International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Robust and Secured Data Hiding Methodology over Digital Images using Deep Learning Enabled Steganographic Norms

V. Raja[1], K. S. Suresh[2]

Submitted: 16/02/2023 **Revised:** 19/04/2023 **Accepted:** 08/05/2023

Abstract*:* Steganography, as opposed to cryptography, is an art form for concealing information in a way that does not draw attention. Since ancient times, people have used this method to communicate and conceal sensitive information from strangers or hackers. Multimedia information is widely utilised as a result of the quick growth of computer networks, and digital media security has received a lot of attention. The facts of the case will be distorted by the manipulated photo used as forensic evidence, and social media photos that have been maliciously altered may harm the persons involved. Information-based digital image self-recovery concealing is used to assure the veracity and integrity of digital media. We suggest a multisource data-hiding system (MDHS), which extracts hidden information on the recipient's side and produces content that is jointly decided by the hidden information sent by all senders. Based on deep learning, this research draws a general conclusion on visual information hiding. Additionally, the suggested approach has the potential to enable lossless data recovery in the event of damage using the dynamic range adjustment technique. Modern information masking techniques based on deep learning are examined and shown. Simulation findings show that the suggested approach outperforms existing cutting-edge strategies in terms of payload and imperceptibility.

Keywords: *Data Hiding; Steganography; Data Embedding; Information Hiding; Digital Watermarking; Multisource;*

1. Introduction

Since the rapid advancement of technology has made the manipulation of digital media simpler, many researchers have turned their attention in the last ten years to the study of successful data hiding techniques. Therefore, it is crucial to create new methods that make it possible to stop the manipulation and distribution of digital content. A taxonomy of information concealment strategies and an explanation of their significance in various fields. One of these methods is steganography, in which a hidden message—which might be text, digital photos, audio, or video data—is concealed using the multimedia content as the cover medium.

A recent development in covert communication is steganography [1]. Steganography hides the existence of communications, whereas traditional cryptography hides the content of messages. Digital photos, videos, audio files, network packets, and other computer files that include perceptually pointless or redundant information can be used as carriers or coverings for hidden messages. We create a "stego-image" by inserting a hidden message into the cover photos. The stego-images must be free of any discernible artefacts caused by embedded messages that might be picked up by either human perception or machine detection algorithms. Only a specific set of bits can be used when using digital data as a data hiding method in order to ensure that the message 'remains secret' and is not detected by either humans or computers. The least significant bits (LSB) are substituted with the data to be hidden, allowing for bit changes while maintaining the integrity of the file. For this reason, the stenographic system must detect the superfluous bits.

Although steganography has been used for a very long time, it has recently attracted a lot of attention due to the development of the digital world, where secret information is concealed by altering data bits [2]. However, steganalysis is also developing at a comparable rate to counter this field. The discipline of finding hidden information in photographs is known as steganalysis. The natural activity of a picture, which is examined by sophisticated algorithms, gets distorted when data is incorporated in it. The least significant bits of the RGB components of the pixel are replaced with the secret data when using LSB modification for image steganography. As a result, each pixel of the image being communicated has some concealed information that may be recovered at the receiving end [3].

Self-embedding methodologies apply information concealment methods to embed the computerised picture's

1Department of Computer Science and Applications
SRM Institute of Science and Technology, Vadapalani, Chennai, Tamil Nadu 600026rajav@srmist.edu.in
2Assistant Professor
Department of Computer Science,
Rajeswari Vedachalam Government Arts College, Chengalpattu-603 001.
E-Mail : ksampathsuresh@gmail.com

inherent data into the image, without damaging the human organoleptic benefits [4]. In the event that digital media is intentionally modified or lost while transmission, self-embedding technology can glean reference data from shards of remaining electronic media data in order to reconstruct the manipulated portions of a picture. This aids in guaranteeing the originality and integrity of the information being provided.

Modern data concealing attempts to lessen the distortion on a particular cover picture that is brought on by the embedding technique [5]. To determine how much to charge for inserting each cover element, the user generates a distortion function in order to obtain the least amount of distortion possible. The distortion brought on the alteration may be measured using the embedding costs that were collected. Then, using a close to ideal steganographic coding, covert information is included into a picture with as little theoretical change as possible. [6].

Online sharing and transmission of digital media is currently widespread due to the rapid advancement of information technology. While this is happening, information hiding technologies like steganography, secret sharing, watermarking, etc. have drawn considerable attention due to the gradual realisation of the lack of protection for critical data in the sharing environment. In an effort to conceal the data's existence, data is embedded in digital media utilising the features of the human visual system (HVS). Images make up a sizable component of digital material, and they are widely used in daily life and have a high degree of representational redundancy. A good embedding method should, in general, accomplish imperceptibility and a sufficient level of embedding. The least significant bit (LSB) embedding technique, which embeds secret data using the spatial redundancy of digital images, offers the advantages of a high payload, strong visual imperceptibility, and simplicity of usage [7] [8].

