J. Vis. Commun. Image R. 74 (2021) 103002

Contents lists available at ScienceDirect

J. Vis. Commun. Image R.

journal homepage: www.elsevier.com/locate/jvci

Full Length Article

# Optimal feature selection-based biometric key management for identity management system: Emotion oriented facial biometric system ☆

Suresh Padmanabhan *, Radhika K.R.

*Department of Information Science and Engineering, BMS College of Engineering/Visveswariah Technological University, Bengaluru, India*

ARTICLE INFO

*Keywords:*
Identity management system
Facial emotions
Metaheuristic optimization

ABSTRACT

Identity management systems with biometric key binding make digital transactions secure and reliable. A novel methodology is proposed to develop an intelligent key management system using facial emotions. Key binding with facial emotions makes use of an intrinsic user specific trait facilitating a more natural computer to human interaction. The proposed system utilizes metaheuristic swarm intelligence based optimization techniques to extract optimal features. The work demonstrates key binding by encrypting an image with a secret key bound to optimal features extracted from facial emotions. Efficiency and correctness of proposed key management is validated by successful decryption at receiving end with any one of the enrolled emotions given as input. Deer Hunting Optimization Algorithm and Chicken Swarm Optimization are merged to select optimal features from facial emotions. The derived algorithm is called Fitness Sorted Deer Hunting Optimization Algorithm with Rooster Update. Seven facial emotions — anger, disgust, fear, happiness, sadness, surprise and neutral are used to extract optimal features from Japanese Female Facial Expressions and Yale Facial datasets to train the neural network. Proposed work achieved better performance results over state-of-art optimization algorithms such as whale optimization algorithm, grey wolf optimization, chicken swarm optimization and deer hunting optimization algorithm. Accuracy of proposed model is 2.2% better than deer hunting optimization algorithm and 12.3% better than chicken swarm optimization for a key length 80.

## 1. Introduction

An identity management system (IMS) ensures security and reliability of digital transactions over a network. Digital services are provided to authenticated users who have valid credentials. Authorized levels of interaction amongst users, identity provider and service providers are to be regulated. Central administration, user self-service, role based access control and integrated user management are essential requirements for identity management systems [1]. Identity management increases efficiency and security of access control while decreasing complexity, cost and repetitive tasks. Integration of biometric traits with identity management systems brings in several advantages over username/password or token based authentication systems. Researchers have evinced a lot of interest in identifying novel physiological and behavioural traits for improving efficiency and security of identity management. Multi-modal biometrics is an area of active research to achieve increased efficiency. A significant challenge faced by researchers is in making biometric credential systems reliable and reproducible without sacrificing efficiency and efficacy of detection.

Biometrics has been used in broad range of applications such as e-commerce, physical and electronic access control, background verification and digital rights management [2]. Fusion of crytpographic keys with user specific traits addresses concerns of template security [3]. User specific traits are stored in smart card and utilized for matching features taken as input during validation [4]. Smart cards enable authentication with matching score within defined threshold value and are preferred over Session Initiation Protocol (SIP) servers [5]. The servers ignore user specific traits and depend on smart card for user verification [6,7].

Conventional user name password or token based authentication systems have limitations. The major issue is that users are required to memorize usernames, passwords or maintain them securely making them susceptible to multiple attacks including dictionary attacks [8]. The solution to ensure secure storage of data involves substitution with cryptographic key [9–11]. Cryptographic models with smaller keys are easily broken while larger and complicated keys are difficult to remember. Larger keys are required to be stored securely and that

☆ This paper has been recommended for acceptance by Zicheng Liu.

* Corresponding author.
*E-mail address:* sureshpadmanb5@gmail.com (S. Padmanabhan).

https://doi.org/10.1016/j.jvcir.2020.103002
Received 3 July 2020; Received in revised form 5 December 2020; Accepted 6 December 2020
Available online 13 December 2020

in turn leads to threat vulnerability. Distribution of secret key is a challenging proposition in symmetric key cryptography [12–14].

Combination of biometrics and cryptography is a major area of research interest. Cryptographic keys are required to be precise to the last bit while user traits inherently show fuzzy nature due to intra-user variations. Biometric key release, key generation and key binding are approaches for combining cryptographic keys with user features [15]. Researchers are exploring newer traits with intelligent deep learning algorithms to perform user authentication. Keystroke dynamics and pattern of typing on mobile phones have been analysed with convolutional neural network to identify the user [16]. Deep learning techniques are employed for face recognition on mobile devices and for recognition systems based on finger veins [17,18].

The major contribution of this work is:This work aims to develop a novel biometric key management system by considering facial emotions and key binding techniques. An environment with enhanced security is built by considering both facial and key features during encryption and decryption. Facial emotion features acquired by extracting Scale Invariant Feature Transform(SIFT) features are computationally complex for machine learning. A novel metaheuristic algorithm, namely, Fitness Sorted Deer Hunting Optimization Algorithm with Rooster Update (FDHOA-RU) has been developed for selecting optimal features from SIFT keypoints. The proposed FDHOA-RU ensures selection of optimal features, thereby, providing improved fitness resulting in higher efficiency during training. FDHOA-RU algorithm has been developed by integrating properties of Deer Hunting Optimization Algorithm (DHOA) and Chicken Swarm Optimization (CSO) algorithms. The FDHOA-RU algorithm circumvents problem of premature convergence by including updates from CSO algorithm. Key extraction from an input image is carried out by Double Random Phase Encoding (DRPE), Bose–Chaudhuri–Hocquenghem (BCH) encoding, shuffling and RSA encryption. The proposed approach has made key generation more specific and reduced the probability of information stealing. Facial emotions have been considered for neural network based training during encryption and decryption process along with the key, thus providing additional support to the biometric recognition system.

