Vol. 5 Issue No. 4, October-December 2023 e-ISSN 2456-7701

Journal of Science and Technological Researches

A Peer Reviewed Journal

Origin of Innovation

Domain: www.jstr.org.in, Email: editor@jstr.org.in

IMAGE STEGANALYSIS USING LEAST SIGNIFICANT BIT (LSB) AND CUCKOO SEARCH OPTIMISATION

BT Ramaiah[1]*, Rajeev Kumar[2], and Reeta Bharadwaj[3]

[1]PG Scholar, Department of IT, DAV Institute of Engineering and Technology, Jalandhar, Punjab, India

[2,3]Assistant Professor, Dept of IT, DAV Institute of Engineering and Technology, Jalandhar, Punjab, India

Email: bridgehead17@gmail.com

Date of Received	**24 October, 2023**
Date of Revised	**27 December 2023**
Date of Acceptance	**16 December, 2023**
Date of Publication	**31 December, 2023**

DOI Link : https://doi.org/10.51514/JSTR.5.4.2023.17-25

IMAGE STEGANALYSIS USING LEAST SIGNIFICANT BIT (LSB) AND CUCKOO SEARCH OPTIMISATION

BT Ramaiah[1]*, Rajeev Kumar[2], and Reeta Bharadwaj[3]

[1]PG Scholar, Department of IT, DAV Institute of Engineering and Technology, Jalandhar, Punjab, India

[2,3]Assistant Professor, Dept of IT, DAV Institute of Engineering and Technology, Jalandhar, Punjab, India

Email: bridgehead17@gmail.com

ABSTRACT

Information system security is a field that safeguards the availability, confidentiality, and integrity of data and information services through the use of steganography, watermarking, and cryptography. One kind of attack that consistently seeks to breach security is steganalysis. Steganography differs from comparable techniques like cryptography and watermarking mostly due to its final goals. Because steganography attempts to conceal the message's presence, it might be challenging for an observer to locate the message. This work suggests a novel feature-based steganalysis that makes use of Cuckoo Search optimization and LBP feature extraction. By utilizing Lease Significant Bit (LSB) insertion, an image dataset is produced. On the basis of accuracy, PSNR, MSE, and calculation time, the experimental results of the suggested approach are compared with the current DCT feature extraction and ABC optimization technique. The suggested approach works better than the current procedures, according to the results.

Keywords: *Information security, Steganography, Confidentiality, Integrity, Availability, Steganalysis, LB P feature extraction, Cuckoo search, LSB*

INTRODUCTION

Steganography is the process of hiding communication in such a way that its existence is undetected, whereas steganalysis is the discovery of concealed communication. Handling big volumes of data often necessitates substantial execution time and computer resources. Consequently, pre-processing must be used, since this may control the execution duration and computing resources. In this work, we provide a novel feature-based blind steganalysis technique for separating stego pictures from JPEG-formatted cover (clean) images. To this end, we introduce an enhanced Artificial Bee Colony (ABC) as the basis for our feature selection method. The social behavior of honeybees in their quest for the ideal food source served as an inspiration for the ABC algorithm. The performance of the classifier and the chosen feature vector's dimension are dependent on the use of wrapper-based techniques in the suggested approach. Two JPEG photos are used for the tests. Comparing the suggested steganalysis procedure to other methods now in use, experimental findings show that it is successful.

A new steganographic application was being developed for each old message concealment technology that was discovered. Traditional techniques are reimagined. In the world of steganography, computer technology has brought about a revolution. With the introduction of personal computers to solve traditional steganographic difficulties in 1985, modern steganography was born. The pace of development was modest at the time, but it has subsequently picked up speed. Nowadays, most steganographic systems employ multimedia content as cover media as people often send digital photos via email and other online communications. In contemporary methodology, the following categories of multimedia steganography may be distinguished based on the nature of the cover object:

- Text Steganography
- Image Steganography
- Audio Steganography
- Video Steganography
- Protocol Steganography

1.1 Steganography Techniques

Digital watermarks are a common way for steganography and watermarking techniques to protect intellectual property and sensitive information from illegal use and access in digital assets including software, movies, books, and music. Digital photos may be altered in a variety of ways to conceal content. Of these, the majority are as follows:

*Author for correspondence

- Least significant bit insertion
- Masking and filtering
- Algorithms and transformations

2. Related work

Many investigations and studies pertaining to sentiment analysis have been conducted in the past few years. Using lexical, hybrid, and machine learning approaches, sentiment analysis has been the subject of several published scientific studies. Here is a quick overview of the several works that have been cited:

Goel et al. [1], The assault on data concealing problem is presented in the study. Targeted Steganalytic Attacks are the goal of the first strategy. The primary focus of the study is on targeted attacks based on first order data. Two techniques that can maintain an image's first-order statistics after embedding have been introduced. The suggested technique increases the security of the algorithms against targeted assaults by retaining the picture statistics, as demonstrated by the experimental results. The second strategy seeks to thwart blind steganalytic attacks, particularly those that use calibration to attempt to infer a cover picture model from the stego image.

