Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/140622

Optimal Image Encryption in Frequency Domain using Hybrid Deer Hunting with Artificial Bee Colony with Hybrid Chaotic Map

S. Saravanan and M. Sivabalakrishnan*[2]

School of Computing Science and Engineering, Vellore Institute of Technology, Chennai, India

Received: 2 Jul. 2020, Revised: 2 Aug. 2020, Accepted: 18 Aug. 2020
Published online: 1 Nov. 2020

Abstract: A novel image encryption method in the frequency domain is proposed in this paper by introducing an optimized Hybrid Chaotic Map (HCM). In the initial step, the Discrete Wavelet Transform (DWT) transforms the image into the frequency domain. The developed image encryption in the frequency domain is composed of various steps, such as frequency domain conversion, key generation, image encryption using optimized HCM, and image decryption. The most important step in the chaotic-based image encryption is the generation of the key which is performed using the Secure Hash Algorithm (SHA-256) cryptographic Hash algorithm. Next, the image encryption is performed by incorporating Piece-Wise Linear Chaotic Map (PWLCM) and Two Dimensional Linear Chaotic Map (2DLCM) using HCM. Performance is enhanced by the parameter optimization when hybridizing the two chaotic maps. During the parameter optimization, the main aim is to maximize the information entropy. The HCM parameter tuning is done by the hybridized optimization algorithm known as the Deer Hunting-based Artificial Bee Colony algorithm (DH-ABC). Performance of the presented method is evaluated by correlating it with various state-of-the-art models.

Keywords: Deer Hunting-based Artificial Bee Colony Algorithm, Discrete Wavelet Transform, Hybrid Chaotic Map, Piece-Wise Linear Chaotic Map, Secure Hash Algorithm-256, Two Dimensional Linear Chaotic Map.

Nomenclature

Abbreviation	Description
HCM	Hybrid Chaotic Map
UACI	Unified Averaged Changed Intensity
GWO	Grey Wolf Optimization
DWT	Discrete Wavelet Transform
PSNR	Peak Signal-to-Noise Ratio
SAGWO	Self Adaptive Grey Wolf Optimization
SHA	Secure Hash Algorithm
PWLCM	Piece-Wise Linear Chaotic Map
XOR	Exclusive OR
ABC	Artificial Bee Colony Algorithm
KPA	Known Plaintext Attack
FRQI	Flexible Representation for Quantum Images
WOA	Whale Optimization Algorithm
2DLCM	Two Dimensional-Logistic Chaotic Map
DE	Differential Evolution
2-D	Two Dimensional
NPCR	Number of Changing Pixel Rate
DH-ABC	Deer Hunting-based Artificial Bee Colony algorithm
LFSR	Linear Feedback Shift Register
MSE	Mean Square Error
CI-WOA	Coefficient Improved-Whale Optimization Algorithm
CPA	Chosen Plaintext Attack
DFT	Discrete Fourier Transform
DHOA	Deer Hunting Optimization Algorithm

1 Introduction

Nowadays, digital image has been extensively used. There is a quick increase in digital signal processing technology

* Corresponding author e-mail: sara.vanan2013@vit.ac.in

and Internet technology. Hence, the major significant research problem relies on the image data security. Data security [6] is safeguarded by the image encryption technique. Few of the random transforms and the phase operations used for designing the image encryption algorithms are the fractional Mellin transform, Hadamard transform, random phase encoding, ... etc. Matthews proposed the initial chaos-based image encryption scheme. The function of diffusion and confusion can be recognized by the chaotic map. On the basis of chaotic features, various image encryption algorithms have been developed [7] [8]. The chaos-based schemes produced by the chaotic map have several limitations, like the weak sensitivity of the key stream and the short cycle length.

Image encryption techniques are divided into two categories: frequency domain methods [9] and spatial domain methods. The image plane itself is referred to as the spatial domain. This technique is dependent on the direct manipulation of pixels present in an image. The correlation between the pixels is destroyed by the general encryption, so the encrypted images are made incompressible [11]. The Fourier transform present in an image is altered depending on the frequency domain processing approaches. The inverse process with no information loss is reconstructed totally by the Fourier transform. Without any information loss, it permits to work in the "Fourier domain" and then go back to its original domain. On the basis of several methods, encryption approaches are realized as usual [10].

Several quantum image encryption algorithms have been developed in 2016 like quantum image encryption algorithm on the basis of quantum image XOR operations advanced [14], quantum frequency transform [13], new quantum image encryption by means of one-dimensional quantum celluar automata [12], and a quantum color image encryption algorithm dependent on a hyper-chaotic system. On the basis of the learning from these quantum encryption algorithms, it can be revealed that the quantum image encryption algorithms research is just a starting only. The encryption framework is lacked for the quantum images. The encryption is recognized by selecting few transform techniques [15]. Thus, a quantum image encryption framework based on the frequency domain transform needs to be developed.

The major enhancement of the paper is enlisted, as follows:

(i) To introduce an optimized HCM by a novel image encryption method in the frequency domain using various steps like "key generation, image encryption using optimized HCM, and image decryption".

(ii) To perform the frequency domain transformation by DWT and the image encryption is performed by HCM with the incorporation of the PWLCM and 2DLCM.

(iii) To enhance the performance of image encryption by optimizing the parameters of HCM to achieve the maximum information entropy using the hybridized DH-ABC.

The organization of the paper is listed, as follows: Section I provides an introduction on the image encryption in the frequency domain. The various literary works related to the image encryption are listed in Section II. The description of the developed methodology for image encryption in the frequency domain is presented in Section III. The key initialization and contribution of HCM are explained in Section IV. Section V provides the optimized hybrid chaotic map for image encryption. Results and discussion are addressed in Section VI. Section VII is devoted to conclusion.

2 Literature Survey

A. Related Works

In 2017, Geng et al. [1] displayed the images in the form of FRQI. The spatial domain transform has recognized the earlier quantum image encryption algorithms for scrambling the original images regarding the position information. The color information present in the images was encoded by the frequency domain. Some conflicts like the spatial domain transform's periodicity made it easier for the recovery of the original image. Therefore, the frequency-spatial domain transforms regarding the iterative framework was proposed. On the basis of the iterative framework, geometric transform and Fibonacci transform were used by the new encryption algorithm multiple times to mess the original images position information. The color information regarding the images was encoded by the double random-phase encoding. All the quantum operations were found to be invertible, so the inverse of the encryption algorithm was known to be the quantum image decryption algorithm. The outcomes revealed that the developed algorithm provided high sensitivity as well as security.