The paper is structured in following manner: An overview of recognition of facial emotions and challenges in binding cryptographic keys with user traits is provided in Section 2 with state-of-the-art works in key agreement protocol. Section 3 describes proposed key management for IMS with novel key binding procedure. Key encryption process is explained in Section 4. Selection of optimal features from facial emotions and training of neural network is described in Section 5. The process of image encryption and decryption with binding of user specific key is covered in Section 6. Section 7 evaluates the approach adopted and compares results obtained with other state of art metaheuristics algorithms. Finally, conclusions are drawn in Section 8.

## 2. Literature review

### 2.1. Facial emotions

Facial emotions introduce natural aspects to conventional face recognition algorithms. Emotion feature set add additional dimension for enhanced versatility to detection accuracy [27]. Local Binary Pattern (LBP), Gabor filter, LBP with Three Orthogonal Planes, Graphics-processing based Active Shape Model (GASM) and Scale Invariant Feature Transform (SIFT) are some feature extraction methods explored to extract emotion feature set [28–30]. Research has been carried out in recent past including exploring deep learning algorithms for identifying and analysing facial expressions [31–33]. Approach adopted in current research uses optimal features extracted from facial emotions to achieve key binding.

### 2.2. Metaheuristic algorithms

Metaheuristic techniques have been researched and provide solutions to optimization problems. Given an optimization problem, there exist several ways to solve the problem. Metaheuristic algorithms solve complex problems by obtaining optimal solutions in reduced time [34]. A metaheuristic approach aims to strike balance between exploration and exploitation. Exploration identifies and narrows down search space while exploitation intensifies search in narrowed down search space. Teaching learning based optimization, particle swarm optimization, differential evolution, genetic algorithms and artificial bee colony optimization techniques are much researched metaheuristic approaches [35]. The algorithms are classified as population based and single-point search. A new variant is hybrid metaheuristic algorithms that combine techniques from different metaheuristic including exact algorithms to generate optimal solutions. Chicken Swarm Optimization [36], Deer Hunting Optimization Algorithm [37,38], Grey Wolf Optimizer [39] and Whale Optimization Algorithm [40] are some state-of-art metaheuristic techniques.

### 2.3. Key agreement protocols

Saini et al. introduced an optical security model associating key of dual random phase encoding technique with fingerprint and face biometrics of user, to make shared key user specific [19]. An encoding key with help of BCH code corrected intra-user biometric variation. A shuffling key particular to a user increased hamming distance between real and fake users. RSA encryption enhanced protection of shuffling key for improved system security. XOR operation of feature vector acquired from user traits with encoded key achieved key binding. Storage of data acquired from XOR operation along with Ravist–Shamir–Adleman (RSA) encoded shuffling key in a token ensured efficiency of implemented approach in retrieving keys utilizing user biometrics.

Panchal et al. used Reed–Solomon encoding to extract statistical characteristics from fingerprints to create codeword specific to user [20]. Support Vector Machine (SVM) based ranking verified identity of user. The work resulted in creation of single and robust biocrypto keys from fingerprint biometrics of users.

Sarkar et al. recommended a session key agreement protocol based on cancellable fingerprint for reliable and secure communication between two users [21]. The proposed protocol improved performance with elliptic curve cryptography. The suggested protocol prevented unauthorized third parties from accessing selected key of the communicating parties. Computational experiments performed on fingerprint features showed developed protocol to be privacy-preserving and well suited for different real world biometric based applications.

Wu et al. suggested an approach for generating bio-key that merged benefits of user key and biometrics verification. Robust bio-keys generated from finger veins in a convenient and flexible framework offered acceptable levels of protection for authentication in a cloud computing scenario [22]. The approach merged technologies such as biometrics, cryptography, and machine learning to get a special feature vector from biometrics space. Experimental and theoretical validation resulted in extraction of firm bio-keys from high quality finger vein images.

Nguyen et al. recommended SIP authenticated key agreement protocol for user–user, user–server and group communications [23]. A short-term token is by the end user used to communicate with other users or multimedia servers, without linking to a trusted server. Experiments revealed that proposed security mechanism opposed known attacks and produced a model with multiple characteristics including protection of biometric template privacy, user access control, long-term secret updates, smart card revocation and end-to-end communications. The verified key agreement stage achieved minimal latency with suitability for broad range of applications.

**Table 1**
Features and challenges of conventional biometrics key agreement protocols.

| Authors [Citations] | Methodology | Features | Challenges |
|---|---|---|---|
| Saini and Sinha [19] | Gabor Filter for feature extraction | - Secure transmission of key - Parallel processing of data for higher speed | - Frequency and time resolution leading to intra-user key variations |
| Panchal and Samanta [20] | - Reed–Solomon encoding for key generation<br>- SVM ranking mechanism | - Resilience to security attacks<br>- Generation of multiple bio-crypto keys | - Secrecy of encoding parameters - Sensitive to outliers |
| Sarkar and Singh [21] | -Session key agreement protocol<br>- Elliptic curve cryptography | - Privacy preserving - Suited for real-time applications | - Explore multiple user traits |
| Wu et al. [22] | High dimension space self-stabilization machine learning | - Flexible user authentication - 128–256 bit key extraction | - Feature accuracy improvement - Slower separation function |
| Nguyen and Chang [23] | SIP authenticated key agreement | - Direct end-to-end communication - Biometric template privacy | - Higher execution time - Key renewal process |
| Zhang et al. [24] | SIP authentication with ECC | - Protection of user privacy - Reduced time for setup. | - Heavy load on gateways for processing data. |
| Feng et al. [25] | ECC | - Anonymity and unlinkability<br>- User impersonation attack resilience | - Computation complexity |
| Jin et al. [26] | - ECC free key binding mechanism<br>- Fingerprint minutia vicinity decomposition and Graph-based-Hamming Embedding | - Satisfies cancellable criterion for template protection.<br>- Applicable to multiple biometric feature representations | - Accuracy and Privacy preservation |

Zhang et al. presented a secure authenticated key agreement protocol for SIP with passwords, smart cards, and biometrics [24]. The major advantages of suggested strategy were: (a) SIP server does not require to maintain a password table to manage data (b) User identity preservation (c) Privacy of user biometric information while matching biometric on SIP server. Security and performance evaluation confirmed efficiency of suggested methodology over conventional methodologies.