Chen et al. [2], The study presents a new and very fast JPEG steganalysis technique that makes use of the JPEG coefficients' intrablock and interblock correlations. Steganalysis of JPEG images has gained more and more interest lately. Each difference JPEG 2-D array's transition probability matrix is computed to take use of the intrablock correlation; similarly, the "averaged" transition probability matrices for those difference mode 2-D arrays are computed to take advantage of the interblock correlation. These matrices' constituents are all utilized as steganalysis characteristics.

Meenpaa et al. [3], The local binary pattern operator, which converts an image into an array or picture of integer labels characterizing the image's small-scale look, is introduced in this chapter as an image operator. Subsequent picture analysis uses these labels or their statistics, most often the histogram. The operator was initially intended for monochrome still photos, but it has since been expanded to include color (multi-channel) images, movies, and volumetric data as well. The several iterations of the real LBP operator in the spatial domain are covered in this chapter. The 3 × 3-pixel block of a picture is where the original version of the local binary pattern operator operates. To determine a label for the center pixel, the pixels in this block are thresholded by the value of the center pixel, multiplied by powers of two, and then added together. Given that the neighborhood has eight pixels, a total of 28 = 256 distinct labels may be produced based on how the center and the neighborhood's pixels compare in terms of grey values.

Ladha et al. [4], In data mining, feature selection is crucial, particularly for large dimensional datasets. A popular procedure in machine learning is feature selection, often called subset selection, in which portions of the characteristics included in the data are chosen so that a learning algorithm may be applied to them. The subset with the fewest dimensions that nonetheless significantly improves accuracy is the best one. We eliminate the last, irrelevant dimensions. One of the two methods (the other being feature extraction) to escape the curse of dimensionality is to do this crucial pre-processing step. In feature selection, there are two methods: forward selection and backward selection. The communities of pattern recognition, statistics, and data mining have been actively researching feature selection.

Kodovsky et al. [5], The notion of the framework, an ensemble classifier that offers scalable machine learning as an alternative to sophisticated Support Vector Machines (SVMs), is further developed in this research. We may take a methodical and tidy approach to feature-space development by substituting ensemble classifiers for support vector machines (SVMs). Rich models were created for the two most popular picture formats, JPEG and raster, to show off the capabilities of the suggested technique. The spatial domain Rich Model (SRM) is a feature space of 34,671 dimensions that is made up of neighboring sample co-occurrences of noise residuals that were produced using various linear and non-linear filters. The 22,510-dimensional Cartesian-calibrated JPEG domain Rich Model (CC-JRM) is made up of submodels that represent various kinds of spatial and frequency relationships between the DCT coefficients of JPEG pictures.

Sagayam et al. [6], The focus of the research is on how search engine indexes are purposefully manipulated through the use of ABC in Web spam. Web spam is the use of various techniques, including repetitive phrases, to influence the prominence or relevance of resources indexed in a way that isn't compatible with the indexing system's intended purpose. Finding out if a search word occurs in a webpage's content or URL is one aspect of using a search engine. In order to build a learning model based on the ant colony optimization (ACO) and bee colony optimization (BCO) algorithms, the content and link characteristics are retrieved from hosts. The best option is contrasted with the optimization of ant and bee colonies. Lastly, it indicates which optimization approach is more effective in identifying spam. In order to create a set of classification rules and comparisons for spam host identification, the author of this research used an algorithm based on ant and bee colony optimization.

Muhammadi et al. [7], The study provides a clear, comprehensive picture of the value of combining different data mining approaches. Through the use of data mining techniques, we are able to use steganalysis to find hidden and secret messages. A variety of data types, including Image, Audio, Text, Video, and Protocol, are given as Domains. This categorization is based on data mining techniques that are steganography-extended steganalysis methods used in this domain to identify embedded messages in stego pictures.

Kodovsky et al. [8], This work suggests ensemble classifiers, a popular alternative to random forests in machine learning, and makes the case that steganalysis is a perfect fit for them. The best steganalysis techniques for digital media are developed as supervised classifiers using feature vectors that have been taken from the source material. Support vector machines (SVMs) appear to be the preferred tool for machine learning. It is necessary that a newly suggested steganographic technique cannot be identified using feature sets that are already known. Therefore, the steganalyst must first choose a model for the cover source that the steganography is to be discovered within before they can proceed with developing a detector. The hardest and longest aspect of developing a detector is generally this one, requiring a lot of tests in which the analyst examines the steganographic approach using different iterations of characteristics that are logically intended to identify the embedding changes.