In 2019, Weisheng et al. [2] analyzed several evaluations of key parameters like correlation, entropy, and histogram uniformity. The statistical attacks were resisted by the good behaviour of the encrypted image. This destroyed the original image's statistical properties. Every cipher pixel was damaged by the cipher-pixels and plain-pixels during the encryption procedure because of the execution of the scrambling operations and chaotic diffusion. Sensitivity of the encrypted plain-text image was also enhanced. Security was also developed against any forms of differential attacks. The hyper digital chaos has introduced high sensitivity, and therefore to guarantee the high security level, a vast key space was given to the encrypted image. Hence, a strong secure capability was provided by the encryption algorithm to resist against the brute-force attacks.

In 2011, Mohammedhasan et al. [3] developed a novel efficient technique for image encryption using the DE technique that utilized the phase and magnitude manipulation. The improvement of this work relied upon deploying the technique of keyed DFT and it was followed by the DE operations for the use of encryption.

A secret key was shared among the decryption and encryption sides. Initially, the encryption was performed on the original image using 2-D keyed DFT. In the second step, the crossover was carried out among the two components of the encrypted image and it was chosen on the basis of the LFSR index generator. In addition, the real parts of the specific components chosen were done with the keyed mutation on the basis of the LFSR index generator. Security of the outcoming indices was ensured by initializing the shared secret key with the LFSR index generator. The image pixels positions were shuffled by this process. On the basis of the DE approach, a novel image encryption scheme, which contained a simple diffusion mechanism. With the same key, an invertible process resulted in the deciphering process. The final encrypted image was a completely twisted one and enhanced the robustness of the developed method. The presented image encryption scheme revealed the simulation outcomes.

In 2009, Qiuming et al. [4] developed an image encryption algorithm in the optical transform's frequency domain with the help of random position scrambling of the phase and amplitude functions. The positions of the phase and amplitude data were scrambled in a random manner in both the vertical and horizontal directions. The key of the algorithm relied on the random position orders. The presented algorithm did not use the random phase encoding. A feasible optical implementation regarding the encryption algorithm was also provided. The capability of the algorithm was revealed by a few numerical simulations.

In 2011, Dubey and Shukla [5] developed a novel technique of multi-media content encryption. The mixture of discrete cosine transform method and two dimensional chaotic maps were developed for the video data encryption in the chaotic map oriented encryption scheme. The presented encryption scheme provided more security. The chaos comprised various interesting properties like deterministic but random such as high sensitivity to ergodicity and initial conditions, complex temporal behaviour, etc. These properties were mostly used for the cryptographic designs.

B. Review

Though image encryption in frequency domain provides several advantages, such as less consumption; less noise; and less reliability, it involves several limitations such as huge size, less frequency tuning range, slow switching time, and high loss of insertion. These issues are a major requirement to be resolved in the future. Major features and challenges of some existing models are listed in Table 1. Iterative framework [1] handles the periodicity of the scramble transforms problem to avoid the attacks and high key sensitivity is also produced. It also fights against the brute-force attack. However, the necessary protection against new attack types is also lacked. Digital image encryption algorithm [2] resists the statistical attacks and it also strengthens the sensitivity of the plain-text during the encryption process. A trade-off is needed between complexity and performance because of the implementation flexibility. DE approach [3] can be employed for real-time image transmission and encryption applications and more diffusion and confusion are achieved in the cipher image. Nevertheless, various image compression techniques are not included and it also cannot be applied to multimedia data. Image encryption algorithm [4] improves the security of the encrypted image and better ability is also provided in the aspects of robustness and security. However, it needs more analysis to attain further confidence. Chaotic map based encryption scheme [5] hides the statistical structure of the image data and the compression is achieved. The independency of the statistics of the cipher is also enhanced on the statistics of the plain text. Standard algorithm is not used for compatibility purposes. These challenges are motivated to find a novel technique for image encryption in the frequency domain.

3 Developed Methodology for Image Encryption in Frequency Domain

A. Architectural View

The proposed encryption method collects the data from three datasets such as: natural, medical, and satellite images. Fig. 1 displays the diagrammatic view of the proposed image encryption in frequency domain by means of HCM. Initially, using the DWT, the images are transformed into frequency domain images. Here, two chaotic maps, like PWLCM and 2DLCM, are combined and the developed model is referred to as the HCM. The SHA-256 cryptographic hash algorithm is used to provide the key here.

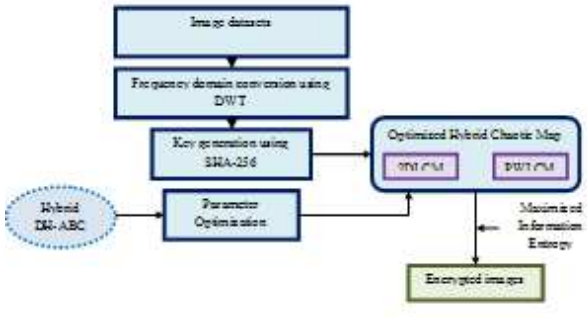

Fig. 1: Architectural view of the proposed image encryption in frequency domain

On the basis of the key that is being generated, the initialization of the piecewise parameters present in both PWLCM and 2DLCM occurs. The optimization of these

Table 1: FEATURES AND CHALLENGES OF THE EXISTING IMAGE ENCRYPTION

Author [citation]	Methodology	Features	Challenges
Geng et al. [1]	Iterative framework	(i) It produces high key sensitivity. (ii) It fights against the brute-force attack. (iii) The periodicity of the scramble transforms problem is handled to avoid the attacks.	It lacks the necessary protection against new types of attacks.
Weisheng et al. [2]	Digital image encryption algorithm	(i) The sensitivity of the plain-text is strengthened during the encryption process. (ii) It has the capability of resisting the statistical attacks.	Due to the implementation flexibility, a trade-off is needed between complexity and performance.
Mohammedhasan et al. [3]	DE approach	(i) It achieved more diffusion and confusion in the cipher image (ii) It can be used for real-time image transmission and encryption applications.	(i) This method cannot be applied to multimedia data (ii) It does not include various image compression techniques.
Qiuming et al. [4]	Image encryption algorithm	(i) It provides better ability in the aspects of robustness and security. (ii) The security of the encrypted image is improved.	More analysis is needed to attain further confidence.
Dubey and Shukla [5]	Chaotic map based encryption scheme	(i) It achieves the compression and also enhances the independency of the statistics cipher on the statistics of of the plain text. (ii) The statistical structure of the image data is hided.	It does not use the standard algorithm for the compatibility purposes.