Feng et al. suggested biometric based authentication scheme in a multi-server architecture [25] based on Elliptic Curve Cryptosystem (ECC) and smart card. The scheme satisfied security and functional requirements in a mobile multi-server environment. The outcomes of presented approach attained enhancement in levels of security with minimal computational and communication overhead.

Jin et al. introduced an ECC-free key binding methodology with cancellable transforms for minutiae-based fingerprint biometrics [26]. The suggested approach depicted potential to be applied to different types of biometric features without being restricted to binary biometrics. FVC2002 and FVC2004 fingerprint datasets were used for experiment and results revealed strong performance in accuracy regardless of increase in size of key with robustness against security and privacy attacks.

Bhagyashri et al. proposed a scheme for encrypting an image using combination of Random phase masks and Fractional Fourier transform [41]. Iterative chaos functions have been used to generate Random phase masks. Image encryption was achieved by applying two sets of chaotic random phase mask and fractional Fourier transform. Reverse operations resulted in decrypted image. The approach tackled vulnerability to security attacks by shuffling pixel values of input image through a random sequence. Experimental results carried out with proposed algorithm showed the encrypted image to have uniform distribution of grey scale values with low correlation among adjacent pixels and high sensitivity to change in secret values of key. The model attained high value of number of pixels change rate (NPCR) and the unified average changing intensity (UACI).

### 2.4. Review

Merging of cryptographic keys with biometrics has been explored using different approaches for key binding. The reviewed state of art work reveal that fingerprint, iris and facial features have been used for key binding. Many challenges still exist for improving biometric-based key management. Table 1 describes the merits and demerits of the reviewed biometric-based key agreement protocols. Fourier Transform enhances signal to noise ratio while ensuring reduced data loss from signal during transfer [19]. The method has a disadvantage in natural concession that is present among the frequency and time resolution. SVM is efficient in high dimensional spaces and will hold any kind of data by altering the kernel [20]. Conflicts for SVM include requirement of increased time to train and sensitivity to outliers. Session key agreement protocol is suitable for real time applications with provision for privacy preservation [21]. Manifold learning requires no human intervention and is suitable for wide range of applications [22]. The challenge with manifold learning is increased time and computation resources. SIP messages are plain text which make troubleshooting easy and is a scalable open standard with ease of implementation at reduced setup time [23,24]. Hacking the registration and heavy load on gateways while processing data are potential conflicts in registering as SIP user. ECC uses lesser power, Central Processing Unit (CPU) resources and memory and is faster [25]. Graph-based Hamming Embedding (GHE) generates a cancellable fingerprint to secure geometric invariant characteristics and Minutiae Vicinity Decomposition (MVD) while reducing the hamming distance [26]. The methodology has a disadvantage of being computationally expensive. Review carried out suggests scope for improvement in biometric based key management systems.

## 3. Key management for IMS with novel key binding procedure

### 3.1. Proposed architecture

Multiple research have been carried out for binding cryptographic key with biometrics. Drawbacks of implemented methodologies of earlier studies include failure in secure transfer of encryption key and difficulty for user to store key in a secure manner. Diagrammatic representation of proposed key management is shown in Fig. 1, depicting both encryption and decryption process. The methodology introduces facial emotions based key binding system to encrypt an image with

