Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 1 (2024)

MOBAA-OBCM: Multiobjective Biometric Authentication Approach and Optimized Beta Chaotic Map

[1]Rathi M, [2]Kalaiselvi R

[1]Associate Professor, Department of Computer Technology, Dr. N.G.P. Arts and Science College, Coimbatore.

[2]Assistant Professor-III, Department of Information Science and Engineering, Kumaraguru College of Technology, Coimbatore.

Abstract:- Applications for information security are increasingly using biometrics authentication. Multi-factor Authentication (MFA) is an authentication technique which needs the user to provide two or additional authentication factors to access a device which increases the security of biometrics systems. This study proposes an effective image encryption method based on Differential Evolution (DE), Optical Processing, and Optimized Beta Chaotic Map (OBCM). It is proposed to combine optical processing and OBCM by biometrics to create the Multiobjective Biometric Authentication Approach (MOBAA), which offers a more complex approach. A user password serves as the seed of a beta chaotic map, representing a knowledge factor, while an interferogram produced by an optical authentication approach serves as a possession factor. Multiobjective fitness function is used to determine the ideal beta chaotic map parameter in DE algorithm. The effectiveness of the proposed method is evaluated against recently created, other image encryption methods. On both grayscale and colour images, the proposed technique's performance has been assessed. The Number of Pixel Change Rates (NPCR), Unified Average Change Intensity (UACI), Peak Signal to Noise Ratio (PSNR), and Mean Absolute Error (MAE) results of the authentication methods are compared with those of existing methods.

Keywords*: Multi-factor authentication, Biometric authentication, chaotic maps, meta-heuristic based image encryption, and differential evolution (DE).*

1. Introduction

Biometrics is an authentication method that entails distinguishing individuals by recognizing one or more physical traits. It describes security procedures that use distinctive biological attributes, such as fingerprint, voice, face, and iris, to confirm a user's identity. This biometric information is saved by biometric authentication systems, which is used to confirm a user's identity when they access their accounts. Biometric authentication is typically more secure than other conventional authentication methods because this data is specific to each user. Biometrics also makes it feasible to pinpoint who has been authenticated and where. It is possible that someone can borrow a password or access a card which is impossible with a biometric authentication method. The use of biometric authentication has a lot of intriguing benefits, but it also has certain disadvantages.

The problem with biometric authentication is that if someone without hands, fingerprint authentication is not possible. When a change happens in life, some of the behavioral authentication techniques become ineffective. For instance, when new shoes are worn, one's gait can vary and it becomes difficult to authenticate that user. Most biometric authentication systems need more installation cost [1]. Databases that contain templates are the target of some attacks. A biometric template in a database can be replaced by a replica made by an impostor. A template can also be taken and used by an unauthorized user. In the literature, biometrics protection approaches are proposed as a way to get around these problems. These security measures can be divided into three categories: biometric cryptosystems, cancelable biometrics, and hybrid techniques [2].

Biometric cryptosystems produce credentials for cryptography applications using biometric features, swapping out password-based keys for biometric-dependent keys [3, 4]. The original feature is transformed into a protected version with specific functionality using cancelable biometric techniques. A hybrid approach is to combine two or more methods to handle the weaknesses of earlier methods. To recognize faces, palmprints, and fingerprints, hybrid approaches have been devised [5, 6]. Other frequent attacks on biometric systems concentrate on the user interface and provide fabricated biometric information, such as a spoofing attack [7]. Therefore, a solution that increases the security of biometric systems is required to address these problems.

In order to increase security, continuous protection of computer devices and preventing unauthorized access of other important services, multi-factor authentication (MFA) was later proposed [8, 14, 15]. MFA algorithms have able to give a higher level of security and behavioral traits [9]. As users were obliged to provide identification proof that is based on two or more independent variables, this step increased security. Security-related information processing has made extensive use of optical techniques.

The majority of research focuses on digital watermarking, image encryption, and data concealing [10,11]. Since optical techniques are susceptible to certain attacks that could jeopardize the security of information. Recently optical technique is introduced to address this problem [12]. In order to offer more reliable information security solutions, chaotic maps have been integrated by optical techniques [13]. According to the initial circumstances, chaotic maps are mathematical functions that behave chaotically and produce various number sequences. Information security systems frequently use algorithms based on chaos functions, specifically on the scrambling process, because of their great sensitivity to initial conditions.

Multi-objective Biometric Authentication Approach (MOBAA) strategy is proposed in order to increase the security of biometrics systems by optical processing and optimized beta chaotic map (OBCM) which is discussed in the proposed methodology section.

2. Literature Review

Nguyen et al [16] proposed a biometric authentication scheme which used multi-factor authentication by fuzzy and non-invertible conversion methods. The capacity of this approach to fight against insider attack makes it stand out when equated to earlier biometric-based authentication protocols. The server administrator is unable to fool the system by pretending to be someone else using the client's database information. Proposed system's speed is kept up by the random orthonormal project which has lesser computing complexity and higher accuracy.

Khan et al [17] proposed a user password and dynamic handwritten signatures in a two-factor authentication configuration. The proposed method retains crucial biometric data even if the user-specific password is stolen, which is a characteristic that is extremely desirable but is missing from advanced transformation techniques. The authors evaluated the framework's performance from the three datasets of signatures that are available to the public. The results show that the projected framework does not eliminate the characteristics that distinguish

between the signatures that are authentic and fake, and the results are on par with the results of the most recent benchmark tests.

Go et al [18] adopted an authentication mechanism which includes two-factor method with certificate, a smartcard and password, OTP etc. Compared to one-factor authentication, two-factor authentication calls for an additional factor. Users constantly have to carry and maintain the additional device or element; thus, loss or exposure can happen which made them to prefer single factor authentication. Fingerprinting is frequently utilized in services because it offers good recognition, inexpensive devices, and is less antagonistic to users. However, due to its immutability, fingerprint identification always employs the same fingerprint template. A problem of reusing fingerprints by a malevolent attacker result from this. In order to address the two-factor issue at hand, they proposed system that includes both a password and fingerprint. Efficiency and accessibility are increased because it does not require a separate device.

Kang et al [19] developed a user password. Because templates made up of feature and permutation vectors can be freely altered, the scheme is provided with a secure cancellation feature. The proposed method introduced the important aspects of the scheme through experimental settings and findings. Potential attacks on the proposed approach as well as ways to strengthen security were considered.