parameters in the addressed HCM is performed by an improved meta-heuristic algorithm. The significant parameters, such as the initial piecewise points of the HCM, are optimized using the hybrid optimization algorithm known as the DH-ABC. The parameters are tuned such that the information entropy of the cipher image must reach the maximum value. The presented technique of HCM for the image encryption is composed of various procedures, such as permutation, diffusion, and transportation. Hence, the optimal initial parameters of HCM-oriented image encryption model, which enhances the effectiveness of the entire image encryption system are described

B. DWT-based Frequency Domain Conversion

The DWT [16] transformation of the provided input image is described in Eq. (1). Depending on the powers of two, the DWT utilizes the position and scale values. The values of t and τ are represented by $t = 2^f$, $\tau = h * 2^f$ and $(f,h) \in E^2$ as shown in (2)

$$X_\psi(t,\tau) = \int_{-\infty}^{\infty} z(u)\psi^*_{t,\tau}(u)du \tag{1}$$

$$\psi_{t,\tau}(u) = \frac{1}{\sqrt{2^f}}\psi\left(\frac{u - h*2^f}{2^f}\right) \tag{2}$$

The reconstruction and decomposition of the signal are the main conflicts in the inverse DWT and DWT, respectively. The main idea behind the reconstruction and decomposition is the high-pass and low-pass filtering using the up and down sampling, respectively. The hierarchically organized decompositions are the decomposition's output. The capability to choose the decomposition level depends on the desired cut-off frequency.(3), (4), and (5) describe the four finite impulse

response filters that are used to satisfy the relationships.

$$m_1(o) = (-1)^o m_0(Mo+1-o) \tag{3}$$

$$\tilde{m}_0(o) = m_0(Mo+1-o) \tag{4}$$

$$\tilde{m}_1(o) = (-1)^{o-1} m_0(Mo+1-o) \tag{5}$$

Here, the length of the filters is described by Mo, in which $o = 1,2,\ldots,Mo$, and $m_1(o)$ and $m_0(o)$ describe the high and low-pass filters, respectively. Once the image is transformed to the frequency domain with the help of DWT, SHA-256 algorithm performs the key generation.

4 Key Initialization and Contribution of Hybrid Chaotic Map

A. Key Initialization

SHA-256 cryptographic hash algorithm [17] is the new hash function and it is described with the help of 32 bit words. This technique utilizes a number of shift and additive constants. Here, the image in frequency domain is considered as the input and the key format is the output that is of constant size and composed of letters and numbers. Let the input image be denoted as Ige^{rgp}. Before the process of key generation, the input image is transformed into gray scale image. Moreover, the cryptographic algorithm known as the SHA-256 cryptographic hash algorithm is used for the key generation. Usually, the gray scale images are composed of grey shades and are present in white and black images. Here, the light intensity is used to describe every pixel values. The average of the addition of the terms R, G and B is divided into 3 for the procedure of conversion. Hence, the image obtained in the final step is referred to Ige^{grey} .

With the chaotic map, the key performs the image encryption and it is extracted using the SHA-256 cryptographic hash algorithm [17]. This hash function is described as the novel one and it is described by 32 bit words. During its functioning, the image is divided into OFC 512 bit blocks $BiBl_{(1)}, BiBl_{(2)}, \ldots, BiBl_{(OFC)}$. The 32 bits of message block nb is denoted by $BiBl_{(0)}^{(mg)}$, the next 32 bits are described by $BiBl_{(1)}^{(mg)}$, and this process is repeated till it reaches $BiBl_{(15)}^{(mg)}$. SHA-256 algorithm makes use of 64 constants, each one is 32-bit, and the subsequent results are maintained using 8 registers. (6) describes the mathematical representation of the expanded message blocks.

$$N_{nb} = \begin{cases} BiBl_{nb}^{(mg)} & for\ nb = 0,1,\ldots,15 \\ \sigma_1(N_{nb-2}) + N_{nb-7} + \sigma_0(N_{nb-15}) + N_{nb-16} & \\ & for\ nb = 16,17,\ldots,63 \end{cases} \tag{6}$$

Here, the terms σ_1 and σ_0 represent the constant functions. In the final step, the size of the key K is given by 1×256. Depending on the input images, the 256-bit key is extracted from the SHA-256 and this is also used to provide the key for the HCM [18].

B. Hybrid Chaotic Map

In the general context, the concept of 2DLCM [19] is found to be tougher over the 1DLCM. When compared with the traditional logistic maps, PWLCM finds its frequent attention in the encryption models.

2DLCM: The mathematical representation is described in (7), and it is derived depending on the discrete form. Here, the term represents the system parameter, and (yf_j, zf_j) represents the piecewise point at j^{th} iteration. (8) describes the trajectory of logistic mapping on the basis of the point j, in which (yf_0, zf_0) represents the initial value of the round.

$$2DLCM = \begin{cases} yf_{j+1} = sypa(3zf_j+1)yf_j(1-yf_j) \\ zf_{j+1} = sypa(3yf_j+1)zf_j(1-yf_j) \end{cases} \tag{7}$$

$$\begin{cases} yf_j = G_{yf}^{2E}(yf_0, zf_0, sypa, j) \\ zf_j = G_{zf}^{2E}(zf_0, yf_0, sypa, j) \end{cases} \tag{8}$$

Generally,(2) describes the complicated dynamic system. Depending on the $sypa$ value, changes happen in the dynamics of the system. Depending on the differences, G is used to denote the rules that are required for operating the map. If the system $sypa \in (-1,1)$ is composed of a single attractive node and two saddle points, then the points, such as yf and zf, tend to become unstable [19].

Piecewise Linear Chaotic Mapping: Compared with the existing logistic map [20], PWLCM [21] has gained more interest on the encryption model. Advantages of PWLCM involve simple representations, excellent dynamical behaviour, and effective implementation. More random sequence is given by the PLCM owing to its superior ergodicity, uniform invariant distribution, superior determinacy, and confusion. The positions of the pixels are used to scramble the provided sequence at the global level. The entire security of the cryptosystem is enhanced by it.