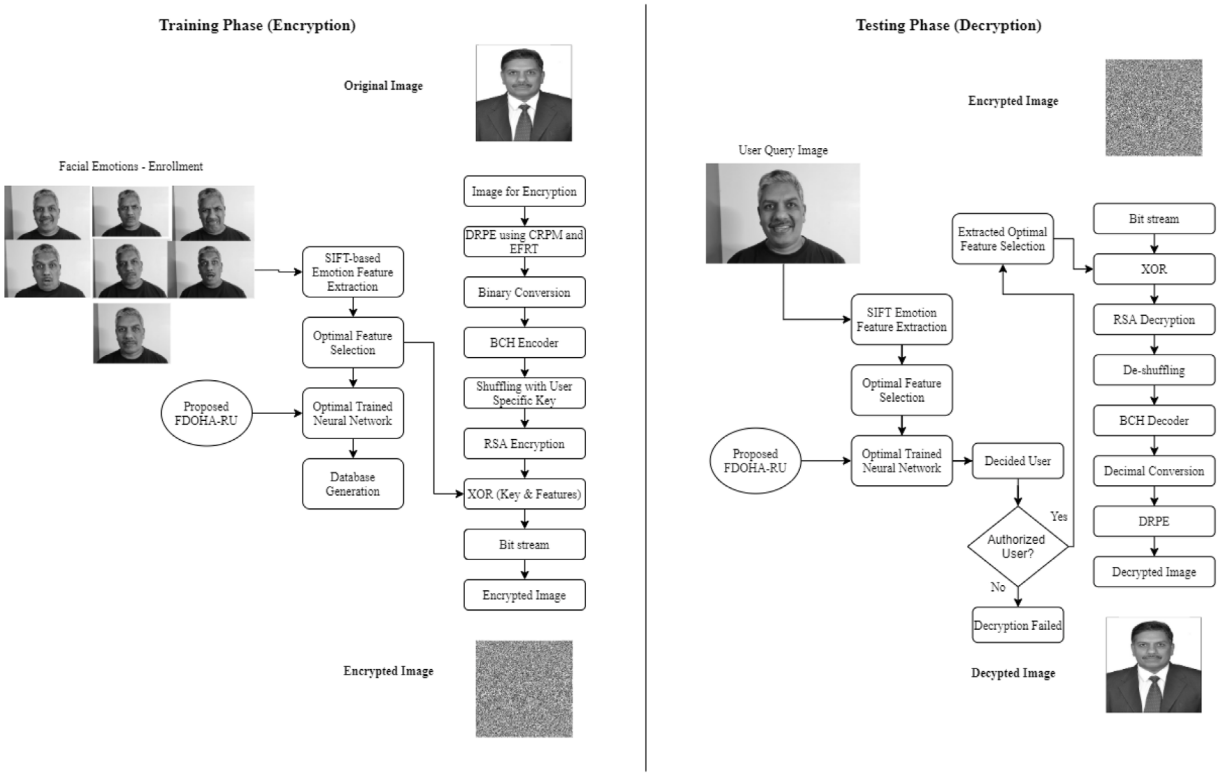



**Fig. 1.** Proposed key binding architecture.

seven different emotions including normal, smile, sad, surprise, anger, fear, and disgust.

The proposed model comprises of two phases: training and testing phase. Encryption is carried out during training phase while testing phase performs decryption. A neural network creates a database during image encryption to store extracted optimal features which is used for detection of authorized and unauthorized users during decryption. Image encryption involves subjecting input image to DRPE using Chaotic Random Phase Masks (CRPM) and Extended Fractional Fourier Transform (EFRT). DRPE is a symmetric cryptosystem that develops two random phase masks, one each at input plane and Fourier plane to convert input image into stationary white noise. The encryption key is generated from CRPM and EFRT of image. The key generated through DRPE is further subjected to binary conversion, BCH Encoding, shuffled with user specific key and finally encrypted by RSA encryption.

Keys encoded by BCH encoder are shuffled to remove overlap between genuine and imposter population. RSA encryption is used to encode shuffled key to provide additional security. Features pertaining to facial biometrics of various users are extracted using Scale Invariant Feature Transform (SIFT). The number of extracted SIFT features of each image is high and to rationalize number of features, an optimal feature selection process is adopted. Optimal features are selected by combining DHOA and CSO. The combined metaheuristics algorithm is termed as FDHOA-RU. The extracted optimal features of facial images are trained with neural network using hybrid FDHOA-RU during encryption phase. The secret key and extracted optimal features are XORed to obtain an encrypted bit stream bound to a user.

Decryption phase considers facial emotions of the authorized as input, from which optimal SIFT features are extracted using FDHOA-RU. Extracted optimal features are evaluated in FDHOA-RU neural network for categorizing authorized and unauthorized users. Decryption is carried out for only the authorized users. XOR operation is carried out between optimally selected features and encrypted bit stream. Resultant values are subjected to RSA decryption, BCH decoder, de-shuffling, and decimal conversion to decrypt the key. De-shuffling is required to be carried out by the same shuffling key that was used during encryption. DRPE is performed to decrypt the original image with various lengths of decrypted key. The process ensures efficient extraction of optimal features from facial emotions for key management.

### 3.2. Key generation process

Input image is encrypted using DRPE. The proposed model uses CRPM and EFRT for DRPE. $C^R$ is the Chaotic Random Phase Mask with which the input image represented by $IM$ is multiplied by, to obtain resultant image represented as $IM_M$ based on Eq. (1).

$$IM_M = IM \times C^R \tag{1}$$

EFRT is performed on $IM_M$. CRPM and EFRT are again applied to convert input image into stationary white noise. The mathematical equation for EFRT of input function $f(p)$ is given in Eq. (2), where coordinates of input and output plane of EFRT are given by $p$ and $q$ respectively and parameters of EFRT are $u$, $v$ and $\phi$. The input function f(p) is in the coordinate 'p' of the input plane. Eq. (2) transforms this input function from coordinate 'p' to the coordinate 'q', which is the coordinate of output plane of extended fractional Fourier Transform (EFRT).

$$f(q) = w \int f(p) \times \exp\left[ z\pi \frac{(u^2p^2 + v^2q^2)}{\tan\phi} - z2\pi \frac{uv}{\sin\phi} pq \right] dp \tag{2}$$

Parameters $u^2$, $v^2$ and $\phi$ are defined in Eq. (3), Eq. (4), and Eq. (5), respectively.

$$u^2 = \frac{1}{\lambda} \frac{\sqrt{fl - dl_2}}{\sqrt{fl - dl_1}} \frac{1}{\sqrt{\{fl^2 - (fl - dl_1)(fl - dl_2)\}}} \tag{3}$$

$$v^2 = \frac{1}{\lambda} \frac{\sqrt{fl - dl_1}}{\sqrt{fl - dl_2}} \frac{1}{\sqrt{\{fl^2 - (fl - dl_1)(fl - dl_2)\}}} \tag{4}$$

$$\phi = \arccos\left(\frac{\sqrt{fl - dl_1}\sqrt{fl - dl_2}}{fl}\right) \tag{5}$$

The parameters of EFRT are distances $dl_1$ and $dl_1$, focal length $fl$ and wavelength $\lambda$. $dl_1$ and $dl_2$ are object and image distances from the lens.

The order of EFRT and seed values of CRPM form key of developed security system. Seed values of first and second CRPM i.e., $CR_1$, and $CR_2$ and parameters of first and second EFRT i.e, $(u_1, v_1, \phi_1)$ and $(u_2, v_2, \phi_2)$ determine encryption key as given in Eq. (6).

$$EK = \left[CR_1, u_1, v_1, \phi_1, CR_2, u_2, v_2, \phi_2\right] \tag{6}$$

DRPE is tested on a 256 × 256 image to generate the encrypted image with seed values as key. The acquired binary key is encoded with help of BCH encoder and denoted as $(BCH\_EK)$. BCH key is further shuffled by a user specific shuffling key $Shuf\_EK$.