In recent years, data concealing technology has advanced to the point that hidden information may be inserted into a particular cover media without suffering significant distortion. Digital photos are becoming the most extensively utilised kind of media for data concealment since they are regularly shared on social networks. The current generation of data-hiding techniques is built on a single sender, who transmits hidden data [15]. By employing numerous senders to broadcast various hidden information to a receiver while using the same picture, we hope to achieve data hiding in this study.

Steganography's main goal is to strengthen data and communication security by hiding a secret message within digital material without lowering the standard of the cover content, which should go unnoticed by HVS. Steganography, unlike cryptography, which aims to render the information unreadable, has recently grown significantly in importance in a wide range of application sectors, including the military and intelligence organisations, who employ secret communications.

In the current paradigm for data concealing, a sender inserts hidden information into a predetermined cover medium. The collected stego media are then anonymously sent across open networks. In some circumstances, such as when gathering military information, several spies (the senders) seek to deliver their commander (the receiver) various intelligence (secret data). In order to provide adequate security and effectiveness, the media also include various secret pieces of information that should only be conveyed once. Multisource data-hiding is preferred in this circumstance since the intelligence should be transmitted to the commander after being embedded into the same specific medium, as seen in Figure 1.

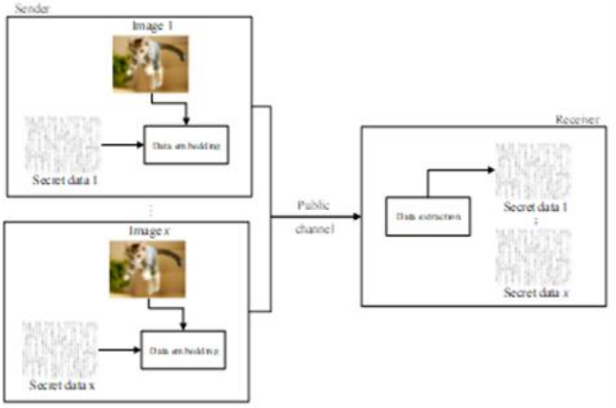


Fig. 1 Multisource data concealing concepts

The content that the receiver extracts is a co-determined consequence of all hidden information rather than the specifics, thanks to the multisource information hiding technique (MDHS) that we provide.

Both the recipient and the non-source senders are unaware of the specifics of the secret material. Different senders are assigned non-overlapping embedding locations in order to achieve the separable scheme. Data extraction occurs after the final data embedding process in the anonymous scheme, which employs sequential data embedding. The comparison of file sizes is a key element in steganalysis. Since it is common practise in the embedding group to throw away the initial cover picture after integrating the confidential information, researchers focus on the gadgets that were utilised to capture the picture. The size of the transmitted picture is then compared to the size of an additional image from the exact same device.

2. Related works

The internet is a crucial tool for communication in today's world, and images make up the majority of the digital material that is shared there. However, the safe transmission of data over the internet is now a significant problem. Many different techniques are employed to secure data or images, with hiding and encryption being the most widely used methods. According to the author's work [9], a hybrid model of digital picture security approach based on image concealing and encryption has been developed. Two levels of protection are to be given to a secret picture in this suggested approach. Using the LSB concealment approach, the secret picture is initially cloaked under a cover image before being converted into the stego image. Now that the stego picture has been obtained, the AES encryption technique has been used to encrypt the stego image.

A reversible data concealing approach for printing with unique colour inks was put out in paper [10] by the author. The particular colour layer is first digitally halftoned into a binary picture before being losslessly compressed using JBIG2. The specific colour layer is included into the normal colour layer during preprocessing. As a result, the same embedded picture may be used for both standard colour printing and printing using unique colour inks. Our test findings demonstrate that, while the embedded image quality is not visibly affected, the amount of information in the special colour layer is significantly reduced by the digital halftoning and JBIG2 image compression processes.

The web is the most famous and important method for the exchange of data in the present development. Electronic media has probably become one of the most well-known and important tools for moving information as the web and information creation have grown. Different strategies and methods are employed to secure these data. Data concealing and scrambling techniques are used to safeguard digital information in the case of picture and text data. The author of article [11] describes improved data security for digital images and text using a hybrid paradigm of data hiding and encryption. Utilised the XOR method for concealment and the AES algorithm for encryption.

Digital picture steganography techniques like differential expansion (DE) and pixel value ordering (PVO) show promise. PVO is a digital picture steganographic technique that deals with sorting pixel values prior to data embedding. DE is a data security technique used in digital picture steganography that conceals hidden data via differences calculated between pixels. Although the earlier PVO and DE-based methods attempted to increase both the capability of embedding as well as the quality of steganographic images will necessitate further research.. In order to increase the quantity of embeddable regions and the embedding capacity in the pixels of a digital picture, author [12] suggests a novel technique that combines PVO with DE. The testing findings revealed that using the current approaches, the maximum number of embeddable areas within utilised photos grew from 17582 pixels to 131009 pixels, resulting in an improvement in embedding capacity from 6.70% to 49.97%.