Babu et al. [9], An image enhancement method for the Cuckoo Search Algorithmin with Morphological Operation is presented coupled this research. Digital pictures are developed these days in numerous image processing applications. Applications for image processing include manufacturing, computer interfaces, machine vision, compression for storage, and more. The outcomes of the experiments show that the suggested method produces original color photographs free of noise and employs an adaptive mechanism to improve the image quality.

Bouchra et al. [10-12], The study examines how well four feature extraction techniques based on the Discrete Cosine Transform (DCT) capture discriminative information for the detection of handwritten numbers. The MNIST reference database and a modified version of the database created by removing non-information-barring sections during pre-processing have been used to assess the approaches. An SVM classifier was used to process each feature set, and its accuracy and reduction rate were assessed. The findings show that, in comparison to their equivalents, the block-based DCT zigzag coefficients produce improved accuracy

3. Present work

Steganography is a method for hiding the existence of secret data in digital media by concealing it. In the suggested Cuckoo approach, the embedding technique is LSB based. The proposed method contains 3 major steps

- Generation of dataset
- Feature extraction
- Feature Optimization

3.1 Step 1: Generation of dataset

The dataset must first be created using cover pictures, and then the Least Significant Bit (LSB) approach must be used to embed the secret message into the cover image in order to produce the stego images. The feature extraction process, which is the second stage, is then given these stego pictures.

The secret picture is transformed using a binary image during the embedding process based on the threshold value. The corresponding block is replaced in its place once the pixel value is greater than or equal to the threshold value. If not, the block contains zero embedded in it. The secret picture is then divided into double shares at that time. The partial copyright info of the hidden image is included in Share 1 of our suggested strategy, and another piece of copyright data is included in Share 2. Subsequently, the hidden picture is embedded. Below is an explanation of it.

3.2 Step 2: Feature Extraction Using LBP

In computer vision, a kind of visual descriptor called Local Binary Patterns (LBP) is utilized for categorization. The specific instance of the suggested Texture Spectrum model is LBP. Since then, it has been discovered to be a potent feature for texture classification; moreover, it has been discovered that combining LBP with the Histogram of Oriented Gradients (HOG) descriptor significantly enhances the detection performance on certain datasets. A comparison of the original LBP's several enhancements in the area of background subtraction. Using the embed picture, an inverse embedding operation is carried out throughout the extraction process to separate the secret data, which appears differently in respect to the information. The extraction method follows the same proportional process as the embedding algorithm, with the ultimate goal of locating the starting picture during the underlying stage.

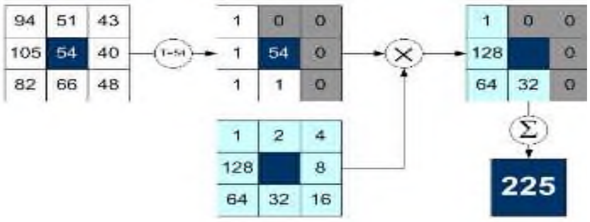


Fig 1. The stages of LBP calculation

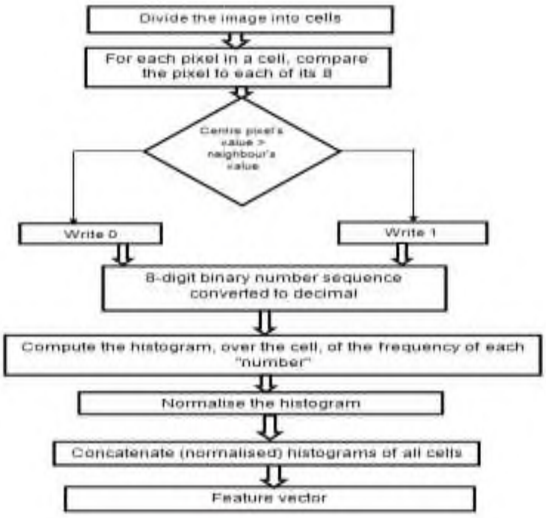

Divide the image into cells
For each pixel in a cell, compare the pixel to each of its 8
Centre pixel's value > neighbour's value
Write 0
Write 1
8-digit binary number sequence converted to decimal
Compute the histogram, over the cell, of the frequency of each "number"
Normalise the histogram
Concatenate (normalised) histograms of all cells
Feature vector

