IRJEAS
NURTURING RESEARCH

INTERNATIONAL RESEARCH JOURNAL
OF
ENGINEERING & APPLIED SCIENCES

ISSN: 2322-0821(O)
ISSN: 2394-9910(P)

VOLUME 11 ISSUE 1
Jan 2023 - Mar 2023

www.irjeas.org

Original Article

Optimized Data Hiding Method based on Meerkat Clan Algorithm for Image Steganography

*Navrinder Kaur[1], Sarabjeet Kaur[2]

[1]*Department of Computer Science Engineering, Adesh Institute of Engineering & Technology, Faridkot, Punjab, India.*
navrinderkaur337@gmail.com
[2]*Assistant Professor, Department of Computer Science Engineering, Adesh Institute of Engineering & Technology, Faridkot, Punjab, India.*
sarb7316@gmail.com

*Corresponding Author - *navrinderkaur337@gmail.com*

DOI – https://doi.org/10.55083/irjeas.2022.v11i01002

Received: 11 November 2022; Received in revised form: 23 January 2023; Accepted: 19 February 2023

Abstract: To fulfill the security criterion of imperceptibility, the secret info is hidden in the cover image using image steganography. To do this, a hidden data bit swaps out the least important part of the cover image. The replacement process produces variability, which has an effect on the imperceptibility parameter. To address this restriction, this research proposes a unique optimal data concealing approach based on the meerkat clan optimization algorithm. This method seeks the best secret data to conceal in the cover image to be able to improve the imperceptibility parameter. The secret data is also divided into 2:4 ratios. The cover image is then divided into smooth and edge regions. A 2-bit LSB technique is utilized to hide data in the smooth area, whereas data hiding in the edge region is accomplished with a 4-bit LSB approach. The simulation is evaluated using multiple performance measures to compare its performance to existing approaches. The suggested technique outperforms the previous method in terms of imperceptibility.

Keywords: Canny Edge Detection, Chaotic Logistic Map, Data Hiding, Image Steganography, Meerkat clan optimization, Security.

1. INTRODUCTION

Digital communication through the Internet's popularity has risen as a means of exchanging information. Although digital media such as text, video, audio, and images may be used to communicate messages/contents, there are security concerns when using digital media [1]. Steganography and cryptography techniques are used in order to address such security concerns. This approach guarantees secrecy, availability of information, and integrity. Cryptography is achieved by scrambling the secret data with the private key which gives encrypted data in the output [2]. The structure of encrypted communications, however, makes them noticeable and attracts hackers to try to decode the message. The art of encoding secret communications in media with the help of images, texts, videos, audio, and protocols, is characterized as Steganography. The media is used for hiding propose known as cover media and media generated after data hiding process is known as stego media. In steganography, 3 key characteristics are appropriate for hiding information, explained below [2-5]:

1. Payload Capacity: A cover image's data is defined by the number of hidden bits that are encoded in per pixel in the image. More data may be included in a cover image by means of a higher number.

2. Imperceptibility: It calculates the maximum signal-to-noise ratio to assess the overall the stego's quality image (PSNR). A low number implies poor image quality, whereas a large number suggests good image quality.

3. Robustness: Because of this, it is difficult for confidential data to be stolen or altered.

Further, steganography can be categorized into two domains named spatial and transform domain [3]. The image's pixels are directly modified for data concealing in the spatial domain. As a result, it has a high embedding capacity. On the other hand, the image pixels are transformed into the frequency domain in the transform domain, and its coefficient is employed for data concealing. In order to enhance the visual quality, we focused on the spatial domain and its feature imperceptibility in this article.

Increasing the imperceptibility parameter for image steganography is the key contribution of this study. The meerkat clan optimization method is used to find the best arrangement for secret data in order to accomplish this aim. In addition, the cover image is pre-processed. Using clever edge detection, the cover image is separated into an edge and non-edge zone. Following the selection of the best secret data order, to hide 4-bits per pixel in the edge region with 2-bits per pixel in the non-edge region, the least significant bit approach is utilized. Researchers in the literature utilize the dataset for the simulation evaluation. According to the peak signal-to-noise ratio, the outcomes demonstrate that the suggested strategy outperforms the already used techniques.