## 4. Key encryption process

### 4.1. BCH encoding and key shuffling

BCH coder encodes the encryption key. There exists a $t$-error correcting code with parameters $t < 2^{r-1}$, $s = 2^{r-1}$, $s - w \leq rt$, $t_r \geq 2t + 1$ for any positive integer $r$. The linear cyclic code has ability to correct upto $t$ random across $(2^{r-1} - 1)$ bit positions. BCH encoded key is split into blocks to perform shuffling operation. Each block of encryption key $(BCH\_EK)$ is designated by a number and the blocks are shuffled by user specific shuffling key $Shuf\_EK$. The shuffled key is indicated by $BCH\_Shuf\_EK$. Shuffling key is presented by authentic user during key retrieval process. Security of shuffled key is ensured by RSA public key encryption represented as $(RSA\_Shuf\_EK)$. The key $(RSA\_Shuf\_EK)$ is associated with user by XORing with optimal features extracted from facial emotions of user.

### 4.2. RSA encryption

RSA encrypts message $MSG$ with public key $(en, s)$. Encoded cipher text $CP$ is decrypted by secret key $(de, s)$. $en$, $de$, and $s$ are positive integers obtained from prime numbers $m$ and $n$ such that $s = m \times n$ and $\phi(s) = (m-1)(n-1)$. $m$, $n$ are secret while $s$ is public. A positive integer $1 < en < \phi(s)$ is chosen randomly such that maximum common divisor of $en$ and $\phi(s)$ is 1. $de$ is calculated as shown in Eq. (7). Mathematical equations defining RSA encryption and decryption are given in Eq. (8), and Eq. (9).

$$de = 1\{\text{mod}(\phi(s))\} \tag{7}$$

$$CP = MSG^{en} \text{ mod } (s) \tag{8}$$

$$MSG = CP^{de} \text{ mod } (s) \tag{9}$$

The encrypted key $(RSA\_Shuf\_EK)$ is merged with biometric feature for secure image encryption with key binding.

## 5. Extraction of optimal features from facial emotions and training of neural network

### 5.1. SIFT-based feature extraction from facial emotions

SIFT identifies salient and stable feature points used for proposed key management. SIFT is image scaling and rotation invariant and moderately invariant to alterations in illumination allowing for alteration in occurrence of occlusion, noise, or clutter. SIFT algorithm is classified into four phases: Scale Space Extrema Detection, Key point Localization, Orientation Assignment and Key point Descriptor. The four phases are described briefly.

(a) *Scale Space Extrema Detection:* SIFT framework identifies key points in scale space by determining image locations with maxima or minima difference-of Gaussian (DoG), $D(x, y, \sigma)$. Keypoints are maxima or minima in scale space. Location and scale of each keypoint is determined. Scale space of an image, denoted as $L(x, y, \sigma)$, is generated by convolving variable-scale Gaussian $G(x, y, \sigma)$ with input image $I_{face}(x, y)$.

$$L(x, y, \sigma) = G(x, y, \sigma) * I_{face}(x, y) \tag{10}$$

with

$$G(x, y, \sigma) = \frac{1}{2\pi\sigma^2} e^{-(x^2+y^2)/2\sigma^2} \tag{11}$$

where $\sigma$ denotes standard deviation of Gaussian $G(x, y, \sigma)$. DoG $D(x, y, \sigma)$ is computed from difference of Gaussians of two scales separated by a factor $k$:

$$D(x, y, \sigma) = (G(x, y, k\sigma) - G(x, y, \sigma)) * I_{face}(x, y) \tag{12}$$

Local maxima and minima of $D(x, y, \sigma)$ are computed by comparing the sample point with eight neighbours in same scale as well as nine neighbours in one up and down scale space.

(b) *Key point Localization:* Final set of key points are selected based on measure of stability. Points with lower contrast and poor localization are discarded as less stable points. A key point with value of $|\ D(x, y, \sigma)\ |$ lower than threshold is removed.

(c) *Orientation Assignment:* Orientations are allocated to identified key points by constructing a histogram of orientation of gradients $\theta(x, y)$ weighted by magnitude $m(x, y)$. $m$ and $\theta$ are given as:

$$m(x, y) = \sqrt{\{L(x+1, y) - L(x-1, y)\}^2 + \{L(x, y+1) - L(x, y-1)\}^2} \tag{13}$$

$$\theta(x, y) = \tan^{-1}\{[L(x, y+1) - L(x, y-1)]/[L(x+1, y) - L(x-1, y)]\} \tag{14}$$

L is Gaussian smoothed image with scale closest to a key point.

(d) *Key point Descriptor:* Descriptor vector defining gradient magnitude and orientation is calculated for each key point. Generated descriptor has three parameters — magnification factor $m$, number of spatial bins and number of orientation bins. Orientation and magnitude are computed for a region size 16 × 16. Neighbourhood is then weighted by a Gaussian window and accumulated into orientation histograms over neighbourhood 4 × 4 regions. Uniqueness of SIFT descriptors is experimented and equivalent accuracy is computed by differentiating number of key points present in testing database. SIFT features extracted from the biometric face image are represented as $\text{Fea}_{ne}^{SIFT}$, where $ne = 1, 2, \ldots \ldots\ldots, N_{fe}$. $N_{fe}$ indicates number of extracted SIFT features. Keypoint descriptors are 128 bit feature vectors. The number of SIFT features, $N_{fe}$, extracted from an image depends upon image characteristics [42].

### 5.2. Optimal feature selection

Metaheuristic techniques are adopted to identify unique reproducible features for detecting authorized users. Selection of optimal features is similar to an optimization problem wherein best solution subset is identified from a given set of solutions. Optimal feature selection in proposed biometric-based key management is achieved by FDHOA-RU, a hybrid mix of CSO and DHOA. CSO is a swarm based optimization technique while DHOA is a hunting optimization problem.