Fig 2. Flow Chart of LBP Vector

- In its most basic form, the LBP feature vector is made as follows:
- Acellularized the window that was being examined, using, for example, 16x16 pixels for each cell.
- Beginning at the left top and working your way down to the left center, left bottom, right top, and so on, compare each pixel in a cell to each of its eight neighbors. Draw a circle around the pixels, tracing it either clockwise or counterclockwise.
- When the value of the central pixel is greater than that of the neighboring pixel, write "0". In the event that not, enter "1". This results in an 8-digit binary number that can be easily converted to decimal.
- For every "number" that appears across the cell (i.e., any combination of pixels that is smaller or larger than the center), compute the frequency histogram. This histogram may be compared to a 256-dimensional feature vector.
- The histogram can be normalized if you like.
- Join the normalized histograms of every cell. Thus, a feature vector for the entire window is acquired.

3.3 Step 3: Feature Optimization using Cuckoo Search Optimization

Cuckoo Search Optimization is used to choose the most pertinent characteristics. Cuckoos are a unique kind of bird, and this conclusion is based on the way the feathery animals are raised. The fundamental idea underlying this computation is that the cuckoo-winged creature deposits its eggs in the nest of another bird. In the unlikely event that the neighboring bird discovers the eggs in its nest are not its own, it will either discard the foreign eggs or leave the nest and build a new one elsewhere. In this way, the winged species that resides there has the ability to detect foreign eggs, and each egg indicates a unique configuration. The goal is to find the best solution to a problem. A cuckoo egg hatches before an egg from a flying species and matures faster than an egg from a bird. Therefore, Pa ϵ [0,1] is the probability that a flying host animal will be able to recognize the outsider eggs. The cuckoo uses demand flights' erratic movement to choose at random the host settle location (Vpq) where it will deposit its egg. It is provided by:

Vpqt+1 = Vt+Spq*Levy(λ)*α

Levy(λ) = (Γ(1+λ)*sin(π* λ/2))/((1+ λ)/2) * λ * S(λ-1)/2

S>0, is the estimated advancement that should be correlated with the size of the relevant issue. In the unlikely event that it is too large, the newly constructed arrangement will deviate too much from the previous configuration. If s is too little, the change won't likely be significant enough to be seen, and this kind of research isn't very effective.

Spq = Vpqt – Vfqt

In this case, p,f ϵ {1,2,…,m}; q ϵ{1,2,….D}; D denotes the number of parameters that need to be improved, and m is the total population of host places.

The winged creature that is the host detects the foreign egg and is likely to see it as a companion because it is an egg:

Prop=(0.9*Fitp/max(Fit)) +0.1

Whereas prop indicates the possibility that the cuckoo's egg will survive, Fitp denotes the arrangement p's wellness evaluation in relation to the nature of an egg in its home place. If Pa ϵ [0,1]>prop, the cuckoo finds a new host's house to lay eggs in, smashes the outsider egg, and marks the egg as belonging to it. If not, the egg will hatch, the cuckoo will grow up and survive for the cutting edge given the fitness function below,

xp=xpmin+ r and (0,1) *(xpmax - xpmin)

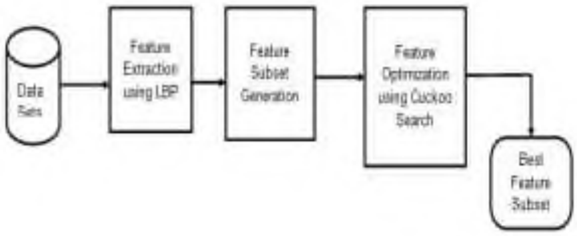

Data Sets
Feature Extraction using LBP
Feature Subset Generation
Feature Optimization using Cuckoo Search
Best Feature Subset

Fig. 3. The General diagram of CS –based FS approach

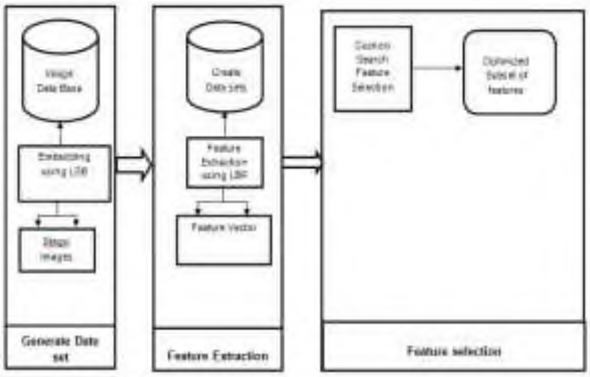


Fig 4. The General structure of proposed steganalysis method

4. Experimental results

Initially, the input image is selected from the database. Medical photos are used as input in this case. In our suggested technique, we are taking into account over 150 to 200 photos for the analysis of the visual cryptography process. Here, we're going to talk about a few sample image outcomes for assessment. Fig. 5(a) displays the sample photographs, and Fig. 5(b) displays the hidden image. As may be seen below,

