, complicated sensor noise, blur, geometric warps, weather-like effects, random erasure, and other changes that happen in the actual world can all make them lose a lot of quality. This channel overfitting will fail if you don't conduct capture, compression, and transmitting correctly.

3. Payload Capacity-Security Trade-off

It's still hard to find a good balance between giving people power and keeping them safe. LSB steganography and similar approaches are quite beneficial, however when the cover medium changes a lot, other steganography methods can find them more easily. Using simpler machine learning methods makes it less likely that overfitting will arise. They are safer, but they are also harder to use and cost more. Because of this, people in the actual world can't use as many tools as they used to.

4. Computational Complexity and Scalability

When there are a lot of feature elements, it becomes much harder and more expensive to quickly train models and make them operate well. SPAM has 686 feature variables, but SRM has 34,671. Deep learning models can be useful, but they might not

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

work on IoT devices because they can't accomplish things on their own and don't have enough power to do so.

5. Detection Resistance Against Adaptive Steganalysis

Steganography also grows better at hiding information in ways that are harder to find and more adaptable. Steganography systems are always trying to outdo each other by coming up with new ways to avoid detection by strong machine learning-based steganalysis tools, while simultaneously keeping their strength and anonymity.

D. Motivation and Contribution

When it comes to data, IoT devices need to be safer and more secure. Deep learning-based photo steganography is a good approach to keep things secret. We need additional high-tech technologies that can keep private information safe in photographs while maintaining the picture and sound quality good because digital media and connected devices are expanding so quickly. Steganography is an old practice, but the ways people used to do it aren't safe anymore. This is because it is easier to break them with more complex steganographic analysis methods, and thus can't be employed in many real-life transfer circumstances. Deep learning approaches like generative adversarial networks and autoencoders can help with these problems by using variable embedding methods that know what they're embedding. There needs to be more investigation into things like how well the model fits the data, how the channel changes aren't stable, and the basic trade-off between security and production. This review paper aims to examine the evolution of photo steganography from traditional techniques to contemporary approaches employing deep learning, alongside an evaluation of their practical efficacy. The authors also seek to find crucial areas of study that will assist make a difference in the future of properly sharing data in Internet of Things situations. The study's aim is to facilitate the development of enhanced steganographic tools. These systems must be able to meet the strict requirements of today's safe chatting networks. They have to find a balance between four things: data capacity, processing speed and quality, strength, and visibility. We can achieve this by applying the newest methods and pointing out the faults from the past study.

6. Key Contributions:

An overview of deep learning-based steganographic designs, including GANs, VRIS models, autoencoders, and methods operating in the transform domain. The goal of this study is to figure out what makes the IoT safer or less safe. To identify significant issues, we must enhance our understanding of structure overfitting, channel-specific training constraints, and the payload-security trade-off that constrains steganographic systems. A complete book goes over the basics of steganalysis algorithms like SPAM, SRM, and DCTR, how to develop your own secret ways, and even today's deep learning systems. This shows how technology is always competing to find new ways to hide information and find new ways to do things. We call this process evolution mapping.

The Multi-Domain Technical Assessment has a lot of information about numerous methods to do things. All of these algorithms work in the spatial domain: LSB, WOW, and HILL. Changes in data are used by DCT, DWT, J-Uniward, and UERD. Some of these use networks of neurons. This test analyzes how well these methods work by seeing how well they can handle different kinds of changes, such as noise patterns, JPEG compression, and changes in shape.

Analysis of the Integration Framework:

- This part explains how to utilize multi-factor identification and steganography together to make sure that the Internet of Things (IoT) is totally safe.
- This study examines the utility of items, including the power requirements and operational speed of a computer.
- The act of learning new things and deciding what to do next. It's quite important to find the regions that need more research.
- For instance, we need hybrid architectures, content-adaptive embedding tactics, multi-scale feature extraction processes, and practical solutions that can work in the real

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

world and still be useful in regions with few resources.