(a) *Chicken Swarm Optimization:* CSO is a nature inspired meta-heuristics algorithm for optimization, inspired by behaviour of chicken swarms comprising of roosters, hens and chicks. Chicken swarms are split into multiple clusters based on behaviour with each cluster consisting rooster $RO$, hens $HE$ and chicks $CH$. Splitting of swarm entities is done based on fitness values. Chickens with worst fitness values are denoted as $CH$, chickens with best fitness values are indicated as $RO$ and named as dominant rooster while remaining are termed as $HE$. Hens select a group on their own to live in. Mother–child relationship between hen and chick is determined and mother hens are represented as $MH$. Mother–child and dominance relationship is constant and status of each is updated for multiple time steps $ts$. Chickens follow rooster of cluster in search of food while chicks follow mother hen while searching for food.

Location of chickens at time step $ts$ is represented by $P^{ts}_{a,b}(a \in [1,\ldots,M], b \in [1,\ldots,ds])$ in dimensional space $ds$, where $M$ is number of chickens. The number, $M$, of roosters are the possible solutions. Roosters with better fitness values search for food in regions broader than roosters with worse fitness values. Better solutions, implying roosters with better fitness value, span over search space with normal distribution with higher standard deviation $\sigma^2$. Equation for movement of roosters based on respective fitness value is given in Eq. (15).

$$P^{ts+1}_{a,b} = P^{ts}_{a,b} * \left(1 + Rnd\left(0,\sigma^2\right)\right) \tag{15}$$

where, $Rnd(0,\sigma^2)$ is a Gaussian distribution function with mean zero and standard deviation $\sigma^2$ as given in Eq. (16). $c$ is index of rooster from total population $M$ and $\epsilon$ is utilized to prevent zero-division error.

$$\sigma^2 = \begin{cases} 1, & \text{if } ft_a \le ft_c \\ \exp\left(\frac{(ft_c - ft_a)}{|ft_a| + \epsilon}\right), & \text{Otherwise }, c \in [1,M], c \ne a \end{cases} \tag{16}$$

Hens with better fitness value refer to more optimal solution values and have more benefits than less fit hens, while searching for food. Hens in a group follow the rooster of group. Positional migration pattern of hens dependent on rooster of group is represented mathematically in Eq. (17).

$$P^{ts+1}_{a,b} = P^{ts}_{a,b} + A_1 * Rd * \left(P^{ts}_{rs1,b} - P^{ts}_{a,b}\right) + A_2 * Rd * \left(P^{ts}_{rs2,b} - P^{ts}_{a,b}\right) \tag{17}$$

$$A_1 = \exp\left(\frac{\left(ft_a - ft_{rs1}\right)}{\left(abs\left(ft_a\right) + \varepsilon\right)}\right) \tag{18}$$

$$A_2 = \exp\left(ft_{rs2} - ft_a\right) \tag{19}$$

$Rd$ is a random number in $[0,1]$, $rs1$ is index of rooster belonging to $a$th hen group and $rs2$ is index of rooster selected randomly from swarm such that $rs1 \ne rs2$. Evidently, $ft_a > ft_{rs1}$ and $ft_a > ft_{rs2}$, therefore $A_2 < 1 < A_1$. Chicks search their food by moving around their mother as represented in mathematical equation Eq. (20).

$$P^{ts+1}_{a,b} = P^{ts}_{a,b} + FM * \left(P^{ts}_{cm,b} - P^{ts}_{a,b}\right) \tag{20}$$

$P^{ts}_{cm,b}$ is position of $a$th chick's mother ($cm \in [1,M]$). Parameter $FM(FM \in (0,2))$ denotes the speed at which a chick follows around mother while searching food. $FM$ of every chick is chosen selected randomly in the range [0,2] to denote speed specific to motion of a chick around mother hen.

(b) *Deer Hunting Optimization Algorithm:* DHOA is a bio-inspired metaheuristics algorithm based on hunting behaviour of humans depicted while hunting a deer. Hunting mechanism is based on movement of two hunters denoted as leader and successor. Search space is an operating parameter while motion dynamics of hunters and deer along with capabilities form constraints of optimization problem. The hunting algorithm factors in dynamics of both hunter as well as prey. A hunter whose position with respect to prey is best is considered as optimal solution at step. Other hunters move towards lead hunter and update their position. If any hunter finds updated position to be better than that of leader then that particular hunter takes over as leader at end of iteration. Positional update of hunters, deer along with additional parameters like wind angle are used to formulate parametric equations. Population of hunters is initialized by Eq. (21), in which $M$ is total number of hunters and $P_a$ is overall population.

$$P_a = \left\{P_1, P_2, \ldots, P_M\right\} \quad 1 < a < M \tag{21}$$

Position and wide angle of deer are significant parameters for defining best locations of hunters. Search space is assumed as a circle and wind angle follows circumference of circle represented in Eq. (22), where $ts$ denotes current iteration, $Rd$ is a random number ranging from 0 to 1 and $\theta$ is wind angle. Position angle of deer for a wind angle $\theta$ is shown in Eq. (23).

$$\theta_{ts} = 2\pi Rd \tag{22}$$

$$\phi = \theta + \pi \tag{23}$$

Position of leader $\left(P^{le}\right)$ and successor $(P^{su})$ are considered as best two solutions. Each hunter strives to acquire best position. Encircling behaviour of hunters with respect to position of lead-hunter is given by Eq. (24), where $C$ and $D$ are coefficient vectors are determined as per Eqs. (25) and (26) respectively. A random number denoting wind speed is generated and denoted by $g$, ranging from 0 to 2. $h$ lies in the range $[-1, 1]$ and $d$ is a random number ranging from 0 to 1. $ts_{max}$ is the pre-determined number of iterations for optimization algorithm.