4.1 Evaluation metrics

The following measures are used to assess the suggested approach, and an example of each is shown below:

"Peak Signal to noise ratio (PSNR)"

The PSNR value is used to assess the embed image's quality. It is the ratio of the embedded picture to the source image. The mean square error (MSE) is used to determine the PSNR. The mean squared error between the highest signal energy and the defiling noise is given by the Mean Squared Error (MSE). The MSE value drops as the PSNR value rises, making it possible to produce an embedded picture with improved quality.

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right)$$

$$MSE = \frac{1}{m*n}\sum_{x=1}^{m}\sum_{y=1}^{n}[I(i,j)-E(i,j)]^2$$

$$MSE = \frac{1}{m*n}\sum_{x=1}^{m}\sum_{y=1}^{n}[I(i,j)-E(i,j)]^2$$

Where;
I (i, j) Original image
E (i, j) Embed image

4.2 Normalized correlation (NC)

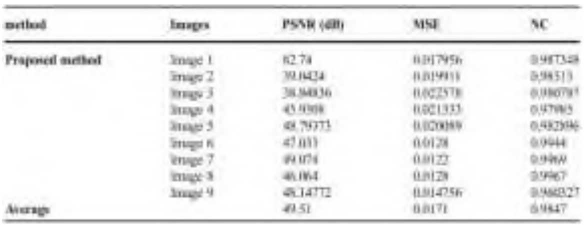
The difference between the recovered source image I(i, j) and the embed image E(i, j) is measured using the NC. The quality of the recovered source picture increases with NC value.

$$NC = \frac{\sum_{x=1}^{m}\sum_{y=1}^{n} E(i,j)-I(i,j)}{h \times w}$$

Where;
E (i, j) Embed image
I (i, j) Restored source image
h Height of the embed image
w Width of the embed image

Using assessment metrics like PSNR, MSE, and NC value, the efficacy of the suggested visual cryptography-based medical picture authentication and verification is demonstrated. These assessment criteria are used to produce a variety of experimental outcomes; a complete explanation is provided in Table 1.

Table 1. Performance of the suggested method with an embedded picture



method	Images	PSNR (dB)	MSE	NC
Proposed method	Image 1	82.74	0.017956	0.987348
	Image 2	39.0424	0.019911	0.98313
	Image 3	38.84836	0.022578	0.980787
	Image 4	45.9308	0.021333	0.97985
	Image 5	48.79373	0.020089	0.982896
	Image 6	47.033	0.0128	0.9944
	Image 7	49.074	0.0122	0.9969
	Image 8	46.064	0.0128	0.9967
	Image 9	48.14772	0.014756	0.984827
Average		49.51	0.0171	0.9847

The efficacy of the suggested technique is evaluated using various medical images. Here, nine images are taken into consideration. Using the suggested approach, the PSNR value for image 1 is 82.74db, the MSE value is 0.017956, and the NC value is 0.9873. Similarly, image 2 yields 39.04 dB PSNR, 0.019911 MSE, and 0.98313 of NC using the suggested approach. The suggested approach yields the following results: an MSE of 0.022578, an NC of 0.980787, and a PSNR of 38.84 decibels. Using the suggested approach, the PSNR value for image 4 is 45.9308 dB, the MSE value is 0.021333, and the NC value is 0.97985.

For image 5, the suggested approach yielded a PSNR value of 48.79373db, an MSE value of 0.020089, and an NC value of 0.982896. Thus, the total PSNR value acquired by applying the suggested technique is 51.07 dB; the total MSE value produced by applying the suggested method is 0.020373; and the total NC value obtained by applying the suggested method is 0.982802. Using the suggested approach, the PSNR value for image 6 is 47.03db, the MSE value is 0.0128, and the NC value is 0.9944. Similarly, image 7 yields 49.074 dB PSNR, 0.0122 MSE, and 0.9969 of NC using the suggested approach.

The suggested approach yields the following values: 46.064 dB for PSNR, 0.0128 for MSE, and 0.9967 for NC. Using the suggested approach, the PSNR value for picture 9 is 48.14db, the MSE value is 0.0147, and the NC value is 0.9847. As a result, our suggested visual cryptography approach for medical picture authentication and verification has a low error value, high PSNR, and NC value. A description of the suggested technique's comparison result is provided in a later section.