In [13], a foolproof method of data concealment via histogram shifting as well as visual secret communication is outlined. Using visual secret sharing, the hidden image is encrypted before being hidden within the host image. Encryption is achieved by splitting the hidden image into n equal parts. Each of these shares is held as an encrypted share by the Trusting Authority, whereas the remaining n are contained in the host image. In order to determine which of these n-1 parts is the k^{th}, the image is employed at the receiving end. The key share must be placed on the k recovered shares before the entire hidden data may be exposed. The extraction of the picture had the highest contrast and no pixel expansion thanks to the employment of the random grid approach and the XOR operation. Using the idea of histogram shifting, the shares have been included into the cover picture.

Digital signatures are an extremely useful verification tool for examining electronic documents, however they do not apply to digital photographs since they may not be validated by a digital signature due to a very little amount of interference. To achieve the double objectives of authenticating the copyright details of an electronic picture and retrieving the original picture without loss, the writer [14] proposes a reversible information-hiding solution with an identification function. After the confidential information has been disrupted, the digital image is then used to embed the QR-coded digital signature. When a digital signature is verified, all that is required is to use the reversible algorithm to extract the QR code from the stego image and restore it to its original state.

A median embedding block ratio of 87.42% is achieved, and the experimental findings show that the information that is reversible concealing approach may be used to conceal information of up to 6 bits per picture block. In addition to being secure against accidental assaults on image processing, this method successfully expands embedding capacity without degrading the quality of the carrier picture. The QR code has a high success rate for electronic identification because of its robust mistake correcting capacity.

3. Methodology

Image Steganography

The technique that is by far the most popular in today's digital world is hiding hidden messages in digital photos. This is so that it may make use of the human visual system's (HVS) finite power. Almost any type of material, including plain text, cypher text, images, and other types of media, can be concealed in a digital picture by encoding it as a bit stream. This discipline will expand extremely quickly as long as computers' ability to handle powerful visuals and the research being done on image-based steganography continue to improve. Steganography frequently uses 8-bit or 24-bit pictures. Images may be used to easily inject data in a variety of ways to conceal it. Using a rather convoluted method, messages may be encoded in 'noisy' areas while still adhering to the format/content of images. Additionally, the messages can be dispersed at random to encode images. Because of its ease of usage, the LSB approach is arguably the most well-known picture steganography method. The amount of information that can be concealed in an image depends on various elements, such as the number of least significant bits used for encryption, the pattern and contents of the image, etc. Specifically, the capacity of an image depends on its usable percentage, encoded bits, and pixel count.

Detect Tampered Area

Even though the image's size wouldn't change, an attacker may alter the watermark's content. The tamper rate is the percentage of blocks that include false information compared to all other blocks. After identifying the suspect image by its contained hash bits, the tampered block is located and its MSB is reconstructed with the use of reference material from adjacent blocks. The reference data obtained from the MSBs in the same subset are embedded across the whole picture, as was previously explained, and they come from various places. Even if purposeful tampering destroys most of the original MSB including associated reference information, a tampered MSB may be reconstructed with reliable reference information. Divide the image into 88-inch pieces and apply distortion. Each pixel's embedded bits contain the watermark, which is retrieved from them. Hash bits from the restored backup have been compared to the newly generated 32. If the 32 newly generated hash bits don't match up with the hash bits of the restored backup information, the block is considered to be "tampered," implying that part of the content inside the transaction has been changed. If the 32 hash bits in the archived information match the new 32 hash bits, we call the backup information a "reserved block."

Multisource Data Hiding Scheme (MDHS)

In other situations, such as anonymous voting, just the outcome is important and not the specifics of each voter's ballot. In this instance, the receiver is not required to know the contents of any hidden information communicated by numerous senders. In order to achieve this, we provide a covert multi-source data collection system in which the receiver's data are the codetermined outcome of all secret data rather than the specifics. The suggested scheme's workflow is depicted in Figure 2, where data embedding operations are carried out sequentially and data extraction follows the last embedding operation. Using the same data-hiding key *P*, the *x* senders sequentially incorporate secret bits $\{a_1, a_2, \ldots, a_x\}$ into a particular cover picture. A co-determined result $i(a_1, a_2, \ldots, a_x)$ of $\{a_1, a_2, \ldots, a_x\}$ is recovered on the receiver side, but the specifics of each a_k are kept secret. The information-hiding key P_0 that is only symmetrically possessed by the receiver and the initial sender, enables this. Here are the specifics.

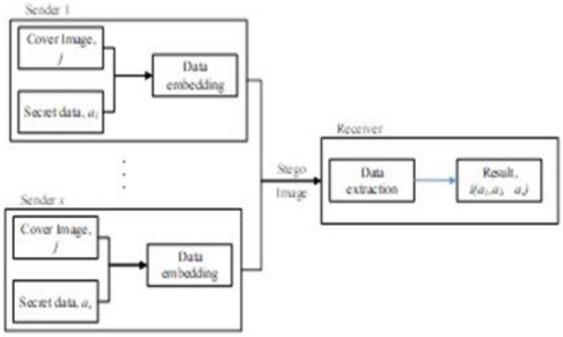


Fig. 2. Methodology for Encrypting Data from Multiple Sources.