HCM: The integral principle of PWLCM into the DLCM results in HCM. Using the parameters such as $\{yf_0, zf_0, sypa, Uf, Bf_1, \ldots, Bf_8\}$, the key that is the 256-bit string is produced by the SHA-246. The term (yf_0, zf_0) describes the initial piecewise point, Uf, and the parameters of the linear congruential generator [18], $sypa$ describes the parameter of the 2DLCM. Moreover, the format of key for the HCM is $\{yf_0, zf_0, g_0, sypa, Uf, Bf_1, \ldots, Bf_8\}$. It describes the initial piecewise point of PWLCM. In the existing 2DLCM and PWLCM, the initial piecewise points are calculated depending on [21] and [19].

Hybrid permutation: Let the image size [19] be represented as $G = L \times F$ and the pixel count in G is represented by MF. The column permutation, i.e. the co-ordinate sequence of z is described by ZF_{se}, and the row permutation, i.e the co-ordinate sequence of y is represented by YF_{se} . The term J_{se} describes the co-ordinate sequence of y . The two terms ZF_{se} and YF_{se} are described in (9)

$$\begin{cases} YF_{se} = \{yf_1, yf_2, \ldots, yf_{MF}\} \\ ZF_{se} = \{zf_1, zf_2, \ldots, zf_{MF}\} \\ J_{se} = \{g_1, g_2, \ldots, g_{MF}\} \end{cases} \tag{9}$$

Here, the notations YF, ZF, and J describe the matrix notation of YF_{se}, ZF_{se}, and J_{se}, respectively.

Hybrid Diffusion: The considerable difference [19] present in the cipher image is described by the minimum difference in the input image. During adequate rounds, the initialization of the diffusion properties takes place. Hence, the input image becomes indecipherable on finishing the second round.

Hybrid Transportation: The matrix E is given [19] by the addition of YF, ZF, and J. The mathematical representation for this description is provided in (10).

$$E = YF + ZF + J \tag{10}$$

With the help of the encryption procedure, the ciphertext image represents the HCM transposition phase as in (11). Also, (12) describes the input image attained during the hybrid transposition's decryption.

$$O = (G+1)\ mod\ US \tag{11}$$

$$G = (O-1)\ mod\ US \tag{12}$$

5 Optimized Hybrid Chaotic Map for Image Encrption

A. Objective Model and Parameter Encoding

The HCM is used by the presented technique to perform the image encryption. The optimization is focused by the parameters of both the chaotic maps to improve the encryption procedure. The combination of PWLCM and 2DLCM results in HCM. The optimization is done by considering the three parameters that are the first piece-wise points of HCM with the help of the presented DH-ABC.

During the proposed encryption process, the image is encrypted using HCM. The encryption procedure is improved by focusing on the optimization process of the parameters of both the chaotic maps. The parameters taken for the optimization are g_0, zf_0, and yf_0. These parameters are optimized using the proposed DH-ABC, so the information entropy between the actual and the cipher image should be maximum, and it is called as the objective function as in (13). Entropy is a measure of image information content, which is interpreted as the average uncertainty of information source. In Image, Entropy is defined as corresponding states of intensity level which individual pixels can adapt. (14) describes the related entropy equation.

$$Ob\ fn = max(Ety) \tag{13}$$

$$Ety = \sum_j Qe_j\ log_2\ Qe_j \tag{14}$$

Here, the probability of difference among the two nearby pixels j is represented by Qe_j.

Chaotic Parameter Encoding: The three parameters that are the initial piecewise points of HCM are considered for the optimization processes with the help of the developed DH-ABC. The solution encoding of the key optimization is displayed in Fig.2 for the HCM-oriented image encryption. The parameters considered for optimization are f_g of PWLCM and zf_0 and yf_0 of 2DLCM. The proposed DH-ABC performs the optimization process. The bounding limit of the solution lies in between the range of (0.001-1).

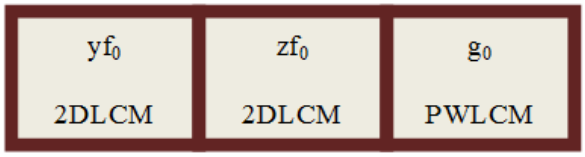

Fig. 2: Solution encoding of the HCM's parameter optimization

The motivation of the existing DHOA [22] is the human's hunting characteristics towards the deer. The main idea is to attain the human's optimal position to hunt the deer. The encircling behaviour is represented in (15) as below.

$$lp_{j+1} = lp^{lr} - B.c.\left|C \times lp^{lr} - lp^{j}\right| \tag{15}$$

In the aforementioned equation, lp represents the position, j represents the iteration, lp^{lr}; B and C represents the coefficient vectors, and c represents the random number.

In the existing ABC [68] algorithm, three types of bees: scout bees, onlooker bees, and employed bees are present. The position of food source is recorded and the search space is performed by the employed bees. This information is then transmitted to the onlooker bees. Every food source's position attains the feasible solution. "Food Number" describes the feasible solution count. Considering the information that is being transmitted by

the employed bees, the food sources are chosen by the onlookers as in (16).

$$y_{lm} = y_{lm}(p-1) + \varphi_{lm}\lfloor y_{lm}(p-1) - y_{nm}(p-1)\rfloor \quad (16)$$

Here, m represents the one dimension of the l^{th} food source, m and l represent the random numbers, as well as $y_{lm}(p)$ and $y_{lm}(p-1)$ represent the location of the new and the old food sources, respectively. The random index value is denoted by n , $n \neq l$ and φ_{lm} describes the random number that lies in between the value of [-1,1]. The position is neglected by the employed bee to become a scout bee that globally searches the new food source as in (17).

$$Y_j(0) = Y_{lb} + (Y_{lb} - Y_{ub}).rand(0,1) \quad (17)$$

Here, the terms Y_{ub} and Y_{lb} represent the upper and lower bounds of the feasible solutions, respectively.

The ABC algorithm has many benefits, such as capability of exploring local solutions, flexible and simple implementation, and robustness. However, there exist few shortcomings, such as slow sequential processing, more objective analyses count, and the requirement of secondary information. Moreover, more potential capability is present in the DHOA algorithm to obtain the best results. Hence, DHOA and ABC are integrated to form the hybrid DH-ABC algorithm. The trial is considered in the proposed algorithm. Trial is incremented when no enhancement happens. The enhancement is performed in the onlooker bee phase. It is decided on the basis of trial checking. If this condition is satisfied, then the onlooker bee's update process is performed as in (9) of DHOA. Hybrid optimization methods are formed by combining many optimization algorithms. Furthermore, convergence occurs in a very fast manner. When differentiated with various machine learning algorithms [23], the convergence behaviour attained the best results. The pseudo code of the proposed DH-ABC is displayed in Algorithm 1.