Fleischhacker et al [20] presented a Multi-Factor Authentication and Key Exchange protocol (MFAKE) which gives à la carte design of MFA, and KE protocols. The framework-based MFAKE protocols can combine any subdivision of several high-entropy private/public keys, low-entropy passwords/PINs, and biometric factors. A single session of an unauthenticated KE protocol is connected to this combination in a modular fashion using effective single-factor password, public key, and biometric authentication protocols to run in parallel and guarantee further secrecy.

Fan et al. [21] proposed a Fresnel domain in which fabrication is done first with synthetic encoded complex amplitude. Phase component is created for the low-level certification images by iterative phase information encoding and multiplexing for the high-level certification images. Next, two phase-type cypher texts situated in two separate Fresnel transform planes are iteratively used to encode the synthetically encoded complex amplitude. As a result, using the same cascaded multilayer architecture, the method comprehends various degrees of approachability to the original certification image for various authority levels.

Souza et al [22] proposed a multifactor technique as a way to improve biometric authentication systems. Optical authentication technique is operated depending on two-beam interference and chaotic maps to biometric authentication as the physical factor. In this view, the interferogram produced by an optical authentication technology serves as a possession factor, and the seed of a chaotic map symbolizes a user password, which corresponds to a knowledge factor. Numerical simulation is used to determine whether the method is practical.

Sajjad et al. [23] implemented a new hybrid technique that verifies the user's authenticity to the system and keeps track of whether they successfully navigated the biometric system as a genuine or fake user. The proposed system consists of two parts: A fingerprint has been first matched to a database of fingerprints. The fingerprint is evaluated against a convolutional neural network (CNN)-based fingerprint model after a similarity match to determine if it is a fake or not. The process is repeated for the face and palm, and after considering all the evidence, the system allows the user to log in. Proposed approach provides efficient and reliable verification by experimental findings over five benchmark datasets.

Choi et al [24] adopted Cao and Ge's approach. It is easily vulnerable to biometric identification errors, sluggish wrong password detection, off-line password attacks, user impersonation attacks, ID guessing attacks, DoS attacks, and their scheme is unable to provide session key agreement. The study then suggests a security

upgraded multi-factor biometric authentication strategy and offers a security analysis as well as a formal analysis utilizing Burrows-Abadi-Needham logic to address the flaws found in Cao and Ge's scheme. The proposed strategy can defend against a variety of potential attack types with higher computational cost, and efficiency.

3. Proposed Methodology

Multi-objective Biometric Authentication Approach (MOBAA) strategy is proposed in order to increase the security of biometrics systems by optical processing and optimized beta chaotic map (OBCM). In this view, the biometric verification serves as the knowledge element, the phase key created using the optical two-beam interference approach, and the biometric verification. The optical technique configurations are utilized as extra secret keys. The coefficients of image blocks are encrypted using pseudo-random key created using the beta chaotic map. However, to encrypt these coefficients, specific conditions must be met. To determine the best beta chaotic map parameter, a multi-objective fitness function for differential evolution is created with the requirement to store the user password and smartcard information to provide better security.

3.1 Optical interference

Two-beam interference can be used to encode an image into two phase masks $M_1 \& M_2$. So, given a non-negative image distribution $O(m,n)$, one is able to construct a complex field distribution by following equation (1),

$$O'(m,n) = \sqrt{O(m,n)}\exp\left(j2\pi\varphi(m,n)\right) \qquad (1)$$

where j is the fictitious unit and $\varphi(m,n)$is a uniform random distribution ranging from $0\ to\ 1$. $O'(m,n)$ has been introduced toward characterizing this original complex area as two phase-only masks.

$$O'(m,n) = \exp\left(jM_1\right) * h(x,y,l) + \exp\left(jM_2\right) * h(x,y,l) \qquad (2)$$

where $h(x,y,l)$is the point pulse response function, $M_1 \& M_2$: are uniform random distributions, and $*$ represents the convolution operation:

$$h(x,y,l) = \frac{\exp\left(\frac{j2\pi l}{\lambda}\right)}{jl\lambda}\exp\ \frac{j\pi}{l\lambda}\left(x^2 + y^2\right) \qquad (3)$$

using la as the separation between the input $M_1 \& M_2$: output planes and λ as the wavelength of the light that was incident [25]. By rewriting, they succeed.

$$\exp\left(jM_1\right) + \exp\left(jM_2\right) = D, \qquad (4)$$

$$D = F^{-1}\left\{\frac{F\{O'(m,n)\}}{F\{h(x,y,l\}}\right\} \qquad (5)$$

where F{} represents the Fourier transform and $F^{-1}\{\}$represents the inverse of it. Finally, the following is how we can reach $M_1 \& M_2$:

$$M_1 = \arg(D) - \arccos(abs(D)/2) \qquad (6)$$

$$M_2 = \arg(D - \exp\left(jM_1\right)) \qquad (7)$$

where $abs(D)$ yields the complex modulus and $\arg(D)$ returns the phaseangle of D. Zhang and Wang [25] proposed an algorithm for image encryption.

Beta chaotic map

The initial value x_0 of an optimised beta chaotic map corresponds to the knowledge factor, and it denoted by a numeric password. By Zahmoul et al. [26], the beta chaotic map is a recent addition to the family of chaotic maps. According to Kaur & Kumar [27], the mathematical definition of a beta chaotic map is as follows:

$$\mathcal{Y}_{n+1} = t \times \text{Beta}(\mathcal{Y}_n; \mathcal{Y}_1, \mathcal{Y}_2, u, v), \qquad (8)$$

where

Beta (y; u, v, y1, y2)

$$= \begin{cases} \left(\frac{(\mathcal{Y} - \mathcal{Y}_1)}{(\mathcal{Y}_c - \mathcal{Y}_1)}\right)^u \left(\frac{(\mathcal{Y}_2 - \mathcal{Y})}{(\mathcal{Y}_2 - \mathcal{Y}_c)}\right)^v \text{if } \mathcal{Y} \in (\mathcal{Y}_1, \mathcal{Y}_2), \text{otherwise} \\ 0 \end{cases} \qquad (9)$$

Given $u, v, \mathcal{Y}_1$ and $\mathcal{Y}_2 \in R_n, \mathcal{Y}_1 < \mathcal{Y}_2$, one has

$$\mathcal{Y}_c = \frac{(u\mathcal{Y}_2 + v\mathcal{Y}_1)}{u + v}, \qquad (10)$$

$$u = l_1 + m_1 \times b \qquad (11)$$

and

$$v = l_2 + m_2 \times b, \qquad (12)$$

where the constants l_1, m_1, l_2, and m_2 are present. The bifurcation parameter is denoted by b. The chaotic map's amplitude is controlled by t. The bifurcation parameter's fluctuation and the initial conditions have an impact on the beta chaotic map. As a result, it strengthens the security of encryption techniques against different threats.