Five sections make up the remaining portion of the document. Section 2 displays the linked work. In Section 3, the MCO algorithm is described. Section 4 describes the recommended strategy. Section 5 displays the simulation findings. Section 6 concludes with a conclusion and future scope of usage.

2. RELATED WORK

We investigated and analyzed the current approaches in this part.

Kalaichelvi et al. [6], In order to protect the data, steganography and cryptography are coupled in this study. To turn a message into a secret message, it must first be encrypted using the updated RSA algorithm. Secondly, employing the Canny edge detection method, the cover image is divided into edge and non-edge pixels. The N1 (two) and N2 (four) bits of the coded communications are then buried in the edge and non-edge pixel areas using the LSB approach. The final four pixels of the cover image are implanted with the length values, N1, N2, and other crucial characteristics to create the stego-image. The concealed data are recovered after eliminating the N1, N2, and length information from the stego-image at the receiver side. Then, using the updated RSA technique, the secret data that was extracted is decrypted. Using two sets of keys increases security using the modified RSA method. Finally, measurements are made of the major performance metrics parameters, including Peak signal to noise ratio, histogram, MSE, and entropy. It has been noted that the suggested method achieves better effectiveness, security, and information-hiding features that are imperceptible to users.

Rajankumar S. Bichkar and Pratik D. Shah [7], This study describes a genetic algorithm-based approach for high-capacity image steganography that is based on secret data alteration (GA). The hidden data is embedded using this novel technology, which replaces the least significant bit (LSB) with steganography. However, before being inserted into the LSBs of the cover image, the hidden data is reorganized and altered. GA controls the settings that are used to organise and change the secret data. Flexible chromosome, a novel idea, is presented, allowing GA to comprehend the chromosomal value in several ways. GA seeks to identify the optimal parameter value that produces stego images with great visual quality.The recommended technique produces stego images with average PSNR values of 40.83 dB and 46.41 dB for data hiding capacities of 2 and 3 bit per pixel (bpp), respectively.

Rajankumar S. Bichkar and Pratik D. Shah [8], This study provides a spatial domain image steganography technique that is both safe and lossless. Finding appropriate places to conceal 2 bits of hidden information for each pixel, which results in coefficients that correspond to the position of the match, allows for the concealment of a stream of secret data in a fourth of the image. By utilizing LSB replacement steganography, these coefficients are hidden in the remainder of the image. Because the ideal spot to conceal these coefficients in the image is found using a genetic algorithm, the proposed solution is extremely secure and difficult to hack. The suggested method's results are contrasted with those of LSB replacement steganography, which also embeds a similar quantity of hidden data. It is noted that the suggested method is significantly better than LSB steganography. The MSE and PSNR values are improved, and the histogram deterioration is reduced to a minimum, eliminating histogram attack. In comparison to 52.21 achieved using the LSB approach, the average PSNR value of the stego-image acquired using the suggested technique is 53.11 dB at a data embedding rate of two bits per pixel.

Hamidreza Rashidy, Kanan and Bahram Nazeri [9], In this research, a brand-new evolutionary algorithm-based technique to high-quality, Image steganography in the spatial domain with no data loss is put forward. Steganography is treated as a search issue in the outlined algorithm. By using a genetic algorithm, we can locate the ideal location in the host image for embedding changed secret data without having to engage in time-consuming searches. Thus, the suggested approach may both increase the quality of the stego image and achieve high embedding power (i.e. the PSNR value). The two basic processes of embedding are to first edit the secret bits and then to incorporate modified hidden info in the host image. From the perspectives of secret concealment efficacy and stego-image quality, the algorithm has been assessed and contrasted with other previously well-liked current techniques. The fact that the suggested technique continuously outperforms the benchmark approaches that were evaluated is highly encouraging. Additionally, experimental results have shown that the stego image is visually identical to the matching host image regardless of the capacity of the embedded hidden image is doubled. We draw the conclusion that the high quality stego image produced by our suggested method satisfies the consumers' favorable need for the embedding capability. Our plan is straightforward and practical for adaptable steganographic uses.