Similarly, the LSB (least significant bits) of the cover image's pixels are used by the cover sequence $j = [j(1), j(2), \ldots, j(p)]^S \in \{0,1\}^p$ in anonymous data from multiple sources concealment. Anonymized data from multiple sources concealment is achieved by doing consecutive information embeddings of the *x* senders and then performing extraction of information at the receiver. When it comes to unnamed multisource information concealment, all *x* senders use the whole *j* for the embedding, while separated multisource information concealment divides *j* into non-overlapping portions. To put it another way, the k^{th} sender incorporates the kth secret bits a_k into j_k, where $a_k = [a_k(1), a_k(2), \ldots, a_k(R)]^S \in \{0,1\}^R$.

In a secret ballot election, the sum of all votes cast is the final tally (data collected by the receiver). That implies

$$i(a_1, a_2, \ldots, a_x) = \sum_{k=1}^{x} \varphi(a_k) \qquad (1)$$

where $\varphi(a_k) \in \{0, 1\}$ denotes either a dissident vote $\varphi(a_k) \in \{0, 1\}$ or a positive vote $(\varphi(a_k) = 0)$ from the *k*-th sender. The value of each $i(a_1, a_2, \ldots, a_x)$ on the receiver side should be retrieved, but the value of each $\varphi(a_k)$ should not be disclosed. R binary bits $a_0 = [a_0(1), a_0(2), \ldots, a_0(R)]^S \in \{0,1\}^R$ achieve this using the data-hiding key P_0. The last R_0 bits, $\{a_0(R - R_0 + 1), \ldots, a_0(R-1), a_0(R)\}$, are then set as $\left((x) < R_0 < R\right)$. Consequently, it is possible to calculate the bits in a_k as

$$a_k(b) = mod(\lfloor \gamma(i)/2^{b-1} \rfloor, 2), b \in \{1,2,\ldots,R\} \qquad (2)$$

where "*mod(·)*" represents the modulo operator, "⌊.⌋" translates to the habit of rounding down, and

$$\gamma(i) = \varphi(a_k) + \sum_{b=1}^{R} 2^{b-1}.a_{k-1}(b) \qquad (3)$$

Given that the receiving side's retrieved data is a_x, that is $\{a_x(1), a_x(2), \ldots, a_x(R)\}$, the method for determining the value of $\gamma(x)$ can be obtained by

$$\gamma(x) = \sum_{b=1}^{R} 2^{b-1}.a_x(b) \qquad (4)$$

Equations (1) and (2) also allow for the deduction that

$$\gamma(x) = \sum_{k=1}^{x} \varphi(a_k) + \sum_{b=1}^{R} 2^{b-1}.a_0(b) \qquad (5)$$

That is

$$\gamma(x) = i(a_1, a_2, \ldots, a_x) + \sum_{b=1}^{R} 2^{b-1}.a_0(b) \qquad (6)$$

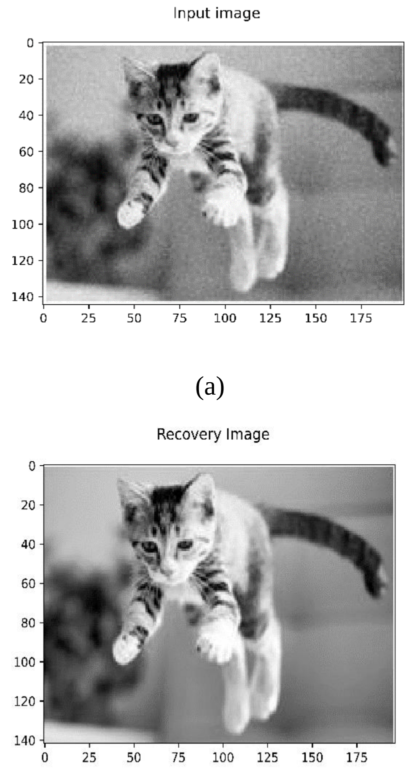
The receiver's possession of the data-hiding key P_0 determines the values of $\{a_0(1), a_0(2), \ldots, a_0(R)\}$ and as a result, the receiver may use this key to calculate the final result, $i(a_1, a_2, \ldots, a_x)$.

$$i(a_1, a_2, \ldots, a_x) = \sum_{b=1}^{R} 2^{b-1}.[a_x(b) - a_0(b)] \qquad (7)$$

Thus, the receiver side can obtain the coincidental endpoint (the sum of all $\varphi(a_k)$). The value of each $\varphi(a_k)$ will remain a secret in the interim. Since all senders have access to the same total number of secret bits, we settle on the integrating technique of repeated datahiding that additionally depends on the STC framework. The repeating embedding approach does not eliminate the distortion caused by data hiding, no matter the quantity of times the operation is performed. This allows for the maintenance of data hiding's invisibility during the *x* embedding durations.