II. RELATED WORK

Picture steganography has come a long way in the previous few decades. This transition happened because of a "arms race" between tools that look for information (steganalysis) and tools that hide information (steganography). The purpose of this part is to read about both new and old ways to do steganography and steganalysis. Things have gotten harder as additional safety issues came up. First, let's look at a few alternative techniques to accomplish steganography. Over time, these thoughts and acts have affected how we see other individuals. Next, we'll talk about more advanced methods that use deep learning. All of this makes it much safer for users to exchange pictures to one another.

A. Traditional Image Steganalysis Algorithms

When professionals need to get information that isn't clear, they use feature extraction methods that they made themselves. A lot of picture steganography tools use this method to get their work done. There are three steps to getting features, modifying features, and identifying groupings [13]. The LSB method, for example, works in the spatial domain, while the JSteg algorithm works in the frequency domain. All of these choices have helped find great examples of steganography. These strategies have worked quite well. You can utilize LSB to hide data by modifying sections of a picture that don't matter. The JSteg approach, on the other hand, hides the information by modifying the values in the discrete cosine transform (DCT). These methods of steganography modify a lot about the data properties of a picture while adding new information.

This shows that they aren't actually secret, yet steganography can still be used. These steps were used to make a lot of famous steganography models. Some examples of these models include the Subtractive Pixel Adjacency Matrix (SPAM), the Spatial Rich Model (SRM), the Discrete Cosine Transform Residual (DCTR), the Projection Histogram Rich Model (PHARM), and the Gabor Filter Residual (GFR) [14]. But as steganography gets more complicated and better at hiding things, it also gets harder to understand and apply. This method makes the flaws with common steganography approaches easier to see. Adaptive steganography methods are not like other approaches that always hide information in the same way. These strategies affect how information is hidden immediately away. When things get hectic and it's hard to articulate what's going on, this helps them keep things to themselves. The update makes it difficult to find information that isn't easy to get to. Figure 2 shows how the typical fixing procedure works. This is how flexible steganography works.

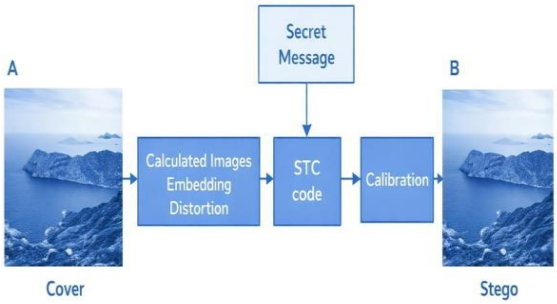

FIGURE 2. ADAPTIVE STEGANOGRAPHY EMBEDDING: COVER AND STEGO IMAGES.

Since flexible steganography was invented, it has grown harder to hide information. These innovations have also changed the usual methods people hide information. For example, the number of feature elements that normal study tools can manage has expanded a lot. Spam had just 686 measurements, but SRM had 34,671. The price goes up a lot since feature factors develop quickly. This condition also makes it a lot harder for the model to learn and modify quickly.

B. VRIS Image Steganography Model

This work creates the VRIS picture steganography model (Figure 3). The goal is to finish the picture-based steganography as rapidly as possible. The goal of this research is to fool both AI and people who look at pictures. Two machine learning methods that Unsupervised Learning (VRIS) is built on include "autoencoders," which learn how to rebuild data, and Generative Adversarial Networks (GANs), which use a generative-discriminative structure to learn. This algorithm is an example of a system that learns on its own.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

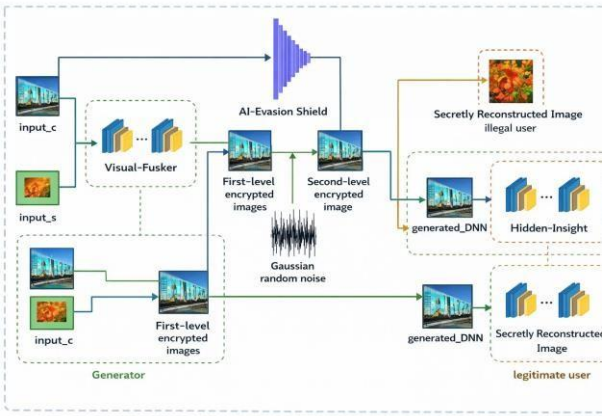

FIGURE 3. BASIC VRIS STEGANOGRAPHY NETWORK DESIGN.