3.2 Multiobjective fitness function

Number of Pixel Change Rates (NPCR), Entropy, and Unified Average Change Intensity values (UACI) metrics have been used in this work to compute multiobjective fitness function. It is described as follows,

$$\text{Max } f(z) = \frac{H(S)}{8} + \left(\frac{NPCR+UACI}{2}\right), \qquad (13)$$

w.r.t. $H(S) \geq t_h$ (14)

where $H(S)$ is indicated as entropy of E' . $t_h$is represented as the smallest amount needed entropy.

3.3 Differential evolution (DE) based encryption process

The beta chaotic map's initial parameters are optimised using DE. The beta chaotic map, has been introduced to encrypt and decrypt the image, and parameters of this map is optimized by DE. A population of potential solutions is how the DE algorithm's fundamental variation operates (called agents). DE algorithm operates using a population of potential solutions as its fundamental variant. If an agent's new position is an improvement, it is accepted and added to the population; otherwise, it is just eliminated. Initialization, mutation, crossover, and selection are the four processes that make up the basic DE algorithmic framework, as depicted in Figure 1.

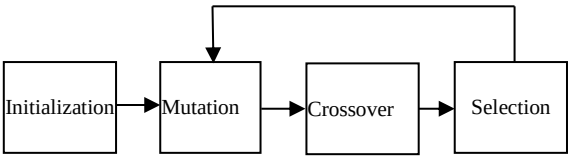


Figure 1. De Consecutive Phases

Initialization: The first step, each t^{th} individual DE solution during the t^{th} iteration has been expressed as a D-dimensional vector using equation (15),

$$X_i^t = \left(X_{i,1}, X_{i,2}, \ldots, X_{i,D}\right) \quad (15)$$

in which $i = 1, 2, \ldots, NP$. At $t = 0$, the initial population condition begins. The initial candidate solutions with lower and upper limit boundaries are able to be created by the initialization step by equations (16-17),

$$X_{min} = \left(X_{min,1}, X_{min,2}, \ldots, X_{min,D}\right) \quad (16)$$

$$X_{max} = \left(X_{max.1}, X_{max,2}, \ldots, X_{max,D}\right) \quad (17)$$

As stated in equation (18), the j^{th} dimensional component for each i^{th} DE solution be able to be initialised with arbitrarily choosing a value among the upper and lower bounds of $X_{max,j}$ and $X_{min,j}$,

$$X_{i,j}^{(0)} = X_{min.j} + rand_{i,j}[0,1]\left(X_{max,j} - X_{min,j}\right) \quad (18)$$

where the uniform distribution by $rand_{i,j} \in [0,1]$.

Mutation: Five frequently employed mutation techniques in DE are represented by their respective search mechanisms as follows:

DE/rand/1:

$$Y_i^t = X_{r_1}^t + F\left(X_{r_2}^t - X_{r_3}^t\right) \quad (19)$$

DE/rand /2:

$$Y_i^t = X_{r_1}^t + F\left(X_{r_2}^t - X_{r_3}^t\right) + F\left(X_{r_4}^t - X_{r_5}^t\right) \quad (20)$$

DE/best/ 1:

$$Y_i^t = X_{best}^t + F\left(X_{r_1}^t - X_{r_2}^t\right) \quad (21)$$

DE/best/2:

$$Y_i^t = X_{best}^t + F\left(X_{r_1}^t - X_{r_2}^t\right) + F\left(X_{r_3}^t - X_{r_4}^t\right) \quad (22)$$

DE/current-to-best/1:

$$Y_i^t = X_i^t + F\left(X_{best}^t - X_i^t\right) + F\left(X_{r_1}^t - X_{r_2}^t\right) \quad (23)$$

where $r_1, r_2, r_3, r_4, r_5 \in [1, NP]$ and $r_1 \neq r_2 \neq r_3 \neq r_4 \neq r_5 \neq i$; X^t_{best} is represented as the optimal solution found by the DE population, which is considered as the last solution, and F is denoted as the scaling factor which has been used to regulate the mutation process by the range [0,1].

Crossover: To create a trial vector, together the mutation and target vectors cross their parts at this step in a probabilistic way (offspring). Equation (24) can be used to define the uniform crossover-generated trial solution as follows:

$$Z_{\mathrm{i}}^{t} = \begin{cases} Y_{i,j}^{t} \; if \; rand_{i,j}[0,1] \leq CR \\ X_{i,j}^{t} \; Otherwise \end{cases} \quad (24)$$

Where $k \in \{1, 2, \ldots, D\}$ is a randomly certain dimension index, Z_{i}^{t} is created from $Y_{i,j}^{t}$, and $\mathrm{rand}_{\mathrm{i,j}}$ is a random number.

Selection

Determining the survival of a target (parent) solution in the following iteration (X_i^{t+1}) of the search process at the same time as preserving the population size of DE in each generation is done by the selection process is described as follows,

$$X_{\mathrm{i}}^{t+1} = \begin{cases} Z_i^t \; if \; f(Z_i^t) \leq f(X_i^t) \\ X_i^t \; Otherwise \end{cases} \quad (25)$$

where the operator f(.) is used to calculate the fitness value or objective function of a certain solution. The current target vector X_i^t will be replaced with Z_i^tin the following iteration if the most recent trial vector Z_i^t yields a superior objective function value. Asynchronous and synchronous approaches can be used to implement the DE selection process. Synchronous mode allows for simultaneous updates to the DE population, whereas asynchronous mode allows for individual updates to the DE population.

3.4 Decryption process

Using the decryption technique, the original image is able to be recovered from an encrypted image. Receiver need the proper security key (Bk) and encryption parameter (α) to decrypt the encrypted image.