$$P_{ts+1} = P^{le} - C \cdot g \cdot |D \times P^{le} - P^{ts}| \tag{24}$$

$$C = \frac{1}{4}\log\left(ts + \frac{i}{ts_{\max}}\right) h \tag{25}$$

$$D = 2 \cdot d \tag{26}$$

Position angle in update rule is taken into consideration to improve search space. Computation of position angle of prey is necessary to define position of hunter. The angle of visualization of prey at iteration $ts$ is defined by Eq. (27).

$$va_{ts} = \frac{\prod}{8} \times Rd \tag{27}$$

Parameter $df_{ts}$ is calculated for updating position of deer based on difference between angles of wind and visualization, as given in Eq. (28). The position angle of prey is updated using Eq. (29).

$$dfn_{ts} = \theta_{ts} - va_{ts} \tag{28}$$

$$\phi_{ts+1} = \phi_{ts} + dfn_{ts} \tag{29}$$

The encircling behaviour is taken by altering the vector $D$ in exploration phase. Position update during exploration phase occurs based on successor rather than position of leader. The mathematical representation of update based on position of successor is given in Eq. (30). Update of position is performed in every iteration till best position is defined, based on objective function.

$$P_{ts+1} = P^{su} - C \cdot g \cdot \left|D \times P^{su} - P_{ts}\right| \tag{30}$$

(c) *Proposed FDHOA-RU:* FDHOA-RU is implemented to select optimal features from extracted SIFT features of facial emotions like normal, smile, sad, surprise, anger, fear, and disgust. Conventional DHOA is inspired by behaviour of humans exhibited while hunting deer. Proposed algorithm combines principles of swarm and hunting optimization to effect a more optimal and efficient solution. FDHOA-RU takes cue from CSO for defining fitness level for each solution in the solution space. All solutions are initially sorted as per fitness value denoted as sort index $SI$. A random number $rn$ between 1 and 7 is used to tag one of the seven selected facial emotion. Prior to starting general update of DHOA, FDHOA-RU updates solution based on length the population $l$ and fitness sort index $SI$. For the condition $l < SI$, solution is updated by the rooster update Eq. (15) of CSO. Algorithm 1 shows pseudo code of proposed FDHOA-RU for biometric-based key management for image encryption.
FDHOA-RU selects optimal features from extracted SIFT features $\mathrm{Fea}_{\mathrm{ne}}^{SIFT}$ and selected optimal features are termed as $\mathrm{Fea}_{\mathrm{ne}^*}^{\mathrm{*SIFT}}$. The selected features are used to update weight function of neural network and train the network.

**Algorithm 1** Pseudo code of proposed FDHOA-RU

**Input** Initialize population of Hunters $(P_a)$
$P_a = \{P_1, P_2, \cdots, P_M\} \quad 1 < a < M$
**Parameter Initialization:**
for each solution in population, calculate fitness function and assign motion as per CSO
Sort fitness index;

$$SI = Sort(Fitness) \tag{31}$$

Motion characteristics of hunter at step $ts$, based on fitness value is;

$$P_{a,b}^{ts+1} = P_{a,b}^{ts} * \left(1 + Rnd\left(0, \sigma^2\right)\right) \tag{32}$$

for iteration $i = 1$ to $ts_{max}$
compute:
- angle of visualization - $va$
- position update - $dfn$
- wind speed - $g$
- Coefficient vectors - $C$ and $D$
- parameter $h$

$for\ l = 1 : length(P_a)$
$If\ l < SI(1 : rn)$
**Explore with respect to Successor** $P^{su}$

$$P_{ts+1} = P^{su} - C \cdot g \cdot \left|D \times P^{su} - P_{ts}\right| \tag{33}$$

Compute fitness of each solution
Recompute best solution for hunter and identify $P^{le}$
Update position of hunters with respect to $P^{le}$

$$P_{ts+1} = P^{le} - C \cdot g \cdot \left| D \times P^{le} - P^{ts}\right| \tag{34}$$

Update $P^{le}$ and $P^{su}$

$ts = ts + 1$
return $P^{le}$

### 5.3. Template generation by neural network

The neural network trains optimal features of emotions associated with face input dataset and generated template forms basis for user authentication. Optimal features of each user extracted from test set is given as training input to neural network. The developed neural network developed is flexible and includes three layers: input, output, and hidden layers [43]. The optimally selected features by proposed FDHOA-RU termed as $Fea_{ne^*}^{*SIFT}$ is the input to neural network. Input and output neurons are denoted by $ip$ and $op$ respectively. Hidden neuron is indicated by $hd$. Outcome of the hidden layer is computed by Eq. (35).

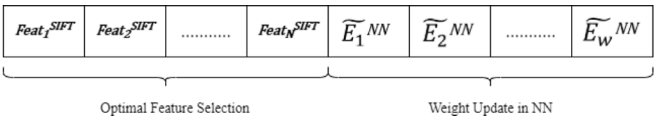



**Fig. 2.** Solution encoding for optimal feature selection and classification.

$$\tilde{B}^{(B)} = \mathrm{Acf}\left(\widetilde{E}_{(\hat{\mathrm{e}}\mathrm{hd}\ )}^{(B)} + \sum_{ip=1}^{\mathrm{Co}(IN)} \widetilde{E}_{(\mathrm{iphd}\ )}^{(B)} Fea_{ne^*}^{*SIFT}\right) \tag{35}$$

Bias weight of hidden neuron is given by $\widetilde{E}_{(\mathrm{ephd})}^{(B)}$, weight from input neuron to hidden neuron is indicated by $\widetilde{E}_{(\mathrm{iphd})}^{(B)}$, count of input neurons is defined by $\mathrm{Co}(IN)$ and activation function is shown as $Acf$. The overall outcome of the network is measured by Eq. (36). Bias weight of output neuron is given by $\widetilde{E}_{(\mathrm{eop})}^{(G)}$ and weight from hidden neuron to output neuron is denoted by $\widetilde{E}_{(\mathrm{hdop})}^{(G)}$.