Algorithm 1: Proposed DH-ABC

The food sources and its fitness are initialized and evaluated.
The employed bees are sent to the available food source
$j = 0$
while(end condition is not satisfied)
The employed bee phase is done
  if $(q_k < 5)$
    if $(prb(k) < 0.7)$
      Do the update process by (15)
    else
      Onlooker bee phase undergoes update process as in (16)
    end if
  else
    Scout bee phase undergoes update process as in (17)
  end if
  if(no enhancement in fitness value)
    $q = q + 1$
  else
    $prb = (0.9 \times fitn(fitn_{max})) + 0.1$
  end if
end while

6 Results and Discussion

A. Experimental Setup

The developed optimal image encryption in frequency domain with hybrid DH-ABC-oriented HCM was implemented in MATLAB 2018a, and the performance evaluations were performed. The datasets gathered are natural, medical and satellite images. The population size was taken as 10 and the maximum number of rounds performed was 25. Performance of the proposed DH-ABC-oriented HCM was differentiated with various meta-heuristic algorithms like SAGWO-2DLCM [24], HCM [24] [25], GWO-HCM [26], SAGWO-HCM [24], WOA-HCM [27], and CI-WOA-HCM to prove the feasibility of the proposed method.

B. Encryption Results

The encryption results of the original and the cipher images along with the histogram are displayed in Fig.3. The pixel intensity values of the histogram of both the actual as well as the cipher images are generated by the histogram evaluations. The histogram is a graph present in the specific image and provides data about the pixel count of an image at every altered intensity value. This analysis is done between the actual images and the corresponding cipher images are also graphically represented. The analysis revealed that the histogram of the actual images is entirely different for all the images and the histograms are nearly similar in the cipher images.

C. Analysis on Information Entropy

The quality of the image encryption is defined using the value of the information entropy. The value of entropy of the cipher image should be important as that of the actual image. Table II describes the obtained entropy values with various models in every category. For the natural images, the mean of the presented DH-ABC-HCM is 7.99, and it is maximum when differentiated with various traditional algorithms. The mean of the developed DH-ABC-HCM for medical images is 2.8% better than SAGWO-2DLCM, 2.7% improved than HCM, GWO-HCM, and WOA-HCM, 2.6% improved than SAGWO-HCM, and 2.64% improved than CI-WOA-HCM. Thus, it was revealed that the proposed image encryption model was very effective in the evaluation of information entropy.

D. Analysis on Key Sensitivity, NPCR, and UACI

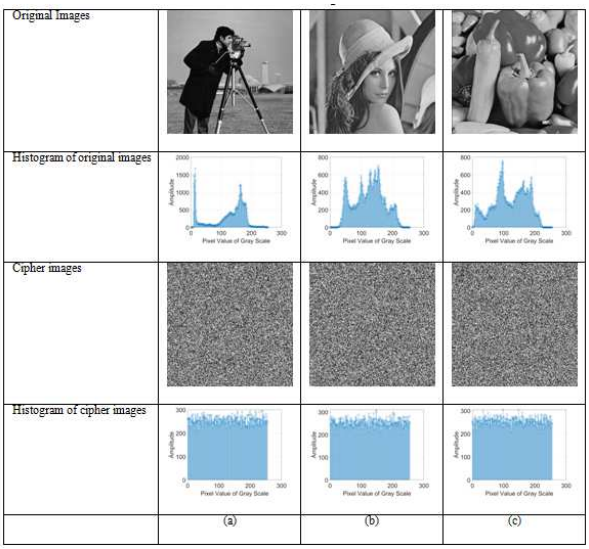

Fig. 3: Solution encoding of the HCM's parameter optimization

Table 2: Analysis on Information Entropy for Proposed and Conventional Image Encryption Models in Frequency Domain

Methods	Natural	Medical	Satellite
SAGWO-2DLCM [24]	7.9676	7.9674	7.9684
HCM [24][25]	7.9562	7.9611	7.963
GWO-HCM [26]	7.9643	7.9667	7.9634
SAGWO-HCM [24]	7.9657	7.9643	7.9675
WOA-HCM [27]	7.9682	7.9711	7.9683
CI-WOA-HCM	7.9723	7.9889	7.9715
DH-ABC (Frequency domain)	7.9913	7.9981	7.9924

Table 3: Analysis on mean for proposed and conventional image encryption models in frequency domain

Key Sensitivity Analysis			
Methods	Natural	Medical	Satellite
SAGWO-2DLCM[24]	16.938	16.75	16.703
HCM [24][25]	16.553	16.785	16.523
GWO-HCM [26]	16.653	16.649	16.554
SAGWO-HCM [24]	16.683	16.785	16.851
WOA-HCM [27]	17.021	16.574	16.852
CI-WOA-HCM	17.105	16.818	16.892
DH-ABC (Frequency domain)	17.585	17.05	17.01
NPCR Analysis			
Methods	Natural	Medical	Satellite
SAGWO-2DLCM [24]	99.561	99.688	99.663
HCM [24][25]	99.692	99.648	99.6
GWO-HCM [26]	99.356	99.521	99.556
SAGWO-HCM [24]	99.495	99.302	99.614
WOA-HCM [27]	99.575	99.619	99.329
CI-WOA-HCM	99.595	99.620	99.624
DH-ABC (Frequency domain)	99.651	99.665	99.687
UACI Analysis			
Methods	Natural	Medical	Satellite
SAGWO-2DLCM [24]	33.4245	33.2795	33.4687
HCM [24][25]	33.4123	33.2785	33.3784
GWO-HCM [26]	33.4512	33.1584	33.1853
SAGWO-HCM [24]	33.4492	33.2589	33.2784
WOA-HCM [27]	33.3425	33.3582	33.3687
CI-WOA-HCM	33.4641	33.4821	33.4798
DH-ABC (Frequency domain)	33.5125	33.5124	33.5001

The analysis on key sensitivity, UACI, and NPCR concerning the mean for the proposed and the existing image encryption techniques in frequency domain is provided in Table III. The difference in percentage among the two cipher images is obtained by 2 keys in a single image, denoted as the key sensitivity.