Self-Recovery

Similar to how self-embedding watermarking is the opposite of image self-recovery. The identical key that was used before to identify the watermark information in the unaltered block is used to decode the sub-block when a tampered one is found. It can be applied to fix the unaltered block in the tampered region in order to provide a visual depiction. We create a reference based on the watermark data at the original spot in order to recover the image. Self-recovery images are obtained by first encoding the watermark information, then performing an inverse quantization and reverse discrete cosine transform (DCT), and then recovering, at least approximatively, the sub-blocks that were altered. The process of finding and recovering images. Input data and a self-Recovery picture are displayed in Figure 3.



(a)

(b)

Fig. 3. (a) Input Data and (b) Recovery Image

Steganalysis algorithms based on deep learning

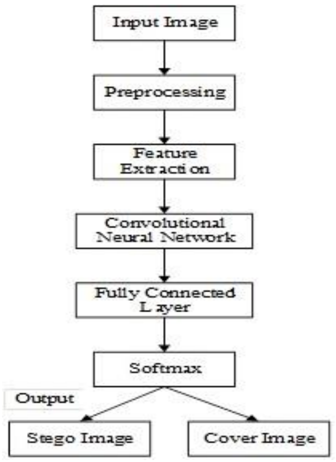


Fig. 4. Structure of the algorithm

Due to the fact that the CNN classification process is similar to the classic steganalysis algorithm approach, CNN model is extensively employed in steganalysis. Figure 4 illustrates the architecture of this method. By preprocessing the picture with a high-pass filter using a conventional approach, the major goal of this algorithm is to improve the noise. For visual feature extraction, the pre-processed picture is sent into the CNN model. A Gaussian function, the activation function only exhibits positive feedback close to 1 when the input is close to zero. The photographs are finally categorised at the completely linked layer, with cover images or stego images serving as differentiating images.

4. Result

We carried out several studies in this part to confirm the viability and efficacy of our schemes. We start by outlining the settings and experimental circumstances. Following that, we present the findings and discussions regarding Invisibility as determined by a few cutting-edge steganalytic tools. Finally, we talk about how complicated our approach is to compute.

Experiment Setup

To show the suggested method's imperceptibility, which is typically measured by the signal-to-noise ratio (PSNR), certain simulations are used. The effectiveness of the suggested strategy will be examined and contrasted with cutting-edge methodologies. Additionally, the simulation results demonstrate the potential of the suggested method for the lossless recovery of partially corrupted data. The well-known picture collection UCID, which comprises 1300 colour images measuring 512 x 384, was used in our research. For data embedding, the well-liked data-hiding techniques HPLP and PROD were used. The other half of the picture characteristics were used for testing, with the other half being used for training. The smallest total error Q_G derived from the testing sets was the criterion used to determine the invisibility of the data concealing, as stated in Equation (8).

$$Q_G = \left(\frac{Q_{HB} + Q_{NO}}{2}\right) \tag{8}$$

where Q_{NO} stands for missed detection rate and Q_{HB} for false alarm rate. Higher Invisibility equals higher Q_G. The average Q_G value across 10 random tests is used to calculate all of the findings. We conducted self-recovery studies on several photographs at tamper rates of 2%, 5%, and 10%, respectively, to guarantee the validity and rigour of the research. As a result of these tests, we now have examples of both tampered and self-healing watermarks, in addition to those that embed themselves. There are three tamper rates (in dB), and their respective PSNR values for the restored images are shown in Table 1 and Figure 5.

Table 1. Values of PSNR for Recovered Images

Tampering rate	3%	6%	9%
Auto-embedded	43.124	44.908	45.542
Corrupted image	19.657	16.102	13.097
Auto Recovered image	39.098	35.031	29.921

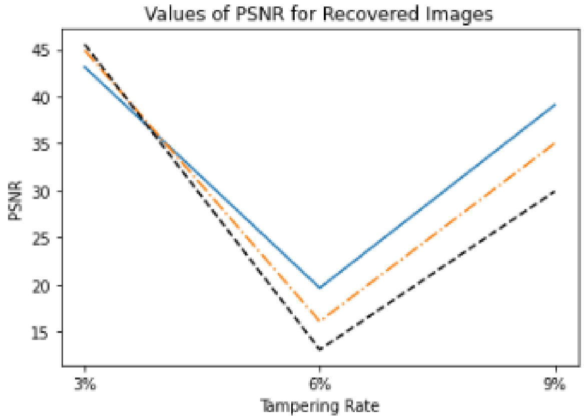
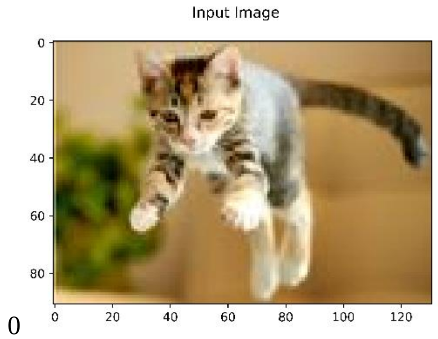