C. VRIS Model Architecture and Design

The VRIS model has three important parts:

This tool can find sections of a picture that are hidden by employing convolutional kernels of different forms. It is called the Visual-Masker Module. Combining features is easy with convolution with several layers and batch leveling methods [15]. The main photo exhibits these qualities when the process is over. It's hard to tell from the cover that the picture is first-level encryption. The AI-Evasion Shield's This program can still discern the difference between cover pictures and second-level protected photos, even when the encryption generates a lot of noise. It makes the hard training approach of steganography better and keeps the machine learning model safe from additional threats. Before handling a photograph that is protected at the first level, random noise is applied to it. This makes the scene much more mysterious and confusing. The effect makes it look like the second floor is safe. You can handle this kind of visual, but it keeps changing and showing up at random times. Randomness makes sure that every piece of noise is different, while controllability makes it easy to change the study. You can test a variety of various things by changing the noise level of a situation. Adding noise makes some portions of a picture tougher to view. This method hides the secret picture better, making it harder to detect and safer from possible dangers.

D. Deep Learning-Based DCT Image Steganography

In classic picture steganography, there are two types of methods: spatial-domain and transform-domain. In space, secret hints are used to modify the colors of items to hide information. These methods don't modify the picture, and they usually operate with spatial data that stays the same. The WOW approach looks for insertion problems and local stability by using directed filters. The program also hides information by putting it in multiple places in a nice way. The HILL method [16] uses data from high-pass, low-pass, and Laplacian filtering to figure out how much it would cost to add anything. This tool shifts words from the smooth side to the rough side. By moving the integers in the transform, transform-domain approaches hide information. This keeps the scene from getting too busy. Reference [17] developed a non-additive distortion model that preserves the borders of blocks in JPEG images. JoCoP, which stands for Joint Cost Learning and Payload distribution, employs attention processes to make better estimations about the costs of embedding and the distribution of the payload. Most of the time, these approaches rely on functions that they have altered. But set embedding patterns don't work effectively for steganography anymore because modern algorithms can quickly find these older ways.

Steganography that works in the frequency domain is getting less safe. Deep learning has opened up new and interesting possibilities for steganography in the past few years. According to [18], "implicit neural representations," or INRs, can leverage a deep cross-modal design to hide multiple types of data in cover pictures. There is also a way to hide a lot of data using steganography. This program utilizes a neural network to put one image within another image of the same size. created CEC, or Cross-Episodic Curriculum, which was supposed to help with integration based on transformers.

E. Deep Image Steganography

1. Image Encryption

Images include a lot of information and look a lot like each other, therefore they can't be utilized very often. People are employing chaos systems more and more to hide things in photographs [19]. The reason is because when there is chaos, you typically have to be careful with starting values, model parameters, ergodicity, and symmetry. Two important processes in photo encryption are rotation, which alters where the pixels are, and diffusion, which changes how many pixels there are. The improper order is being used for two steps. The weird way the unsteady systems acted split the

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

picture coding process into two parts. You can do these things on data at the pixel, block, RNA (six-bit), DNA (two-bit), and bit levels.

2. Image Steganography

Watermarking and steganography are two ways to hide data in pictures. But they all want different things. The first person is in charge of finding out who owns an image, and the second person generally talks about secrets. "Embedding" and "extracting" are two fundamental parts of picture steganography. The LSB method is particularly prominent in the field of location analysis. The least important part of the binary code is modified in the carrier picture to hide the secret picture. This is a straightforward, tidy, and helpful way to get things done. But it's not that strong. When photographs are modified, algorithms that function in the transform domain do a better job of keeping private data safe than those that work in the spatial domain. Reference [20] demonstrates numerous methods to effectuate the modification. Three examples of this kind of procedure are the discrete cosine transform (DCT), the discrete Fourier transform (DFT), and the discrete wavelet transform (DWT). In general, algorithms that work in the spatial domain are faster, but they are more likely to fail during an attack than those that function in the transform domain. This is because moves with names are harder.