E. Analysis on Autocorrelation

The quality analysis on autocorrelation for proposed and conventional image encryption models in frequency domain is displayed in Table IV. The observation from the natural images revealed that the presented DH-ABC-HCM attained maximum correlation among the actual and the cipher image when it was differentiated with the state-of-the-art algorithms. The analysis on autocorrelation for the proposed and conventional image encryption models with reference to adjacent pixels in frequency domain is shown in Table V. Here, the experimentation of the horizontal is performed by analyzing the correlation among the horizontal matrixes of the image pixels. Therefore, in most cases, the presented DH-ABC-HCM algorithm presented better results.

Table 4: Analysis on autocorrelation for proposed and conventional image encryption models in frequency domain

Methods	Natural	Medical	Satellite
SAGWO-2DLCM [24]	0.0079	0.003278	0.01212
HCM [24][25]	0.013547	0.004497	0.00518
GWO-HCM [26]	0.003634	0.00733	0.000939
SAGWO-HCM [24]	0.005586	0.00564	0.007496
WOA-HCM [27]	0.0156	0.00519	0.004645
CI-WOA-HCM	0.003022	0.002832	0.000812
DH-ABC (Frequency domain)	0.004022	0.00258	0.00678

F. Evaluating the Quality of Encryption

Table 5: Analysis on autocorrelation for proposed and conventional image encryption models with reference to adjacent pixels in frequency domain

Horizontal			
Methods	Natural	Medical	Satellite
SAGWO-2DLCM [24]	0.001739	0.000112	0.003381
HCM [24][25]	0.00783	0.0019	0.01463
GWO-HCM [26]	0.005489	0.00314	0.002398
SAGWO-HCM [24]	0.01179	0.001241	0.00136
WOA-HCM [27]	0.00194	0.00224	0.00774
CI-WOA-HCM	0.001160	0.001018	0.001342
DH-ABC (Frequency domain)	0.00105	0.001008	0.00124
Vertical			
Methods	Natural	Medical	Satellite
SAGWO-2DLCM [24]	0.001375	0.00228	0.008373
HCM [24][25]	0.00152	0.00788	0.01117
GWO-HCM [26]	0.001507	0.00783	0.00731
SAGWO-HCM [24]	0.003327	0.00206	0.00867
WOA-HCM [27]	0.00892	0.00995	0.00732
CI-WOA-HCM	0.001244	0.008176	0.006792
DH-ABC (Frequency domain)	0.00115	0.00701	0.00604
Diagonal			
Methods	Natural	Medical	Satellite
SAGWO-2DLCM [24]	0.00785	0.002822	0.002594
HCM [24][25]	0.00619	0.003992	0.00228
GWO-HCM [26]	0.01642	0.01191	0.01082
SAGWO-HCM [24]	0.01436	0.00219	0.01301
WOA-HCM [27]	0.018774	0.00185	0.002464
CI-WOA-HCM	-0.00067	0.001586	0.002163
DH-ABC (Frequency domain)	-0.0007	0.00106	0.00187

The encryption quality of the presented DH-ABC-HCM in image encryption under frequency domain differentiated with the traditional techniques in terms of MSE, PSNR, Maximum deviation, irregular deviation, deviation from uniform histogram, contrast analysis, and average difference is displayed in Table VI, respectively. The outcomes revealed that the proposed DH-ABC-HCM performs better than the state-of-the-art algorithms.

G. Analysis on Noise Sensitivity

The noise sensitivity analysis on image encryption in frequency domain is done by including salt, pepper and Gaussian noise to the actual image. Initially, the image encryption is done by adding the images with these noises Table VII describes performance of the proposed DH-ABC-HCM and the conventional algorithms in terms of the histogram equalization, autocorrelation and information entropy analysis by altering the noise variance from 0.02, 0.04, 0.06, 0.08, and 0.1. The analysis

Table 6: Validating encryption quality in terms of MSE,PSNR,Maximum Deviation,Irregular Deviation,Deviation from Uniform Histogram,Contrast Analysis and Average Difference

MSE			
Methods	Natural	Medical	Satellite
SAGWO-2DLCM [24]	9277.3	14167	8813.7
HCM [24][25]	9227.6	14183	8815
GWO-HCM [26]	9207.5	14004	8819.5
SAGWO-HCM [24]	9295.4	14238	8890.9
WOA-HCM [27]	9324	14209	8947.3
CI-WOA-HCM	9324.3	14300	8950.3
DH-ABC (Frequency domain)	9357.5	14999	9700.3
PSNR			
Methods	Natural	Medical	Satellite
SAGWO-2DLCM [24]	8.299	3.0206	4.4214
HCM [24][25]	8.324	3.0127	4.4163
GWO-HCM [26]	8.2753	3.0726	4.4111
SAGWO-HCM [24]	8.2925	2.996	4.3968
WOA-HCM [27]	8.2812	3.006	4.3892
CI-WOA-HCM	8.2712	3.0005	4.3745
DH-ABC (Frequency domain)	8.2674	3.0004	4.3514
Maximum Deviation			
Methods	Natural	Medical	Satellite
SAGWO-2DLCM [24]	2573.2	5008.7	6006.9
HCM [24][25]	2622.6	5006.1	6009.7
GWO-HCM [26]	2607.9	4957.4	6010.5
SAGWO-HCM [24]	2632.5	4953.2	6019.8
WOA-HCM [27]	2620.3	5001.9	5999.8
CI-WOA-HCM	2735.2	5130.9	6080.5
DH-ABC (Frequency domain)	2737.8	5141.9	6941.5
Irregular Deviation			
Methods	Natural	Medical	Satellite
SAGWO-2DLCM [24]	4983.2	1837.6	2913.2
HCM [24][25]	5050	1884	2958.4
GWO-HCM [26]	4994.8	1930.8	2947.2
SAGWO-HCM [24]	5001.6	1858	2935.2
WOA-HCM [27]	5003.6	1892.4	2939.2
CI-WOA-HCM	5180	1940.8	2980.2
DH-ABC (Frequency domain)	5365	1978.8	2982.2
Deviation from Uniform Histogram			
Methods	Natural	Medical	Satellite
SAGWO-2DLCM [24]	0.17422	0.17578	0.17295
HCM [24][25]	0.2043	0.19512	0.19141
GWO-HCM [26]	0.19512	0.18877	0.19531
SAGWO-HCM [24]	0.19932	0.20078	0.19355
WOA-HCM [27]	0.2	0.1915	0.1998
CI-WOA-HCM	0.1658	0.17195	0.17059