4.3 Comparative analysis

Comparing the suggested technique's comparative yields with those of the old procedures allows for the evaluation of the proposed method's efficiency. We have utilized both the suggested approach and the current method for comparison. Here, the suggested approach (LSB + LBP based cuckoo search optimization) takes into account previous research. Fig. 5 displays a graphical depiction of the PSNR value comparison. It is displayed below.

Table 2. Comparing the Proposed PSNR Value to the Current

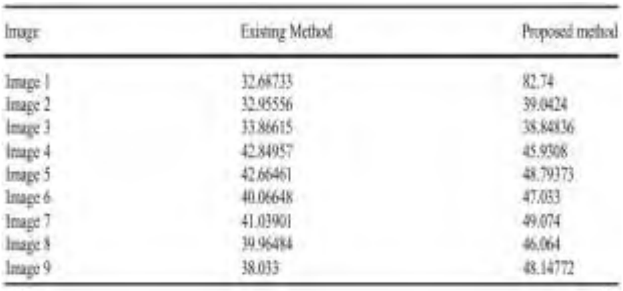


Image	Existing Method	Proposed method
Image 1	32.68733	82.74
Image 2	32.95556	39.0424
Image 3	33.86615	38.84836
Image 4	42.84957	45.9308
Image 5	42.66461	48.79373
Image 6	40.06648	47.033
Image 7	41.03901	49.074
Image 8	39.96484	46.064
Image 9	38.033	48.14772

It is evident from the above figure that, for image 1, the PSNR value obtained with the suggested technique is 82.74db, whereas the PSNR value obtained with the current method is 32.68db. For image 2, the PSNR obtained using the present technique is 32.95db, whereas the PSNR produced using the suggested method is 39.04db. For image 3, the PSNR value acquired using the current technique

e-ISSN 2456-7701
Vol. 5 Issue No. 4, October-December 2023

is 33.86 dB, whereas the PSNR value obtained using the suggested method is 38.84 dB. For image 4, the PSNR value produced using the suggested technique is 45.93db, while the value obtained using the present method is 42.84db.

The PSNR value for picture 5 produced with the suggested approach is 48.79db, compared to 42.66db using the current method. For picture 6, the PSNR value produced using the present approach is 40.066db, whereas the value acquired using the suggested method is 47.033db.

For picture 7, the PSNR value acquired using the current technique is 41.03 dB, whereas the PSNR value produced using the suggested method is 49.074 dB. For picture 8, the PSNR value produced using the suggested technique is 46.064db, whereas the value obtained using the present method is 39.96db.

The PSNR value for image 9 produced using the suggested technique is 48.14db, compared to 38.033db using the current method. Because the suggested approach has a higher PSNR value than the current method, it is the most effective.

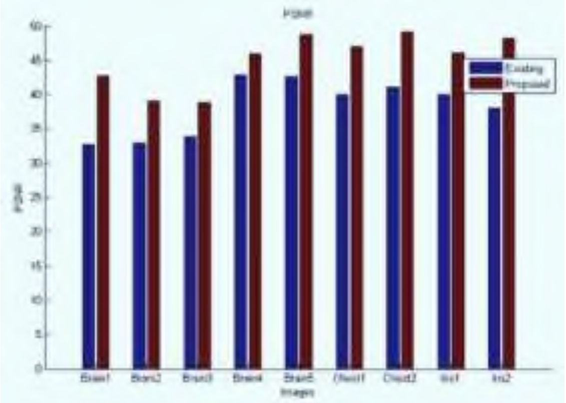


Fig 5. Comparing the suggested PSNR value to the existing

Table 3. Comparing the proposed MSE value to the existing

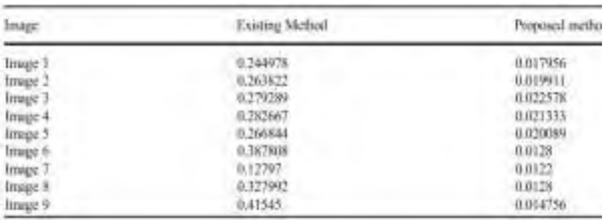


Image	Existing Method	Proposed metho
Image 1	0.244978	0.017956
Image 2	0.263822	0.019911
Image 3	0.279289	0.022578
Image 4	0.282667	0.021333
Image 5	0.266844	0.020089
Image 6	0.387808	0.0128
Image 7	0.12797	0.0122
Image 8	0.327992	0.0128
Image 9	0.41545	0.014756

Fig 6 displays the graphical depiction of the MSE value comparison. It is displayed below.

The MSE values for picture 1 generated by the proposed and current methods are 0.017956 and 0.244978, respectively, as shown in Fig. 7. The MSE values for picture 2 obtained with the current and suggested methods are 0.263822 and 0.019911, respectively. For picture 3, the MSE values that were produced using the current and suggested methods are 0.279289 and 0.022578. The MSE values for picture 4 obtained with the current approach and the suggested method are 0.282667 and 0.021333, respectively.