Fig. 5. PSNR recovered image

Because of the disruption caused by the picture on the transmission channel, the sophisticated algorithms that are employed in steganalysis to analyse the abnormality are similarly likely to miss this minor distortion. The embedded new behaviour is maintained in the noise bed by the program's iterative technique. The data is therefore replayed throughout the remaining matrix of pixels if it is finished before all of the image's pixels have been traversed, and a noise bed of a coherent nature is thus created, which won't raise any red flags. This method of selective feeding only modifies one bit per pixel; as a result, the image size is almost unchanged. Peak signal to noise ratio is greater than it is for the general LSB replacement approach, indicating less picture distortion. The status of the stego picture is also confirmed to be more likely undetected by this parameter value, since a greater value predicts smaller distortions that will behave in accordance with the transmission channel's normal disturbances. This would allow the picture to pass without raising any red flags. Metrics such as Mean-Squared Error as well as Peak Signal-to-Noise Ratio, along with to their corresponding histograms, are frequently used to compare stego image against cover outcomes as an indicator of image quality, validating the findings. Maximum Signal-to-Noise Ratio (PSNR) is the ratio of the smallest signal-to-noise value to the largest signal-to-noise value in the image. It is expressed as a number of decibels (dB). PSNR is a valuable measure to use when contrasting different restoration methods on an identical image. In Figure 6 we see a histogram representation of the data. MSE and PSNR values for various models is shown in Table 2.



0

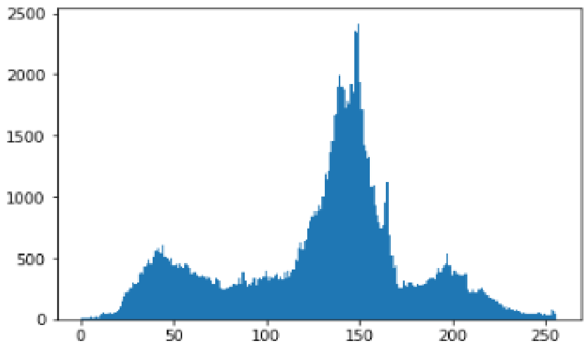


Fig. 6. Histogram of Image

Table 2 MSE and PSNR values for various Models

Input Image	Auto-Regressive Generative Models		Proposed Method	
	PSNR	MSE	PSNR	MSE
Cat	44.236	0.443	72.980	0.643
Balloon	38.983	0.420	66.512	0.521

Invisibility

In Figure 7, we see how the suggested separable multisource information-hiding technique performs in terms of its Invisibility (PE values) for different numbers of senders. The horizontal axis shows the embedding payload (bits per pixel), which is the secret information that has been encrypted utilising the industry-standard embedding technique HPLP. The findings show that PE values with varying sender counts are quite close to one another. The little variation is due to testing's randomization, therefore the performance of Invisibility is unaffected by the quantity of senders. Information concealing will remain invisible even if the amount of senders is increased, as the Invisibility is defined by the embedding technique and payload, which remain constant at L/k bits per pixel regardless of the sender count.

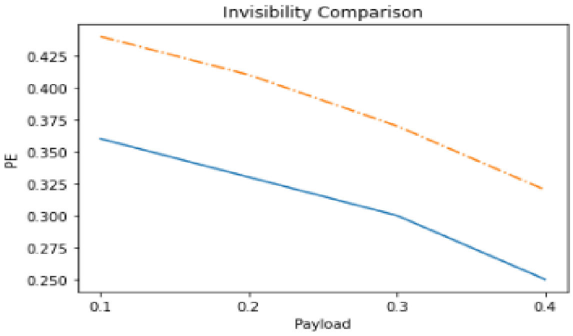


Fig. 7. Invisibility comparison between SRMd and SCRM.

Since the baseline embedding methods form the backbone of our scheme, we need to make sure that it doesn't compromise the Invisibility of existing methods for information concealment. Figures 8 show Invisibility comparison among our scheme and the baseline embedding methods with 5 senders (n = 5), where HPLP and PROD stand in for each instance of our method with hidden information embedded using those corresponding protocols. It is clear that the Invisibility of the current data-concealing techniques has not diminished thanks to our system for multisource data hiding. This makes sense given that the incorporation matrices that are generated with a tried-and-true method for information concealing and kept in our programmes, are what ultimately decide the Invisibility. This illustrates that our technique is successful in multisource information concealment without compromising the invisibility of the information concealing.