DH-ABC (Frequency domain)	0.2158	0.23195	0.19999
Contrast Analysis			
Methods	Natural	Medical	Satellite
SAGWO-2DLCM [24]	523.61	521.84	533.4
HCM [24][25]	522.88	529.47	512.16
GWO-HCM [26]	530.65	518.41	520.52
SAGWO-HCM [24]	535.6	499.3	514.64
WOA-HCM [27]	520.06	533.64	520.84
CI-WOA-HCM	518.8	498.69	510.82
DH-ABC (Frequency domain)	538.8	548.69	540.82
Average Difference			
Methods	Natural	Medical	Satellite
SAGWO-2DLCM [24]	24.673	-84.604	-50.971
HCM [24][25]	25.81	-84.373	-50.657
GWO-HCM [26]	24.601	-83.284	-50.64
SAGWO-HCM [24]	24.782	-84.934	-51.837
WOA-HCM [27]	24.91	-84.281	-51.601
CI-WOA-HCM	24.598	-85.417	-51.924
DH-ABC (Frequency domain)	25.998	-82.437	-49.924

showed that the less sensitivity is obtained by the proposed algorithm over the noise image encryption.

H. Analysis on Attacks

The two attack types of the image encryption, such as the CPA and KPA, are listed in Table VIII. Here, the fail condition of the algorithms in the presence of attack is denoted by 0 and overwhelming the attacks is denoted by 1. It was observed that the presented method attained 1 in all attack types.

I. Computational Complexity

The computational complexity of the presented and the existing image encryption models in frequency domain using several image sizes is tabulated in Table IX. The proposed method achieved minimum computational time when it was compared with the existing methods.

7 Conclusion

This paper introduced an enhanced image encryption model using a novel HCM. Various steps were composed, such as frequency domain conversion, key generation, image encryption using optimized HCM, and image Decryption. The major improvement was the key generation and it was accomplished using the SHA-256 cryptographic hash algorithm in the chaotic-based image encryption. HCM was introduced by combining the PWLCM and 2DLCM to perform the image encryption. The piece-wise points of HCM were enhanced to improve the performance. The presented DH-ABC algorithm has optimized the parameters. The maximum information entropy was attained as the objective function by the optimized HCM. From the analysis, the information entropy of the developed DH-ABC-HCM for medical images is 2.8% better than SAGWO-2DLCM, 2.7% better than HCM, GWO-HCM, and WOA-HCM 2.6% better than SAGWO-HCM, and 2.64% better than CI-WOA-HCM.

Table 7: Noise sensitivity analysis of the image encryption in terms of histogram equalization, autocorrelation and information entropy in frequency domain

Methods	**Histogram Equalization**				
	Variance=0.02	Variance=0.04	Variance=0.06	Variance=0.08	Variance=0.1
SAGWO-2DLCM [24]	1405.1	1394.1	1477.2	1453.8	1387.9
HCM [24][25]	1437.9	1327.1	1353.9	1593.3	1396.7
GWO-HCM [26]	1435	1521.6	1455.6	1462.9	1427.5
SAGWO-HCM [24]	1458.4	1511.8	1400.7	1377.9	1505.4
WOA-HCM [27]	1404	1390.1	1472	1460.1	1396.3
CI-WOA-HCM	1344	1384.9	1500.9	1504	1415.6
DH-ABC (Frequency domain)	1388	1484.9	1550.9	1514	1455.6
Methods	**Autocorrelation**				
	Variance=0.02	Variance=0.04	Variance=0.06	Variance=0.08	Variance=0.1
SAGWO-2DLCM [24]	0.015335	-0.00293	-0.00044	0.004411	0.025376
HCM [24][25]	0.012874	-0.00635	-0.01256	0.016754	-0.00214
GWO-HCM [26]	-0.00554	0.001147	0.016858	0.011188	0.001687
SAGWO-HCM [24]	0.016922	0.020089	-0.01216	-0.00899	0.023887
WOA-HCM [27]	-0.01099	0.001289	-0.02554	0.005613	0.019705
CI-WOA-HCM	0.009592	0.001048	0.01322	0.002872	0.001595
DH-ABC (Frequency domain)	0.00	0.001248	0.01922	0.002972	0.001995
Methods	**Information Entropy**				
	Variance=0.02	Variance=0.04	Variance=0.06	Variance=0.08	Variance=0.1
SAGWO-2DLCM [24]	7.9566	7.9578	7.9518	7.9542	7.9581
HCM [24][25]	7.9555	7.9611	7.9591	7.9447	7.9567
GWO-HCM [26]	7.955	7.9498	7.9531	7.9545	7.9559
SAGWO-HCM [24]	7.9537	7.9509	7.9582	7.958	7.9511
WOA-HCM [27]	7.9569	7.9573	7.9529	7.9545	7.9578
CI-WOA-HCM	7.961	7.9778	7.9615	7.9611	7.9654
DH-ABC (Frequency domain)	7.991	7.9978	7.9815	7.9811	7.9854

Table 8: Analysis on attacks by proposed and existing image encryption models in frequency domain

Methods	KPA	CPA	Chosen KPA
SAGWO-2DLCM [24]	0.62044 (0)	-0.00272 (1)	0.96719 (0)
HCM [24][25]	0.86558 (0)	-0.13266 (1)	-0.88948 (1)
GWO-HCM [26]	0.25443 (0)	0.38199 (0)	-0.76242 (1)
SAGWO-HCM [24]	0.013809 (1)	-0.25801 (1)	0.42284 (0)
WOA-HCM [27]	0.34867 (0)	0.055505 (0)	0.49017 (0)
CI-WOA-HCM	-0.15084 (1)	-0.79067 (1)	-0.24214 (1)
DH-ABC (Frequency domain)	-0.1514 (1)	-0.79167 (1)	-0.24514 (1)

Table 9: Computational complexity of the proposed and conventional image encryption models

Methods	32×32 (sec)	64×64 (sec)	128×128 (sec)	256×256 (sec)	554×554 (sec)
SAGWO-2DLCM [24]	0.26569	0.70446	3.5167	15.55	89.238
HCM [24][25]	0.16443	0.76302	3.5058	15.639	88.557
GWO-HCM [26]	0.15392	0.72327	3.3346	15.494	87.346
SAGWO-HCM [24]	0.15454	0.77542	3.3137	15.324	87.932
WOA-HCM [27]	0.15113	0.72182	3.2761	15.36	88.305
CI-WOA-HCM	0.15067	0.70175	3.2677	15.259	89.155
DH-ABC (Frequency domain)	0.145	0.71	3.18	14.59	87.24

References

[1] H. Wang, J. Wang, Y. Geng, et al. Quantum Image Encryption Based on Iterative Framework of Frequency-Spatial Domain Transforms, *International Journal of Theoretical Physics*, **56**, 3029-3049 (2017).