3.5 User registration scheme

The user must create three keys relating to the above factors as part of the registration process. The user begins by selecting a base image$I_1(m,n)$ from a database or a personal one, such as an image of their face. The system generates a support image $I_2(m,n)$ with a random amplitude distribution. According to the equation, the images $I_1(m,n)$and $I_2(m,n)$ are encoded to a complex field $C(m,n)$

$$C(m,n) = I_1(m,n) + I_2(m,n) * j \quad (26)$$

The complex field $C(m,n)$is modulated by a random-phase mask $p(m,n)$as follows

$$C'(m,n) = C(m,n)p(m,n) \quad (27)$$

where $p(m,n) = exp(j2\pi\varphi(m,n))$ is the complex field, $\varphi(m,n)$ being a random distribution among 0 and 1. The complex field $C'(m,n)$ is then split to two phase-only masks, $pk(m,n)$ and $pl(m,n)$ (phaselock) (phase key). The phase key and lock will be mixed up as follows:

$$pl'(m,n) = mod(pl(m,n) + floor(a(m,n) \times 10^{14}), 256) \quad (28)$$

$$pk'(m,n) = mod(pk(m,n) + floor(b(m,n) \times 10^{14}), 256) \quad (29)$$

where $x_0$and y_0 serve as the initial value and $k_x$and $k_y$serve as the control parameters, respectively, and $a(m,n)$ and $b(m,n)$ are chaotic sequences produced by a Chebyshev map. As a result, scrambled phase lock and phase key are represented by $pl'(m,n)$and $pk'(m,n)$. The password that the user chose is represented by

the initial value x_0. Only the system designer is aware of the security information for the parameters k_x, $k_y$and y_0 .

3.6 Authentication process

Figure 2 illustrates the three steps of the authentication procedure. The biometric authentication is carried out as initial step, decoding of the scrambled phases as second and the interference method to retrieve the original base image as final.

The user enters the numeric password and inserts the security card or token, which contains the phase key.

The beginning value x_0, system information ($y_0, k_x and\ k_y$), and the password are utilised together to create the proper chaotic sequences $a(m,n)$and $b(m,n)$ required to decode the scrambled phases. The initial phases, $pl(m,n)$and $pk(m,n)$, are then retrieved as

$$pl(m,n) = mod(pl'(m,n) - floor(a(m,n) \times 10^{14}), 256) \quad (30)$$

$$pk(m,n) = mod(pk'(m,n) - floor(b(m,n) \times 10^{14}), 256) \quad (31)$$

Hash function H is used on the newly created phase key $pk(m,n)$that results in the reconstruction of the hash string S. $pk(m,n)$to increase template security, the scrambled phase key $pk'(m,n)$is replaced with the reconstructed phase key $pk(m,n)$. The complicated field C'can be modified in the third step using the unscrambled phase key and phase lock (m,n). The initial base image can then be acquired as

$$I1(m,n) = Re\{C'(m,n)p^*(m,n)\} \quad (32)$$

where the operations $Re\{\}$ indicate the real portion of a complex number and $p^*(m,n)$is the complex conjugate of the random-phase mask $p(m,n)$. The decoded base image is matched to the unique base image to total the authentication process. The Mean Square Error (MSE) metric was used in this study to measure how closely the unique actual image and the rebuilt base image match with each other.

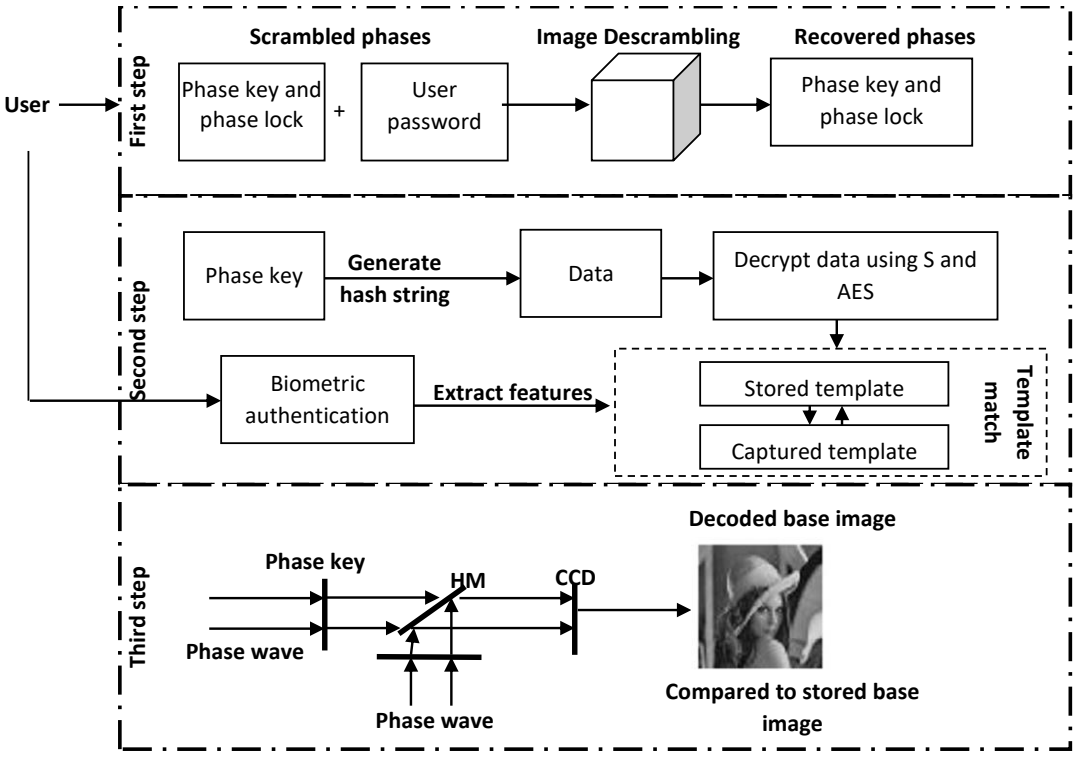


Figure 2. Multi-Factor Biometric Authentication Approach (MFBAA)

4. Experimental Results and Discussions

The effectiveness of the proposed image encryption technology is tested in this section through a number of experiments. The outcomes are contrasted with well-established meta-heuristic-based image encryption methods. Results from the simulation are produced in MATLAB2013a running on a 2.20GHz i5 processor with 8GB RAM on Windows 10. Six photos were used to test the proposed image encryption technology [28] with Grayscale images (Cameraman, Lena, and Baboon), and colour images (boat, an aeroplane, and peppers). These images measure 256 by 256 pixels. Traditional meta-heuristic-based image encryption methods including Genetic Algorithm (GA) [29], DNA [30], DHS [31], and Chaotic Map (CM) [22] are contrasted by proposed system.