2.1 Motivation

In the existing papers, authors hide the secret data using LSB method which generates variability. To overcome this limitation, authors used the optimization algorithm to determine the optimal secret data form and cover image scanning order. In the literature, genetic algorithm is deployed for it. It faces numerous challenges. Therefore, we have explored other optimization algorithm and chosen the most optimal optimization algorithm for the proposed method.

3. MEERKAT CLAN ALGORITHM

There are a total of 37 species of meerkats, spread across 18genera and 2 sub-families. These small (<1Kg) carnivores are members of the mongoose family. As cooperative breeders, meerkats happily coexist in colonies of up to fifty. The meerkat is a very gregarious member of the mongoose family; other sociable members of the genus include the banded mongoose and the dwarf mongoose. Because of their desert-adapted anatomy, meerkats can only be found in the drier parts of south-western Africa (consisting Namibia, Botswana, southern Angola, and South Africa) [10].

3.1 MEERKAT BEHAVIOUR

Meerkats are seeking creatures that inhabit large, open networks with several entrances and only depart during the day. They are regarded as sociable, and colonies of up to forty can exist. Animals from the same species routinely groom each other to strengthen social ties. The group's alpha pair frequently trace scratches to demonstrate their dominance, and subordinates will frequently lick and groom the alphas to keep note of such behaviors. When the group comes back together after a brief break, these behaviors are typically practiced. The majority of meerkats in a given group are the alpha pair's offspring and siblings.

3.1.1 Sentry Behavior

Within their colonies, meerkats develop benevolent behavior; while the others hunt or play, one or more will stand sentry (lookout) to alert them if something potentially harmful occurs. The meerkat serves as a sentry and barks if a hunter is discovered, while the others run and hide in one of the many holes in the ground. They should be able to move freely around their territory. The sentry meerkat emerges from the burrow first, searching for hunters while continuing to bark to draw the others in. Meerkat sentry will cease barking and the others will be safe to go once the threat has passed. Meerkats will also keep an eye on any juvenile members of the pack. While the dominant female is missing and the others are still in the group, non-breeding females frequently tend to the young of the alpha couple. They will also defend the youngsters from harm, often at the expense of their own lives. If there is a threat, the babysitter will take the children to a secure subterranean spot and be ready to aid them, or she will collect the children and lie on top of them.

3.1.2 Foraging Behavior

Animals extend out and feed individually while maintaining visual and verbal contact; this is typical for sociable mongooses. A pack normally waits at least a week between trips in order to give a region time to replenish its food supply while systematically foraging inside its home territory. Small and forefeet are used to dig out hidden prey. Food is frequently shared by adults with the pack's young members.

3.1.3. Behavior of the Babysitter

Meerkats participate in a variety of helpful activities. Baby-watching, when helps stay in the a den with pups 25 while the rest of the group is out for pup feeding and foraging, where helpers give the pups some of their food while foraging, are the two main contributions to supportive maintenance. Both babysitting and puppy-feeding come at a major energy cost to the helper: babysitters skip meals 24 hours maximum, which results in little weight loss, while puppy-feeders quit their own foraging supplies in favor of bringing them to the puppies.

3.2 ALGORITHM USING MEERKAT CLAN

We can learn how living things arrange their natural activity into algorithmic routines by carefully studying how they behave. The novel meta-heuristics under discussion in this paper are hence nature-inspired algorithms. These innovative techniques, which are optimization algorithm meta-heuristics, are mostly obtained by picking the ideal and a randomization structure. The former directs the algorithm toward optimality (utilization), while the far-off avoids both the program's loss of variation and its bordering in local optima (examination). Achieving global optimality may be facilitated by a strong stability between inquiry and use.