The MSE values obtained with the current and suggested methods are, respectively, 0.266844 and 0.020089. Using both the suggested and current methods, picture 6 yielded an MSE value of 0.387 and 0.0128, respectively.

The MSE values for picture 7 obtained with the current and suggested methods are 0.127 and 0.0122, respectively. The MSE value for picture 8 is 0.0128 for the suggested technique and 0.3279 for the present method. The MSE values obtained with the current and suggested methods are, respectively, 0.415 and 0.0147. As a result, our suggested approach has a lower MSE value than the current one.

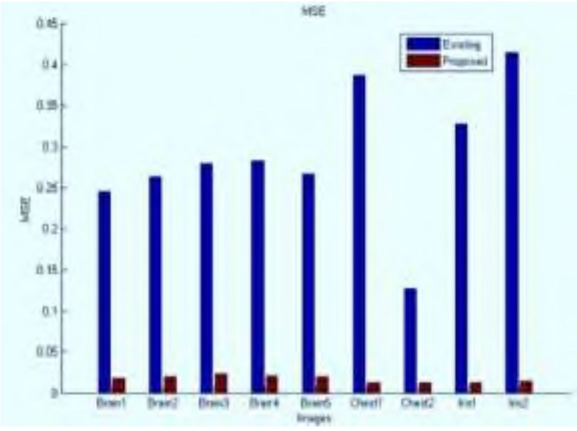


Fig 6. Comparing the suggested MSE value to the existing

Today, data security is a difficult problem in data communications that affects many different aspects, such as reliable database maintenance, robust data encryption, and secure communication channels. Visual cryptography is a unique sort of encryption that conceals data in pictures such that, when the right key image is used, human eyesight can decrypt it. Visual cryptography makes use of two see-through pictures. The secret information is contained in the other image, while random pixels are present in the first. One of

e-ISSN 2456-7701
Vol. 5 Issue No. 4, October-December 2023

the photos cannot have the secret information extracted from it. To show the information, layers and transparent photos are needed. Particular applications for it include biometric security, watermarking, electronic remote voting, bank client identification, and so on. A biometric cryptosystem uses a key pair created from the individual's identify, such as fingerprint imprints, to give a more secure approach to encryption and decoding techniques. Furthermore, there is a possibility that a forged signature will be encountered during a transaction in a core financial system.

Additionally, a customer's password in the online banking system might be compromised and used improperly. Visual cryptography, which enables visual information (text, images, etc.) to be encrypted so that the human visual system can conduct the decryption without the assistance of computers, can be used to tackle this kind of security difficulty.

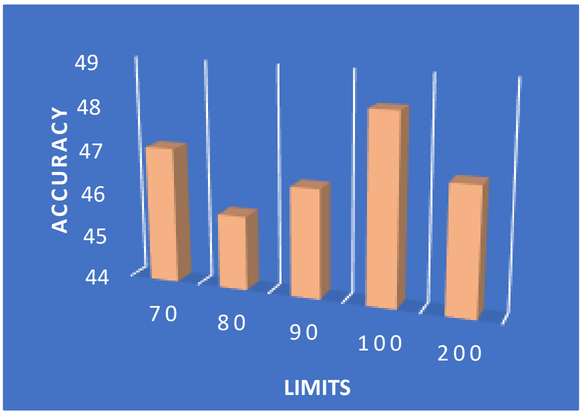


Fig. 7. Impact of various limits on accuracy of LSB Cuckoo method

This section evaluates the efficiency of the recommended technique across several parameter settings. Figures 7 and 9 demonstrate how thresholds affect the chosen subset of features. The optimal values for LSB cuckoo and LBP are 300 and 100, respectively. This value indicates that using this group of qualities leads to the maximum level of fitness. Our proposed technique effectively improves LSB cuckkoo and LBP accuracy, as seen by these figures. Figure 7 illustrates how different limit types affect the proposed technique. The recommended limit value is 100.