4.1 Performance Measures

The effectiveness of approaches is assessed using the four well-known performance metrics PSNR, MAE, NPCR and UACI.

Peak signal to noise ratio (PSNR): PSNR is a metric for assessing the results of a decrypted image in assessment toward the original image. By definition, PSNR is [32],

$$\mathrm{PSNR} = 10\log_{10}\frac{(2^{n-1})^2}{\mathrm{MSE}} \qquad (33)$$

$$\mathrm{MSE} = \frac{1}{\mathrm{RC}} \sum_{i=1}^{i=R} \sum_{j=1}^{j=C} \left[I_{mg}(i,j) - D_{mg}(i,j) \right]^2 \quad (34)$$

Mean Square Error (MSE): MSE between I_{mg} and D_{mg} is represented by MSE. Bits per pixel are represented by the integer n. Rows and columns of an image or a graph are denoted by R *and* C. The encrypted images' PSNR should be kept to a minimum. PSNR should be increased for decrypted images.

Mean Absolute Error (MAE): The difference among input and encrypted images is measured by the MAE. As stated in [33], MAE is

$$\mathrm{MAE} = \frac{1}{\mathrm{RC}} \sum_{i=1}^{R} \sum_{j=1}^{C} \left| I_{mg}(i,j) - E_{mg}(i,j) \right| \quad (35)$$

The input and encrypted images differ significantly when MAE is at its greatest value.

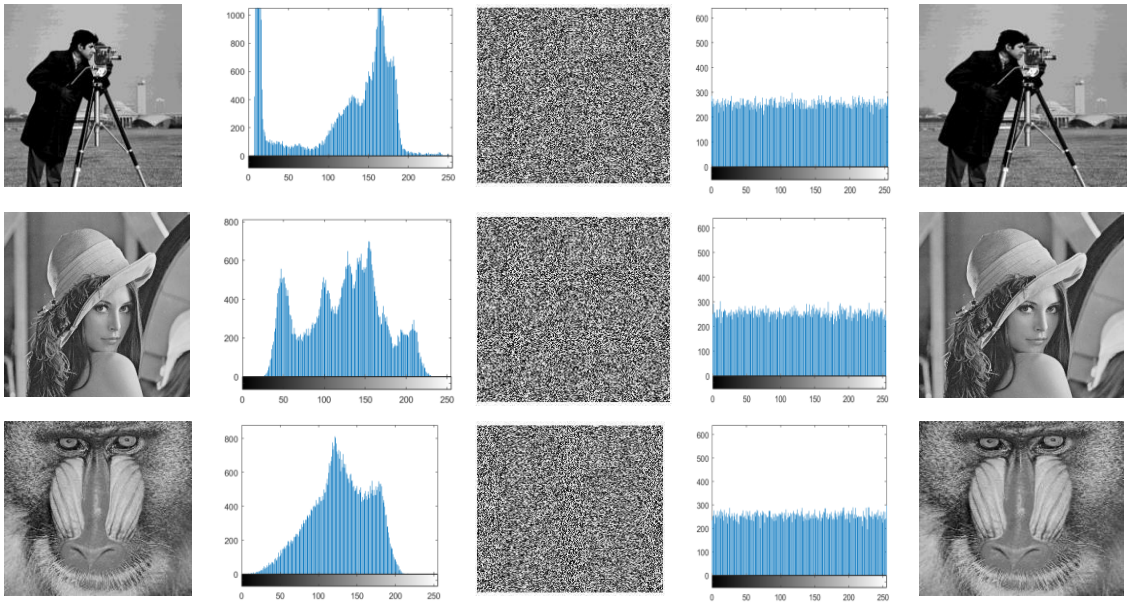
NPCR& UACI: NPCR and UACI can be calculated using the formulas [34],

$$\mathrm{UACI} = \frac{\sum_{i=1}^{i=R} \sum_{j=1}^{j=C} |E_{mg}(i,j) - E'_{mg}(i,j)|}{255 \times R \times C} \mathrm{X}\ 100 \quad (36)$$

$$D_f(i,j) = \begin{cases} 0 \text{ if } E_{mg}(i,j) = E'_{mg}(i,j), \\ 1 \text{ if } E_{mg}(i,j) \neq E'_{mg}(i,j), \end{cases} \quad (37)$$

$E_{mg}(i, j)$ and $E'_{mg}(i, j)$ are two encrypted images by a one pixel variation. The values of these metrics are UACI $\in$[0, 0.34] and NPCR $\in$[0, 1].

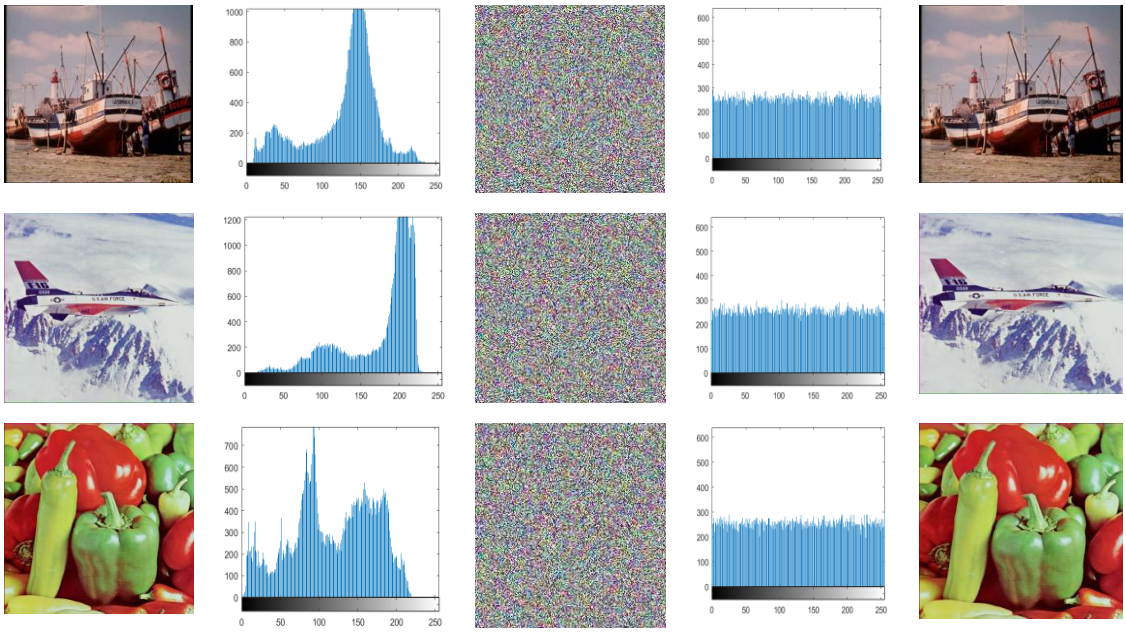
Encryption results of gray, and color images by the proposed image encryption technique, are shown in Figures 3 and 4.