3. Deep Learning

Deep learning (DL) is a kind of machine learning (ML) that has done better than regular machine learning on more classification and regression tests [21]. increasingly particular, deep learning-based picture steganography has been employed increasingly regularly lately. A lot of them are well-known, but CNN and generative adversarial network (GAN) are two of the most well-known. This kind of neural network (CNN) works well when used on data that can be seen. Before applying a convolution kernel (sometimes called a "filter") to get rid of extraneous data, a convolutional neural network (CNN) looks for patterns in the data. We need to know these things about these qualities. In [22], CNN-based steganography models utilize a "encoding network" to hide data and a "decoder network" to find it. People often utilize GANs, which are deep learning systems, to produce fresh copies of raw data that appear like the actual thing. You can also use them to detect the difference between true and fraudulent data. A GAN has two networks: a generator network and a discriminator network.

4. JPEG-Based Image Steganography

Some kinds of steganography work in the space realm. Others adjust the settings of the discrete cosine transform (DCT) that JPEG files store. There are various ways to make sure anonymity by using content-adaptiveness. Because most of the information in these systems is stored in less reliable places, it is harder to keep track of when modifications have been made to the data. We chose to look into these changes since they are hard to see. After looking at the outcomes of earlier studies, including [23], we decided to use nsF5 [24], JPEG universal wavelet relative distortion (J-Uniward), and uniform embedding revised distortion (UERD) [25]. The next lines give a brief example of what they are.

TABLE 1: KEY IMAGE STEGANOGRAPHY METHODS POLL

Method	Advantage	Disadvantage	Research Gap
Embedding LSB	Easy; high capacity	Not very strong against compression and strikes	Making things stronger without making them more complex
WOW or HILL	Adaptive anchoring in areas with roughness	Moderate ability to resist compression	Making it harder for a wide range of attacks to work
GAN-centered	Adversarial training; high stealthiness	Mechanistic overfitting; expensive to compute	Creating strong multi-modal GANs
Based on autoencoder	Efficient healing and embedding	Not very strong against changes	Building strong autoencoders with a lot of different training
VRIS Framework	Multi-module with two lie capabilities	Complex; needs a lot of training data	Making building easier while keeping safe
DCT-using	Resilient to JPEG compression	At high rates, block artifacts.	Adaptive strategy development
DWT-SEP] based on DWT	Analysis at multiple resolutions	How hard it is to implement	Automated picking of coefficients
J-Uniward or UERD	JPEG-optimized universal distortion	Takes a lot of computer power	Lowering the difficulty of deployment
Lowering the difficulty	flexible tactics that were learned	Needs training data in pairs	Unsupervised methods of training

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

of deployment			
built on transformers	Modeling of global setting	Very high cost for calculations	IoT gadgets that are efficient and easy to use
Adaptive to content	Lowered blurring; raised safety	The extra work that needs to be done by a computer	Content study in real time
Compression-based Sensing	Using compression Feeling Payload is lower, but quality is better.	Lossy recovery case	Getting perfect recovery

Steganography works sometimes. Some people tweak the discrete cosine transform (DCT) that JPEGs use. Being content-adaptive doesn't help anyone get found. A lot of these systems store data in places that aren't as safe, which makes it tougher to keep track of changes. We decided to check at these adjustments because they aren't particularly clear. We chose nsF5 [24], JPEG universal wavelet relative distortion (J-Uniward), and uniform embedding revised distortion (UERD) [25] as our techniques after looking at the outcomes of past work, such [23]. The next few lines give a little example of what they are.

F. Research Gap

1. Addressing Mechanistic Overfitting in Neural Architectures

The primary objective of the study should be to develop systems capable of altering their automatic arrangement of items upon the discovery of new information regarding the characteristics of the cover image and the anticipated conditions for transfer.

2. Enhancing Robustness to Comprehensive Perturbation Models

Add a lot of different noise levels to your workouts. JPEG compression at different quality levels, explosive noise, noise patterns that only some sensors exhibit, multiple blur kernels, changes in shape, random erasing, and flaws in both weather modeling and shape change are just some of the difficulties that should be grouped together. The best way to fix each incorrect model is not to try to make it better. The next stage should be to make systems that are stable and can work with a lot of diverse models.