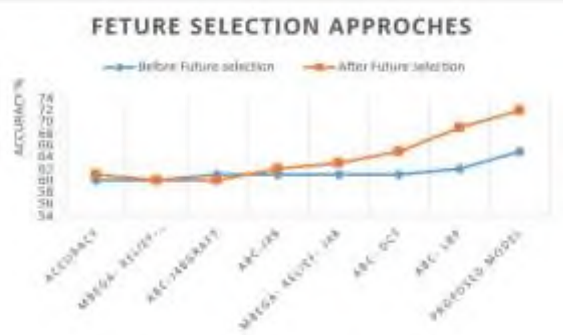


Fig. 8. A comparison of the differential steganalysis method's classification accuracy on LSB cuckoo method

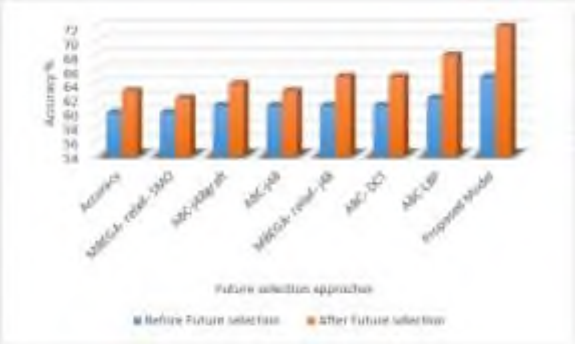


Fig. 9. A comparison of the various steganalysis method's classification

CONCLUSION

Steganography is a technique used to communicate secrets behind seemingly innocent coverings in an attempt to hide their presence. The usage and use of digital picture steganography and its variants are expanding.

People are looking at steganography as a way to get around laws that forbid powerful encryption and cryptography and send communications discreetly. Steganography and steganalysis will always be developing new methods to oppose each other, just like with the other major inventions of the digital age: the conflict between cryptographers and cryptanalysis, security professionals and hackers, record labels and pirates.

This work presents a novel image steganalysis LBP approach that utilizes the wrapper strategy for classification and is based on the optimization feature extraction of Cuckoo Search. The proposed approach is a unique feature-based resilient steganography technology which preserves the local structure of the cover in the final stego image. When compared to the LBP-based DCT approach, the recommended strategy performs better than most state-of-the-art steganographic systems, as shown by several performance evaluation experiments. Modern steganography breaks the local structure of the cover, enabling strong statistical feature-based steganalysis to find hidden data.

References

[1]. Piyush Goel, “Data Hiding in Digital Images: A Steganographic Paradigm”, proceedings of theses, IIT Kharagpur, May 2008.

[2]. Chen, C., & Shi, Y. Q. “JPEG Image Steganalysis Utilizing both Intrablock and Interblock Correlations. In IEEE International, Symposium on Circuits and Systems, ISCAS (pp. 3029–3032). Seattle, WA, 2008.

[3]. Meenpaa, T., Ojala, T., Pietikainen, M., Soriano, “Robust Texture Classification by Subsets of Local Binary Patterns. In: Proc. 15th International Conference on Pattern Recognition, vol. 3, pp. 947–950, 2010.

[4]. L ladha & T Deepa, “Feature Selection Method and Algorithms”, International Journal on Computer Science & Engineering (IJCSE), May 2011.

[5]. Jan Kodovsky, “Steganalysis of Digital Images Using Rich Image Representations and Ensemble Classifiers” proceedings of Dissertation, Graduate School of Binghamton University, State University of New York, 2012.

[6]. R Sagayam & Mrs K Akhilandeshwari, “Ant Colony & Bee Colony Optimisation for Spam Host Detection”, International Journal of Engineering Research & Development vol 4, issue 8, pp.26-32, Nov 2012.

[7]. Mohammadi, F. G., & Abadeh, M. S, “A Survey of Data Mining Techniques for Steganalysis”, (pp. 1–25). Rijeka:In. Tech Recent advances in steganography 2012.

[8]. Kodovsky J, Fridrich J & Holub V, “Ensemble Classification for Steganaysis of Digital Media”, IEEE transactions on Information Forensics and Security, PP.432-444, 2012.

[9]. Ratna Babu, K. and K.V.N. Sunitha, “Enhancing Digital Images Through Cuckoo Search Algorithm in Combination with Morphological Operation”, Journal of Computer Science, July 2014.

[10]. Singh, S. P., Nitu Singh, Jai Shanker, Yogendra Kumar, and Dhananjai Yadav. "Pressure Dependence of Debye Temperature AND Thermoelastic Properties for HCP-IRON (ε-FE)." *J. Sci. Tech. Res.* 4, no. 2 (2022): 01-05.

[11]. Prajapati, Vinita, Rekha Pyasi, and P. L. Verma. "DFT Computations of EPR Hyperfine Coupling Constants of Some Isotropic Transition Metal Complexes." *Journal of Science and Technological Researches* 4, no. 4 (2022): 30-34.

[12]. Bouchra E L Quacimy, Mounir Kerroum & Ahmed Hammouch, “Feature Extraction Based on DCT for Handwritten Digit Recognition”, IJCI International Journal of Computer Science Issue, VOL 11, Nov 2014.