(a) (b) (c) (d) (e)

Figure 3. (a) Grayscale images (b) Histogram (c) Encrypted Images

(d) Histogram of Encrypted Images (e) Decrypted Images.



(a) **(b) (c) (d)** (e)

Figure 4. (a) Colour Images (b) Histogram (c) Encrypted Images

(d) Histogram of Encrypted Images (e) Decrypted Images.

Tables 1 and 2 compare the performance of the proposed and existing image encryption algorithms using NPCR, UACI, PSNR, and MAE. The findings show that, when compared to other strategies, the proposed encryption strategy offers the highest NPCR, UACI, PSNR, and MAE.

Table 1. Metrics Analysis Using Methods for Gray Images

Image name	Metric	GA [29]	DNA [30]	DHS [31]	CM [22]	OBCM
Cameraman	**NPCR**	0.9963	0.9965	0.9969	0.9974	0.9978
	UACI	0.3343	0.3349	0.3352	0.3356	0.3363
	PSNR	66.7238	68.6428	72.9115	76.3456	88.3692
	MAE	79.3285	81.9769	82.6578	83.7643	132.5221
Lena	**NPCR**	0.9971	0.9975	0.9979	0.9981	0.9985
	UACI	0.3318	0.3327	0.3334	0.3340	0.3345
	PSNR	65.2365	66.1812	67.3104	67.9872	95.2581
	MAE	72.9875	73.2391	74.4372	75.3245	81.2532
Baboon	**NPCR**	0.9969	0.9971	0.9975	0.9979	0.9982
	UACI	0.3323	0.3331	0.3342	0.3350	0.3375
	PSNR	64.1121	65.8253	66.5814	89.6351	90.3622
	MAE	69.5769	71.7526	72.2468	73.4179	132.5212

Table 2. Metrics Analysis Using Methods for Color Images

Image name	Metric	GA [29]	DNA [30]	DHS [31]	CM [22]	OBCM
Boat	**NPCR**	0.9934	0.9945	0.9956	0.9966	0.9978
	UACI	0.3324	0.3328	0.3331	0.3343	0.3358
	PSNR	65.6211	63.9128	66.5250	83.1251	85.6251
	MAE	80.1222	82.1263	81.1801	87.1621	90.3625
Airplane	**NPCR**	0.9934	0.9945	0.9953	0.9972	0.9982
	UACI	0.3214	0.3247	0.3319	0.3338	0.3354
	PSNR	64.0139	65.1360	66.1924	89.5572	92.6321
	MAE	77.1207	78.2531	83.2354	84.9284	88.3252
Peppers	**NPCR**	0.9932	0.9943	0.9952	0.9965	0.9975
	UACI	0.3381	0.3394	0.3510	0.3366	0.3372
	PSNR	64.1423	65.1051	65.1490	89.1753	92.6571
	MAE	70.2503	79.8532	75.9725	86.9325	89.5412

The comparison of authentication methods (GA, DNA, DHS, CM, and the new OBCM algorithm) using NPCR results for colour and grayscale photos is shown in Figure 5. According to the findings, the proposed system has higher NPCR results for six photos, with values of 0.9978, 0.9985, 0.9982, 0.9978, 0.9982, and 0.9975. NPCR results of methods of GA, DNA, DHS, and CM are 0.9932, 0.9943, 0.9952, and 0.9965 using peppers image.

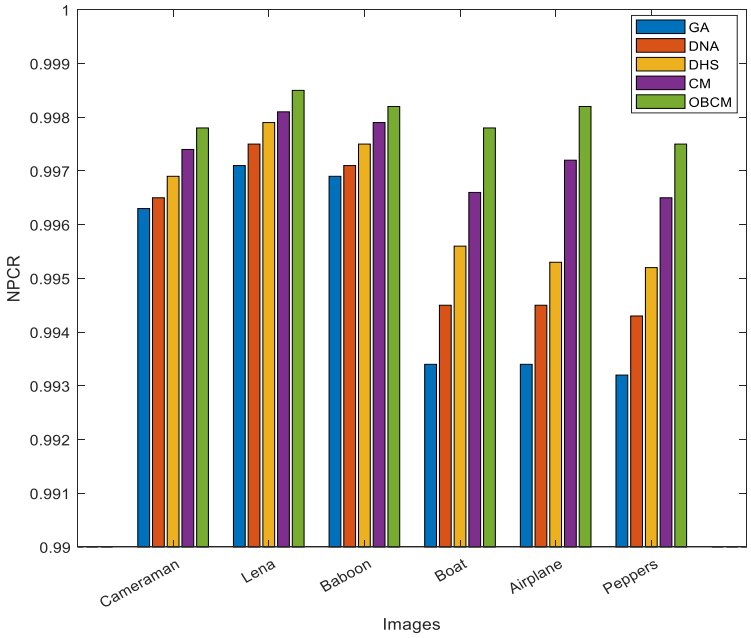


Figure 5. NPCR Results Comparison of Authentication Methods

The comparison of authentication methods (GA, DNA, DHS, CM, and the new OBCM algorithm) using UACI results for colour and grayscale photos is shown in Figure 6. According to the findings, the proposed system has higher UACI results for six photos, with values of 0.3363, 0.3345, 0.3375, 0.3358, 0.3354, and 0.3372. UACI results of methods of GA, DNA, DHS, and CM are 0.3381, 0.3394, 0.3510, and 0.3366 using peppers image.