Meerkats are social animals that live in colonies of 5–30 individuals. They share parenting and bathroom duties since they are sociable creatures. Every mob is ruled by a dominating alpha male and a dominant alpha female. Every mob has its own region, yet they migrate there when food is scarce or when a more powerful crowd calls for it. In the event of the latter, the weaker group will attempt to expand in another way or remain before they become more hardy and locate their vanished burrow.

Every mob also includes a member known as a "sentry," who keeps watch over the group, recognises danger, and alerts the other mob members. The sentry either stands on the ground, climbs a tree, or hides in the bushes to keep watch. The sentry keeps an eye on the mob's foraging activities as well as the burrowing plan. When a threat is detected, the sentry barks loudly, and the crowd flees for safety.

According to the earlier discussion of MCA that was inspired by Meerkat animals, the general processes for MCA are listed below. These steps can vary depending on the problem being solved.

1. Initialization step, create a clan of persons chosen by chance, then discover the worst foraging and care rate, the size of the clan for foraging.
2. Determine the clan's health
3. Selected the strongest as the "sentry"
4. Divide the clan into two factions (foraging & care)
5. For the foraging group, make buddies.
6. Select the foraging group's most underprivileged members, then swap them for the best members of the caring group.
7. Take out the worst people from the care group, then pick someone else at random.
8. If sentry is a better option, replace the top forager with sentry.

4. METHOD PROPOSED

The primary goal of this study is to minimize variability in image steganography in order to improve imperceptibility. Initially, secret data is read and optimal form of secret data is determined using meerkat clan optimization algorithm based on the objective function. We have taken MSE as an objective function. Next, the cover image has been read and split into the edge and non-edge (smooth) utilizing the clever edge detection method. In the edge region, 4-bit LSB-based data hiding is done, whereas, in the non-edge region, 2-bit based data hiding. Next, the edge and non-edge regions are concatenated to generate the image of stego in the output. Finally, the performance of the suggested technique numerous measures was used to assess such as mean square error (MSE), peak signal to noise ratio (PSNR), and entropy. Next, MCO algorithm how determine the optimal form of secret data is given below.

1. Initialize the MCO algorithm parameters and objective function.
2. Randomly create clans of population in the lower and upper limit.
3. Compute the fitness based on the objective function and determine the greatest option for a sentry.
4. Split the clan population into two categories: foraging and caring.
5. Generates neighbors for the foraging unit at random.
6. Next, choose the worst population in the foraging group and exchange they possess the best people in the intervention group.
7. After that, eliminate the worst population from the caring group and produce a new individual by chance.
8. If necessary, the greatest forager with sentry, which is recognized as the best solution.