[2] M. Guan , X. Yang , W. Hu, Chaotic image encryption algorithm using frequency-domain DNA encoding, *IET Image Processing*, **13**, 1535-1539 (2019).

[3] I. S. Abuhaiba and M. A. Mohammedhasan, Image Encryption Using Differential Evolution Approach in Frequency Domain, *Signal and Image Processing : An International Journal(SIPIJ)*, **2**, (2011).

[4] Z. Liu, Q. Li, J. Dai, X. Zhao, X. Sun, S. Liu, and M. Ashfaq Ahmad, Image encryption based on random scrambling of the amplitude and phase in the frequency domain, *Optical Engineering* , **48**, 087005(1-6) (2009).

[5] A. K. Dubey and C. K. Shukla, Chaos based Encryption and Decryption of Image and Video in Time and Frequency Domain, *IJCA Special Issue on Network Security and Cryptography*,**5**(35-39), (2011) .
[6] R.Tao, Y. Xin, Y. Wang, Double image encryption based on random phase encoding in the fractional Fourier domain, *Opt. Express*, **15**, 16067–16079 (2007).
[7] N.R. Zhou,Y.X. Wang, L.H. Gong, Novel optical image encryption scheme based on fractional Mellin transform, *Optics Communications*, **284**(13),3234-3242 (2011).
[8] Y.Wang, K. Wong, X. Liao, A new chaos-based fast image encryption algorithm, *Applied Soft Computing*, **11**, 514-522 (2011).
[9] X.C.Zhang, Z. Zhou, Y. Niu, An image encryption method based on the Feistel network and dynamic DNA encoding, *IEEE Photonics Journal*, **10**, (2018).
[10] A. Mitra, Y V. Subba Rao, and S. R. M. Prasnna, A new image encryption approach using combinational permutation techniques, *Journal of computer Science*, **1**, 127 (2006).
[11] B. Mohammad Ali and J. Aman, Image Encryption Using Block-Based Transformation Algorithm, IAENG Int. *Journal of Computer Science*, **35**, 15-23 (2008).
[12] P. Refregier and B. Javidi, Optical image encryption based on input plane and Fourier plane random encoding, *Opt. Lett*, **20**, 767-769(1995).
[13] M. Joshi, Chandrashakher, and K. Singh, Color image encryption and decryption using fractional Fourier transform, *Opt. Commun*, **279**, 35-42 (2007).
[14] T.J. Chuang, J.C. Lin, New approach to image encryption, *J. Electronic Imaging*, **7**, 350-356 (1998).
[15] Di Xiao, X.F. Liao, An analysis and improvement of a chaos based image encryption algorithm, *Chaos Solutions and Fractals*,**40**, 2191-2199 (2009).
[16] R. Haddadi, E. Abdelmounim, M. E. Hanine, and A. Belaguid, Discrete Wavelet Transform Based Algorithm for Recognition of QRS Complexes, *World of Computer Science and Information Technology Journal*, **4**, 127-132 (2014).
[17] I. Algredo-Badillo, C. Feregrino-Uribe, R. Cumplido, and M. Morales-Sandoval, FPGA-based implementation alternatives for the inner loop of the Secure Hash Algorithm SHA-256, *Microprocessors and Microsystems*, **37**, 750-757 (2013).
[18] Y. Wu, J. P. Noonan, G. Yang, and H. Jin, Image encryption using the two-dimensional logistic chaotic map, *Journal of Electronic Imaging*, **21**, 013014(1-15) (2012).
[19] S. Koppu, and V. M. Viswanatham, Medical image security enhancement using two dimensional chaotic mapping optimized by self-adaptive grey wolf algorithm, *Evolutionary Intelligence*, **11**, 53–71 (2018).
[20] A. Patro, and B. Acharya, An efficient colour image encryption scheme based on 1-D chaotic maps, *Journal of Information Security and Applications*, **46**,23-41 (2019).
[21] X. Zhang, L. Wang, Z. Zhou and Y. Niu, A Chaos-Based Image Encryption Technique Utilizing Hilbert Curves and H-Fractals, *IEEE Access*, **7**, 74734-74746 (2019).
[22] G Brammya, S. Praveena, N .S. Ninu Preetha, R. Ramya, B. R. Rajakumar and D. Binu, Deer Hunting Optimization Algorithm: A New Nature-Inspired Meta-heuristic Paradigm, *The Computer Journal*, (2019).
[23] M. Marsaline Beno, I. R. Valarmathi , S.M. Swamy, and B. R. Rajakumar, Threshold prediction for segmenting tumour from brain MRI scans, International Journal of Imaging Systems and Technology, **24**, 129-137 (2014).
[24] C. Y. Lin and S. Fu Chang, Generating Robust Digital Signature for Image/Video Authentication, *Multimedia and Security Workshop at ACM Multimedia*, Bristol, UK. (1998).
[25] M. Naor and A. Shamir, Visual cryptography, Advances in Cryptology- EUROCRYPT94, *Lecture Notes in Computer Science*, **950**, 1-12 (1995).
[26] C. Lu and H. and M. Liao, Structural digital signature for image authentication: an incidental distortion resistant scheme, *IEEE Transactions on Multimedia,* **5**, 161-173 (2003).
[27] Rivest, Shamir and Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, *Communications of the ACM*, **21**,120-126 (1978).

S. Saravanan is a Research Scholar in School of Computing Science and Engineering at Vellore Institute of Technology Chennai Campus, Chennai, India. He received his M.E degree in Computer Science and Engineering from Anna University, Chennai, India. His research interests Image Processing, Data mining.

M. Sivabalakrishnan working as Associate Professor in School of Computing Science and Engineering at VIT Chennai Campus since 2013. He has 20 + years of Teaching Experience. He has completed M.E. in Computer Science and Engineering from Anna University Chennai in 2004. He has completed his Ph. D in 2012. from Anna University Chennai. He has published more than 25 papers in International and National journals. His area of Interest is Image processing, Data Mining, Machine Learning.