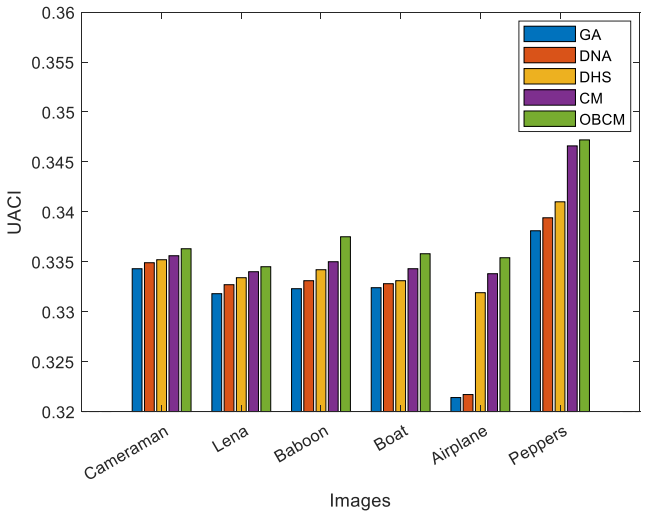


Figure 6. UACI Results Comparison of Authentication Methods

Figure 7 compares the PSNR values for various authentication techniques (GA, DNA, DHS, CM, and the proposed OBCM algorithm) using colour and grayscale photos. According to the results, the proposed system has higher PSNR results for six photos, with values of 88.3692, 95.2581, 90.3622, 85.6251, 92.6321, and 92.6571. PSNR values of methods like GA, DNA, DHS, and CM, are lower at 64.1423, 65.1051, 65.149, and 89.1753 for peppers image.

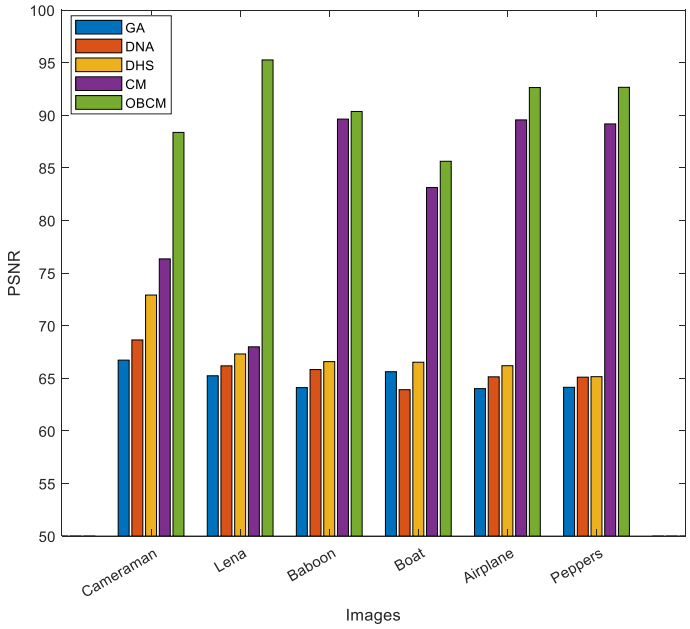


Figure 7. PSNR Results Comparison of Authentication Methods

4.2 Execution Time

Execution time (ET) is the amount of time (in seconds) required to carry out a specific image encryption method. It is the combination of the provided technique's compile (CT) and runtime (RT). ET has been assessed using the MATLAB script's "tic" and "toc" operators. The study of ET in seconds for the encryption and decryption operations is shown in Tables 3 and 4, respectively. However, image size has no impact on how long the decryption process takes to complete (See Table 4). The proposed system for the photos 1-6 executes in less time, with execution times for encryption of 6.25 seconds, 12.19 seconds, 20.43 seconds, 6.57 seconds, 16.51 seconds, and 20.47 seconds.

Table 3. Execution Time Comparison of Encryption Process

Image name	Size	GA [29]	DNA [30]	DHS [31]	CM [22]	OBCM
Cameraman	**256×256**	12.53	8.73	7.92	7.36	6.25
Lena	**512×512**	18.25	16.48	18.92	14.41	12.19
Baboon	**1024×1024**	39.55	32.61	29.15	23.55	20.43
Boat	**256×256**	22.62	11.63	10.21	8.24	6.57
Airplane	**512×512**	34.68	21.57	26.54	20.45	16.51
Peppers	**1024×1024**	44.56	40.92	32.95	24.82	20.47

Table 4. Execution Time Comparison of Decryption Process

Image name	Size	GA [29]	DNA [30]	DHS [31]	CM [22]	OBCM
Cameraman	**256×256**	0.0632	0.0312	0.0287	0.0251	0.0215
Lena	**512×512**	0.0562	0.0425	0.0365	0.0254	0.0182

Baboon	**1024×1024**	0.0512	0.0410	0.0392	0.0305	0.0261
Boat	**256×256**	0.0622	0.0515	0.0504	0.0455	0.0405
Airplane	**512×512**	0.0578	0.0663	0.0460	0.0384	0.0354
Peppers	**1024×1024**	0.0615	0.0632	0.0518	0.0415	0.0365

5. Conclusion and Future Work

In this paper, a beta chaotic map based on Differential Evolution is used in the biometric domain to encrypt images. Multiobjective fitness function is computed based on performance metrics like NPCR, UACI, PSNR, and MAE. In the proposed technique, a user first records a biometric template before registering in the system. A base image by determination is encoded by two-beam interference and a phase key is selected by the user and the AES encryption is used to encrypt biometric data. Next, based on a beta chaotic map, the user selects a password which has been used to a chaotic sequence. The proposed method can adjust the beta chaotic map's necessary parameters for secure key creation. For each input image, the beta chaotic map can provide a distinct set of secret keys. The user preserves both the password and a phase key which is stored as an interferogram in a smartcard. According to the experimental findings, the proposed technique works better than other methods in terms of NPCR, MAE, PSNR, and UACI. Future work will concentrate on refining the proposed approach with the necessity to store template information in the system database. Future development will also focus on making the system more secure so that user credentials may be updated.

References

[1] Leng L, Zhang J, “Palmhash code vs. Palmphasor code”, Neurocomputing, 108:1–12, 2013.

[2] Leng, L. and Zhang, J., “Dual-key-binding cancelable palmprint cryptosystem for palmprint protection and information security”, Journal of Network and Computer Applications, 34(6), pp.1979-1989, 2011.