3. Balancing Computational Efficiency with Security

We need to make deep steganographic methods better so they don't get caught. These changes will also aid the math that measures features, which is increasing very quickly. We need to look into neural architecture design, knowledge distillation, and making lightweight models that can be safely used on IoT devices with low resources.

4. Advancing Beyond Single-Path Embedding Strategies

One option to find content-based embedding methods that can work in multiple contexts is to use multi-branch designs or ensemble methods. This is because single encoder-decoder systems don't perform effectively when things are different right now. Some of these strategies entail coming up with new ways to use different steganographic technologies and hybrid models that combine the best parts of each.

5. Improving Steganalysis Resistance Through Adversarial Training

It's more difficult to set up elaborate active training systems in the training loop when you employ new steganalysis approaches instead of just simple differentiators. This is because you need to know that the information you gather will stay in the same place, even if new means to access it are created. One thing they are doing is adding things that don't assist, including feature-based steganography models and deep learning detection.

6. Creating Practical IoT-Specific Solutions

Make sure that the technologies you use for steganography work with the Internet of Things. These systems should be able to deal with a lot of different types of tool power and network circumstances, as well as changes in the needs of the organization straight away. It's preferable to make tools that actually work than models that only demonstrate that something might work.

III. CONCLUSION

The purpose of the project was to find new ways to employ deep learning in photo steganography. The next thing to do was explain about how the brain has altered over time. Some things have gotten better, but the packages are still too huge, not covert enough, and unsafe. It's becoming more clear that common approaches aren't the ideal way to do things because modern steganography can easily get around them. It's hard to get them to work in a different way in a lot of distinct relocation instances. When it comes to steganography, the deep learning method lets you use different embedding methods depending on the picture and the channel. Architectures like GANs, autoencoders, and transformers make stego visuals that look a lot like the actual thing and take up a lot of space. Here's a useful example of a model that learns from other people's data, avoids AI, and uses a multi-module system to hide data in different ways. It's that kind of type, the VRIS type. But mechanical overfitting is still a concern because models don't operate well when things in the real world change, such when engines have issues or new compression methods are employed. It's evident how hard these challenges are because the feature measurements go from 686 in SPAM to more than 34,000 in SRM. In the future, the most essential item to research should be blended designs that combine deep learning and multi-scale feature extraction along with content-adaptive algorithms and flawless compression. Combining multi-factor verification with steganography is an interesting technique to make the Internet of Things safer. These systems strive to find a compromise between transferring data safely, using computer resources effectively, and meeting the needs of real-time speed.

ACKNOWLEDGMENT

Not Applicable

REFERENCES

[1] Li M, Zhan J, Ge Y. Image progressive steganography based on multi-frequency fusion deep network with dynamic sensing. Expert Systems with Applications. 2025 Mar 10; 264:125829.

[2] Min-Allah N, Nagy N, Aljabri M, Alkharraa M, Alqahtani M, Alghamdi D, Sabri R, Alshaikh R. Quantum image steganography schemes for data hiding: a survey. Applied Sciences. 2022 Oct 13;12(20):10294.

[3] Shang F, Lan Y, Yang J, Li E, Kang X. Robust data hiding for JPEG images with invertible neural network. Neural Networks. 2023 Jun 1; 163:219-32.

[4] Shang F, Lan Y, Yang J, Li E, Kang X. Robust data hiding for JPEG images with invertible neural network. Neural Networks. 2023 Jun 1;163:219-32.

[5] Rehman, Mujeeb Ur, Arslan Shafique, and Aminu Bello Usman. "Securing medical information transmission between IoT devices: An innovative hybrid encryption scheme based on quantum walk, DNA encoding, and chaos." Internet of Things 24 (2023): 100891.

[6] El-Hajj, M., & Beune, P. (2024). Lightweight public key infrastructure for the Internet of Things: A systematic literature review. Journal of Industrial Information Integration, 41, 100670.