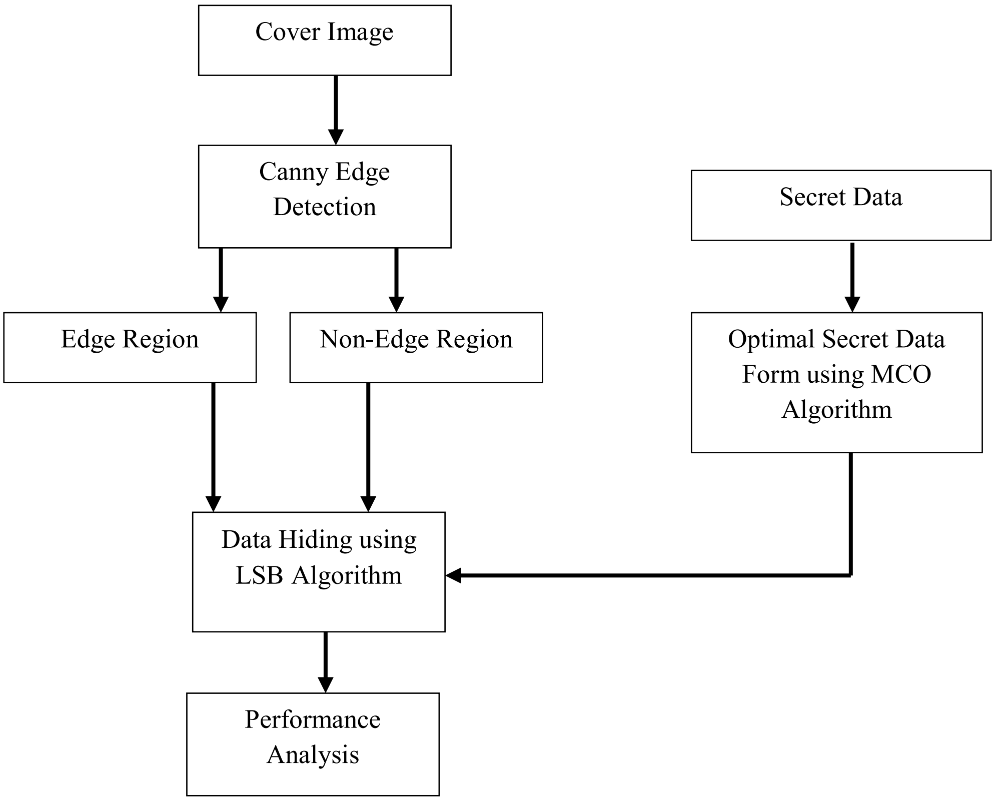

Figure 1: Block Diagram of the Method Proposed

5. SIMULATION EVALUATION

In this part, the suggested approach is simulated using standard dataset cover images to assess its performance over current methods. MATLAB is used to run the simulation.

5.1 Simulation Setup

The simulation setup used to test the suggested technique is described in this section. The USC-SIPI Image Database is used to download the images for the common dataset. There are several photographs in both colour and grayscale in the database. In our work, grayscale photographs have been taken into consideration, and their 256x256 resolution has been taken into account. In MATLAB, the secret data is produced at random. Also used to increase imperceptibility is the meerkat clan optimization (MCO) method. In Table 1, the MCO parameters are displayed.

Table:1 MCO Parameters

Variables	Value
Population Size	50
Number of Iterations	100
Clan Size	21
Care Size	10
ForagingSize	10
Foraging Rate	0.1

5.2 Performance Indicators

Table 2: shows performance indicators are calculated for the method proposed [11-13].

Table 2: Performance Metrics

Parameters	Equation
Mean Square Error	$MSE = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(A_{ij} - B_{ij})^2}{MN}$ (1)
Peak Signal to Noise Ratio	$PSNR = 10\log_{10}\frac{I^2}{MSE}$ (2)
Entropy	$E = \sum_{i=o}^{2^{M-1}} p(m_i) \times \log_2\left(\frac{1}{p(m_i)}\right)$ (3)

In Eq. (1), AB denotes the stego and cover image. In Eq. (2), I denote the greatest intensity we can represent in the cover image. In Eq. (3), $p(m_i)$ denotes the probability of the pixel.In the steganography, high significance of PSNR required whereas similar entropy in the cover and stego image.

5.3 Simulation Results

Table 3 demonstrates the simulation results of the method proposed. The results demonstrate that the method proposed achieves high PSNR due to low value of MSE. On the other hand, similar entropy of cover and stego image.

Table 3: Simulation Results for the Method Proposed

Images	MSE	PSNR (in dB)	Entropy	
			C	S
Lena	0.05	43.01	7.70	7.78
Baboon	0.05	43.92	7.22	7.29
Barbara	0.1	44.90	7.30	7.33
Peppers	0.99	45.01	7.65	7.74
Airplane	0.1	44.02	7.82	7.90

The previous approach suggested by Kalaichelvi et al. [6] based on the PSNR parameter is then in comparison to the new method being utilized in the analysis. The PSNR values for the proposed and suggested method are displayed in Table 4. The outcome demonstrates that the proposed technique outperforms the suggested method by existing author in terms of PSNR.