[3] Li H, Zhang J, Zhang Z, “Generating cancelable palmprint templates via coupled nonlinear dynamic filters and multiple orientation palmcodes”, Inform Sci 180(20):3876–3893, 2010.

[4] Rathgeb, C. and Uhl, A., “A survey on biometric cryptosystems and cancelable biometrics”, EURASIP journal on information security, 2011(1), pp.1-25, 2011.

[5] Nagar A, Nandakumar K, Jain AK, “A hybrid biometric cryptosystem for securing fingerprint minutiae templates”, Pattern Recog Lett 31(8):733–741, 2010.

[6] Leng L, Zhang J, “Dual-key-binding cancelable palmprint cryptosystem for palmprint protection and information security”, J NetwComput Appl 34(6):1979–1989, 2011.

[7] Haupt, G. and Mozer, T., “Assessing biometric authentication: a holistic approach to accuracy”, Biometric Technology Today, 2015(3), pp.5-8, 2015.

[8] Banyal, R.K.; Jain, P.; Jain, V.K., “Multi-factor authentication framework for cloud computing”, In Proceedings of the Fifth International Conference on Computational Intelligence, Modelling and Simulation (CIMSim), Seoul, Korea, 24–25 September 2013; pp. 105–110.

[9] Frank, M.; Biedert, R.; Ma, E.; Martinovic, I.; Song, D. “Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication”, IEEE Trans. Inf. Forensics Secur., 8, 136–148, 2013.

[10] Li, J., Li, J., Pan, Y. and Li, R., “Optical image hiding with a modified Mach–Zehnder interferometer”, Optics and Lasers in Engineering, 55, pp.258-261. 2014.

[11] Wang, X., Chen, W. and Chen, X., "Optical binary image encryption using aperture-key and dual wavelengths", Optics express, 22(23), pp.28077-28085, 2014.

[12] Zhang Y, Xiao D, "Double optical image encryption using discrete chirikov standard map and chaos-based fractional random transform", Opt Lasers Eng 51(4):472–480, 2013.

[13] Chen Jx, Zhu Zl, Fu C, Zhang Lb, Yu H, "Analysis and improvement of a double-image encryption scheme using pixel scrambling technique in gyrator domains", Opt Lasers Eng 66:1–9, 2015.

[14] Nag, A.K., Roy, A. and Dasgupta, D., "An adaptive approach towards the selection of multi-factor authentication". In 2015 IEEE symposium series on computational intelligence, pp. 463-472. 2015.

[15] Fleischhacker, N., Manulis, M. and Azodi, A., "A modular framework for multi-factor authentication and key exchange", In International Conference on Research in Security Standardisation (pp. 190-214). Springer, Cham, December 2014.

[16] Nguyen TAT, Nguyen DT, Dang TK, "A multi-factor biometric based remote authentication using fuzzy commitment and non-invertible transformation", In: Information and communication technology EurAsia conference. Springer, pp.77–88, 2015.

[17] Khan SH, Akbar MA, Shahzad F, Farooq M, Khan Z , "Secure biometric template generation for multi-factor authentication", Pattern Recog 48(2):pp.458–472. 2015.

[18] Go W, Lee K, Kwak J, "Construction of a secure two-factor user authentication system using fingerprint information and password", J IntellManuf 25(2):pp.217–230, 2014.

[19] Kang J, Nyang D, Lee K, "Two-factor face authentication using matrix permutation transformation and a user password", Inform Sci 269:pp.1–20, 2014.

[20] Fleischhacker N, Manulis M, Azodi A, "A modular framework for multi-factor authentication and key exchange", In: Security standardisation research. Springer, pp.190–214, 2014.

[21] Fan D, Meng X, Wang Y, Yang X, Pan X, Peng X, He W, Dong G, Chen H, "Multiple-image authentication with a cascaded multilevel architecture based on amplitude field random sampling and phase information multiplexing", Appl Opt 54(11):pp.3204–3215, 2015.

[22] Souza, D., Burlamaqui, A. and Souza Filho, G., "Improving biometrics authentication with a multi-factor approach based on optical interference and chaotic maps", Multimedia Tools and Applications, 77(2), pp.2013-2032, 2018.

[23] Sajjad, M., Khan, S., Hussain, T., Muhammad, K., Sangaiah, A.K., Castiglione, A., Esposito, C. and Baik, S.W., "CNN-based anti-spoofing two-tier multi-factor authentication system", Pattern Recognition Letters, 126, pp.123-131, 2019.

[24] Choi, Y., Lee, Y., Moon, J. and Won, D., "Security enhanced multi-factor biometric authentication scheme using bio-hash function", PloS one, 12(5), pp.1-32, 2017.

[25] Zhang Y, Wang B, "Optical image encryption based on interference", Opt Lett 33(21):2443–2445, 2008.

[26] Zahmoul, R., Ejbali, R. &Zaied, M., "Image encryption based on new beta chaotic maps," Opt. Lasers Engin. 96, 39–49, 2017.

[27] Kaur, M. & Kumar, V., "Color image encryption technique using differential evolution in nonsubsampled contourlet transform domain," IET Imag. Process. 12, 1273–1283, 2018a.

[28] Dataset, "The USC-SIPI image database," Signal and Image Processing Institute, 2017.

[29] Abdullah, A. H., Enayatifar, R. & Lee, M., "A hybrid genetic algorithm and chaotic function model for image encryption," AEU — Int. J. Electron. Commun. 66, 806–816, 2012.

[30] Enayatifar, R., Abdullah, A. H. &Isnin, I. F.,"Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence," Opt. Lasers Engin. 56, 83–93, 2014.

[31] Talarposhti, K. M. &Jamei, M. K.,"A secure image encryption method based on dynamic harmony search (DHS) combined with chaotic map," Opt. Lasers Engin. 81, 21–34, 2016.

[32] Rawat, N., Kim, B. & Kumar, R., "Fast digital image encryption based on compressive sensing using structurally random matrices and Arnold transform technique," Optik — Int. J. Light and Electron Opt. 127, 2282–2286, 2016.

[33] Zhang, Y., Xu, B. & Zhou, N., "A novel image compression–encryption hybrid algorithm based on the analysis sparse representation," Opt. Commun. 392, 223–233, 2017.

[34] Belazi, A., El-Latif, A. A. A. &Belghith, S., "A novel image encryption scheme based on substitution permutation network and chaos," Sign. Process. 128, 155–170, 2016.