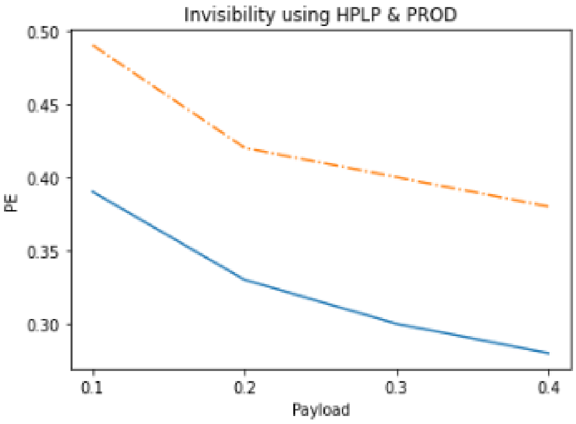


Fig. 8. Comparisons of invisibility between HPLP and PROD.

Computational Complexity

Computational complexity is a significant indicator of data concealment. Additionally, we ran tests to assess how computationally complex our plan was in comparison to the standard embedding algorithms. The average embedding time (s) for each of the 1300 photos is displayed and after all 1300 images were used for data embedding. Similar to this, "HPLP-Separable" and "PROD-Separable" refer to the situations of our technique with hidden information incorporated via HPLP and PROD, correspondingly.

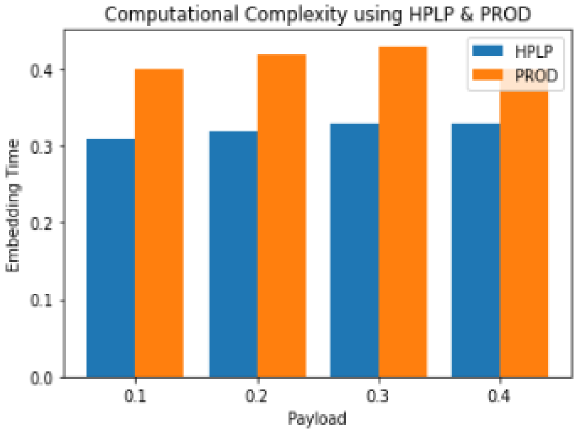


Fig. 9 Computational Complexity using HPLP & PROD

Figure 9 demonstrates that compared to the established embedding methods, our approach has a similar or lower computational cost. This shows that our approach satisfies the multisource criterion of the modern information-hiding architecture without adding raising computational complexity. Additionally, it should be noted that a larger payload does not result in a longer embedding time. This is due to the distortion function being the primary determinant of the computing cost of a contemporary data-hiding scheme. Secret data may be implanted fast using the almost ideal steganographic coding with the determined embedding costs. When using the same steganalysis method, the comparisons are expressed as the CNN training time consumption and the detection accuracy of Machine Learning models. Evidently, CNN's lower rate makes it more effective at avoiding detector detection. The CNN-based techniques, however, show promise for growth in terms of feature learning benefits. Accuracy Comparison between GAN and CNN Model is shown in Table 3 and Figure 10.

Table 3. Accuracy Comparison between GAN and CNN Model

Models	Group	Execution cost (s)	Precision
CNN	Source Images	32.19	0.93
	Generated Images		0.91
GAN	Source Images	30.45	0.88
	Generated Images		0.78

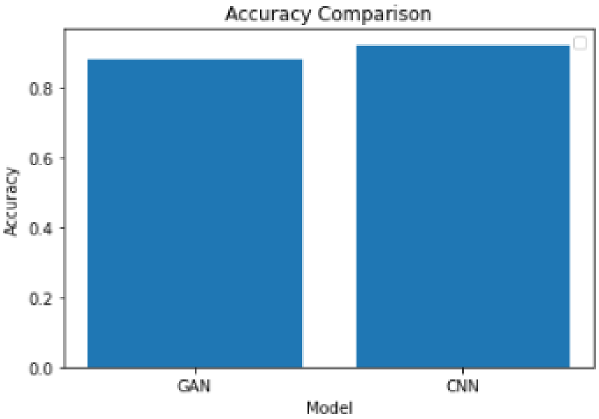


Fig. 10. Accuracy Comparison between GAN and CNN Model

5. Conclusion

Information concealing technology, a hotspot for study in the field of information security, delivers hidden information through a carrier. The conventional information-hiding algorithm gets its dense picture via modification and depends on the precise design of humans. As deep learning has matured and found its way into other fields, multiple data concealing methods have evolved on its back. Image concealment is one among them, and because of its substantial steganographic capability, it has become a study hotspot. The multisource data-hiding system (MDHS) that we suggest extracts all secret data from the receiver's side as well as the content that was collected by the receiver via the same cover picture, many senders can each deliver a distinct hidden piece of information to a recipient via multisource data concealing. Instead than obtaining the specifics of the hidden information, the receiver seeks to derive a co-determined conclusion from the secret data sent by all senders.

References

[1] A. G. Devi, A. Thota, G. Nithya, S. Majji, A. Gopatoti and L. Dhavamani, "Advancement of Digital Image Steganography using Deep Convolutional Neural Networks," 2022 International Interdisciplinary Humanitarian Conference for Sustainability (IIHC), Bengaluru, India, 2022, pp. 250-254, doi: 10.1109/IIHC55949.2022.10060230.