Table 4: Comparative Analysis with the Existing Methods

Images	Kalaichelvi et al. [6]	Proposed Method
Lena	42.88	43.01
Airplane	43.17	43.92
Peppers	44.44	44.90
Lion	44.65	45.01
Cat	43.32	44.02

6. CONCLUSION

In this research, we developed an improved data-hiding technique on the basis of the Meerkat optimization algorithm. This algorithm looks for the best secret data form to hide data. Additionally, the cover image and data in 2:4 ratios are divided into two sections known as the smooth and edge area. In the smooth region, 2-bit LSB data concealing is accomplished, whereas 4-bit LSB is done in the edge region. The photographs from the common dataset are used to evaluate the simulation. The outcomes demonstrate that the suggested approach produces strong PSNR and comparable entropy between the cover and stego image. Finally, comparison study demonstrates that the suggested technique outperforms the current method in terms of PSNR.

REFERENCES

[1] Zhang, C., Lin, C., Benz, P., Chen, K., Zhang, W. and Kweon, I.S., 2021. A brief survey on deep learning based data hiding, steganography and watermarking. *arXiv preprint arXiv:2103.01607*.

[2] Cheddad, A., Condell, J., Curran, K. and Mc Kevitt, P., 2010. Digital image steganography: Survey and analysis of current methods. *Signal processing*, *90*(3), pp.727-752.

[3] Hamid, N., Yahya, A., Ahmad, R.B. and Al-Qershi, O.M., 2012. Image steganography techniques: an overview. *International Journal of Computer Science and Security (IJCSS)*, *6*(3), pp.168-187.

[4] Kumar, A., Karmakar, A. and Agarwal, A., 2021. Optimized Data Hiding Technique Using Egyptian Vulture Optimization Algorithm For Image Steganography. *Design Engineering*, pp.12525-12541.

[5] Subhedar, M.S. and Mankar, V.H., 2014. Current status and key issues in image steganography: A survey. *Computer science review*, *13*, pp.95-113.

[6] Kalaichelvi, V., Meenakshi, P., Vimala Devi, P., Manikandan, H., Venkateswari, P. and Swaminathan, S., 2021. A stable image steganography: a novel approach based on modified RSA algorithm and 2–4 least significant bit (LSB) technique. *Journal of Ambient Intelligence and Humanized Computing*, *12*(7), pp.7235-7243.

[7] Shah, P.D. and Bichkar, R.S., 2021. Secret data modification based image steganography technique using genetic algorithm having a flexible chromosome structure. *Engineering Science and Technology, an International Journal*, *24*(3), pp.782-794.

[8] Shah, P.D. and Bichkar, R.S., 2018. A secure spatial domain image steganography using genetic algorithm and linear congruential generator. In *International conference on intelligent computing and applications* (pp. 119-129). Springer, Singapore.

[9] Kanan, H.R. and Nazeri, B., 2014. A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm. *Expert systems with applications*, *41*(14), pp.6123-6130.

[10] Al-Obaidi, A.T.S., Abdullah, H.S. and Ahmed, Z.O., 2018. Meerkat clan algorithm: A new swarm intelligence algorithm. *Indonesian Journal of Electrical Engineering and Computer Science*, *10*(1), pp.354-360.

[11] Ardiansyah, G., Sari, C.A. and Rachmawanto, E.H., 2017, November. Hybrid method using 3-DES, DWT and LSB for secure image steganography algorithm. In *2017 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE)* (pp. 249-254). IEEE.

[12] Kumar, A., Karmakar, A. and Agarwal, A., 2021. Privacy-Preserving Method for Public Health Surveillance Data using Image Steganography. *Tobacco Regulatory Science*, *7*(6), pp.6814-6830.

[13] Hussain, M., Wahab, A.W.A., Idris, Y.I.B., Ho, A.T. and Jung, K.H., 2018. Image steganography in spatial domain: A survey. *Signal Processing: Image Communication*, *65*, pp.46-66.

Conflict of Interest Statement: *The authors declare that there is no conflict of interest regarding the publication of this paper.*