[7] Yuan, W., Chen, X., Zhu, Y. & Zeng, X. Http payload covert channel detection method based on deep learning. Netinfo Secur. 23, 53–63. https://doi.org/10.3969/j.issn.1671-1122.2023.07.006 (2023).

[8] Zhang, Z., Q. Lai, and C. Zhou. "Survey on fuzzing test in deep learning Frameworks." Netinfo Secur. 24, no. 10 (2024): 1528-1536.

[9] Wu, Xiaowei, and Hongxiao Zhu. "Association testing for binary trees—A Markov branching process approach." Statistics in Medicine 41, no. 14 (2022): 2557-2573.

[10] Mahmoud, Mahmoud M., and Huwaida T. Elshoush. "Enhancing LSB using binary message size encoding for high capacity, transparent and secure audio steganography–An innovative approach." IEEE Access 10 (2022): 29954-29971.

[11] Wani, Mohd Arif, and Bisma Sultan. "Deep learning based image steganography: A review." Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery 13.3 (2023): e1481.

[12] Wu, X. and Zhu, H., 2022. Association testing for binary trees—A Markov branching process approach. Statistics in Medicine, 41(14), pp.2557-2573.

[13] Coito, T., Firme, B., Martins, M. S., Vieira, S. M., Figueiredo, J., & Sousa, J. M. (2021). Intelligent sensors for real-Time decision-making. Automation, 2(2), 62-82.

[14] Jakaraddi HR, Kwari M, Haarika A. A Secure Web-Based Cyber Defense Framework using AES Encryption, Steganography and Machine Learning. International Journal of Computer Technology and Electronics Communication. 2025 Nov 19;8(6):11692-7.

[15] Kim, Kyoungok, and Jong Baek Kim. "Two-step model based on XGBoost for predicting artwork prices in auction markets." International Journal of Knowledge-based and Intelligent Engineering Systems 28.1 (2024): 133-147.

[16] Semwal, A. and Londhe, N.D., 2024. A multi-stream spatio-temporal network based behavioural multiparametric pain assessment system. Biomedical Signal Processing and Control, 90, p.105820.

[17] Oleiwi ZC, Dihin RA, Alwan AH. Improved framework for blockchain application using lattice based key agreement

protocol. International Journal of Electronics and Telecommunications. 2023;69(1):5-10.

[18] Shukla, S., & Patel, S. J. (2024). A design of provably secure multi-factor ECC-based authentication protocol in multi-server cloud architecture. Cluster Computing, 27(2), 1559-1580.

[19] Chen, J., Lu, Y., Yu, Q., Luo, X., Adeli, E., Wang, Y., Lu, L., Yuille, A.L. and Zhou, Y., 2021. Transunet: Transformers make strong encoders for medical image segmentation. arXiv preprint arXiv:2102.04306.

[20] Jiang, Yifan, Shiyu Chang, and Zhangyang Wang. "Transgan: Two pure transformers can make one strong gan, and that can scale up." Advances in Neural Information Processing Systems 34 (2021): 14745-14758.

[21] Vellela, S. S., & Balamanigandan, R. (2024). An efficient attack detection and prevention approach for secure WSN mobile cloud environment. Soft Computing, 28(19), 11279-11293

[22] Kaur, Harjeet, et al. "Using machine learning techniques in business analytics: lessons from agile project management." 2024 7th International Conference on Contemporary Computing and Informatics (IC3I). Vol. 7. IEEE, 2024.

[23] Vellela, S. S., & Balamanigandan, R. (2023). An intelligent sleep-awake energy management system for wireless sensor network. Peer-to-Peer Networking and Applications, 16(6), 2714-2731

[24] Liu, Y., Zhang, X., Li, Y., Zhou, J., Li, X., & Zhao, G. (2022). Graph-based facial affect analysis: A review. IEEE Transactions on Affective Computing, 14(4), 2657-2677

[25] Gupta, Sandeep, et al. "A survey of human-computer interaction (HCI) & natural habits-based behavioural biometric modalities for user recognition schemes." Pattern Recognition 139 (2023): 109453.