[2] A. Kotkar, S. Khadapkar, A. Gupta and S. Jangale, "Multiple layered Security using combination of Cryptography with Rotational, Flipping Steganography and Message Authentication," 2022 IEEE International Conference on Data Science and Information System (ICDSIS), Hassan, India, 2022, pp. 1-5, doi: 10.1109/ICDSIS55133.2022.9915922.

[3] J. Singh and M. Singla, "A Novel Method of high-Capacity Steganography Technique in Double

Precision Images," 2021 International Conference on Computational Performance Evaluation (ComPE), Shillong, India, 2021, pp. 780-784, doi: 10.1109/ComPE53109.2021.9751905.

[4] L. Lyubchyk, G. Grinberg, O. Dunaievska and M. Lubchick, "Recurrent Estimation of Hidden Markov Model Transition Probabilities from Aggregate Data," 2019 9th International Conference on Advanced Computer Information Technologies (ACIT), Ceske Budejovice, Czech Republic, 2019, pp. 64-67, doi: 10.1109/ACITT.2019.8779890.

[5] S. Ali and N. Bouguila, "Maximum A Posteriori Approximation of Dirichlet and Beta-Liouville Hidden Markov Models for Proportional Sequential Data Modeling," 2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Toronto, ON, Canada, 2020, pp. 4081-4087, doi: 10.1109/SMC42975.2020.9283011.

[6] T. Chadza, K. G. Kyriakopoulos and S. Lambotharan, "Contemporary Sequential Network Attacks Prediction using Hidden Markov Model," 2019 17th International Conference on Privacy, Security and Trust (PST), Fredericton, NB, Canada, 2019, pp. 1-3, doi: 10.1109/PST47121.2019.8949035.

[7] E. H. Rachmawanto, D. R. I. M. Setiadi, C. A. Sari, P. N. Andono, O. Farooq and N. Pradita, "Spread Embedding Technique in LSB Image Steganography based on Chaos Theory," 2019 International Seminar on Application for Technology of Information and Communication (iSemantic), Semarang, Indonesia, 2019, pp. 1-6, doi: 10.1109/ISEMANTIC.2019.8884266.

[8] J. Deng, M. Tang, Y. Wang and Z. Wang, "LSB Color Image Embedding Steganography Based on Cyclic Chaos," 2019 IEEE 5th International Conference on Computer and Communications (ICCC), Chengdu, China, 2019, pp. 1798-1802, doi: 10.1109/ICCC47050.2019.9064335.

[9] H. Arora, G. K. Soni, R. K. Kushwaha and P. Prasoon, "Digital Image Security Based on the Hybrid Model of Image Hiding and Encryption," 2021 6th International Conference on Communication and Electronics Systems (ICCES), Coimbatre, India, 2021, pp. 1153-1157, doi: 10.1109/ICCES51350.2021.9488973.

[10] M. Ueda and S. Imaizumi, "A Reversible Data Hiding Scheme for Printing with Special Color Inks Using Digital Halftoning," 2019 IEEE 8th Global Conference on Consumer Electronics (GCCE), Osaka, Japan, 2019, pp. 1135-1138, doi: 10.1109/GCCE46687.2019.9015581.

[11] H. Arora, P. Kumar Sharma, K. Mitanshi and A. Choursia, "Enhanced Security of Digital Picture and Text Information with Hybride Model of Hiding and Encryption Techniques," 2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), Erode, India, 2022, pp. 1238-1241, doi: 10.1109/ICSCDS53736.2022.9760822.

[12] N. J. de La Croix, C. C. Islamy and T. Ahmad, "Reversible Data Hiding using Pixel-Value-Ordering and Difference Expansion in Digital Images," 2022 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT), Solo, Indonesia, 2022, pp. 33-38, doi: 10.1109/COMNETSAT56033.2022.9994516.

[13] S. Kukreja and G. Kasana, "A Secure Reversible Data Hiding Scheme for Digital Images using Random Grid Visual Secret Sharing," 2019 Amity International Conference on Artificial Intelligence (AICAI), Dubai, United Arab Emirates, 2019, pp. 864-869, doi: 10.1109/AICAI.2019.8701360.

[14] K. Luo, W. Gao and R. Yuan, "A Study of Reversible Data Hiding Technology with an Authentication Function," 2022 4th International Conference on Artificial Intelligence and Advanced Manufacturing (AIAM), Hamburg, Germany, 2022, pp. 52-57, doi: 10.1109/AIAM57466.2022.00018.

[15] V. M. Manikandan and P. Renjith, "An Efficient Overflow Handling Technique for Histogram Shifting based Reversible Data Hiding," 2020 International Conference on Innovative Trends in Information Technology (ICITIIT), Kottayam, India, 2020, pp. 1-6, doi: 10.1109/ICITIIT49094.2020.9071553.