$$\hat{G}_{op} = \mathrm{Acf}\left(\widetilde{E}_{(\hat{e}op)}^{(G)} + \sum_{hd=1}^{Co(OP)} \widetilde{E}_{(hdop)}^{(G)} \tilde{B}^{(B)}\right) \tag{36}$$

To provide better training to neural network, weight function

$$\widetilde{E}_l^{NN} = \left\{\widetilde{E}_{(\mathrm{ehd})}^{(B)}, \widetilde{E}_{(\mathrm{eop})}^{(G)}, \widetilde{E}_{(\mathrm{iphd})}^{(B)}, \widetilde{E}_{(\mathrm{hdop})}^{(G)}\right\}$$

is selected optimally. Corresponding measured error is given in Eq. (37).

$$EM1 = \left\{ \underset{\widetilde{E}_{(\hat{e}hd)}^{(B)}, \widetilde{E}_{(\hat{e}op)}^{(G)}, \widetilde{E}_{(iphd)}^{(B)}, \widetilde{E}_{(hdop)}^{(G)}}{\arg\min} \right\} \sum_{op=1}^{G(Co)} \left|G_{op} - \hat{G}_{op}\right| \tag{37}$$

Actual and predicted outputs are indicated as $G_{op}$ and $\hat{G}_{op}$ respectively. The error difference between the actual and predicted result given in Eq. (33) is optimized using FDHOA-RU algorithm.

## 6. Encryption and decryption of image

### 6.1. Solution encoding and objective model

The proposed FDHOA-RU algorithm is used for both feature selection as well as training of neural network. Once SIFT features $\mathrm{Fea}_{ne}^{SIFT}$ are given, optimal SIFT features $Fea_{ne^*}^{*SIFT}$ are extracted. The weight function $\widetilde{E}_l^{NN}$ of neural network is optimized by FDHOA-RU for more accurate detection of authorized user. Encoding solution for optimal feature selection and classification is shown in Fig. 2.

Optimally generated features are represented as $\mathrm{Fea}_{ne^*}^{*SIFT}$, in which $ne^* = 1, 2, \ldots, N_{*fe}$ and $N_{*}f_e$ are total number of features selected by FDHOA-RU algorithm. $\widetilde{E}_{l^*}^{NN}$ are the optimal weights. The solution element bound varies from a minimum of 1 to a maximum of number of SIFT features in an image for optimal feature selection. Total length of solution corresponding to optimal feature selection is $M_{DE} \times N_U$, where $M_{DE}$ refers to common number of features from all images and $N_U$ refers to number of users.

The main objective function considered for optimal feature selection and classification for biometric key management-based image encryption is minimization of error difference between predicted and actual as shown in Eq. (38).

$$ObFun = \mathrm{Min}(EM1) \tag{38}$$

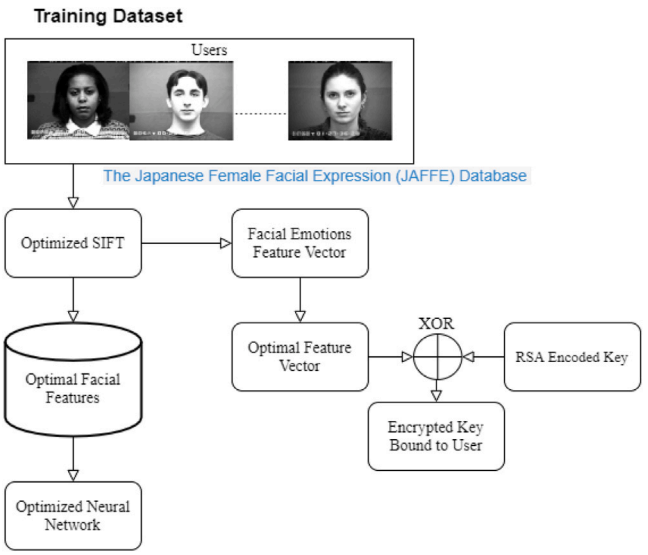



**Fig. 3.** Encryption process.

### 6.2. Encryption

The encryption process utilized to encrypt image is shown in Fig. 3. Various emotions of users are given as input and the encryption process stores the encoded key corresponding to various emotions like normal, smile, sad, surprise, anger, fear, and disgust as target on the template. Encryption of input image leads to an encoded stream of bits which form an input to decryption system.

### 6.3. Decryption

The encoded stream of bits obtained after DRPE, RSA and user key binding form input to decryption stage. The proposed decryption process detects users for various types of emotions. Fig. 4 depicts decryption process used in developed model. A user feeds facial emotions at decryption stage after which optimal features are extracted using FDHOA technique. The extracted optimal user provided for decryption are validated with neural network trained template. The user bound biometric key is XORed with input encrypted stream only after positive authentication to obtained RSA encrypted key.

## 7. Results and discussions

### 7.1. Experimental setup

The optimal feature selection-based biometric key management for IMS using facial emotions has been implemented in MATLAB 2018a installed on a PC with Windows 10 OS, 8 GB RAM and 64-bit operating system. Hardware platform for proposed work has not been implemented and has been left as future work. Facial biometric related to seven different emotions — normal, smile, sad, surprise, anger, fear, and disgust has been used. Following datasets have been used for experiments.

(a) *Japanese Female Facial Expression (JAFFE) Database:* Data has been downloaded from URL https://zenodo.org/record/3451524#.Xb_jq5ozbIU. The database contains 213 images with 7 facial expressions (6 basic facial expressions + 1 neutral) posed by 10 Japanese female models. Images are 256 × 256 grey level, in .tiff format, with no compression.

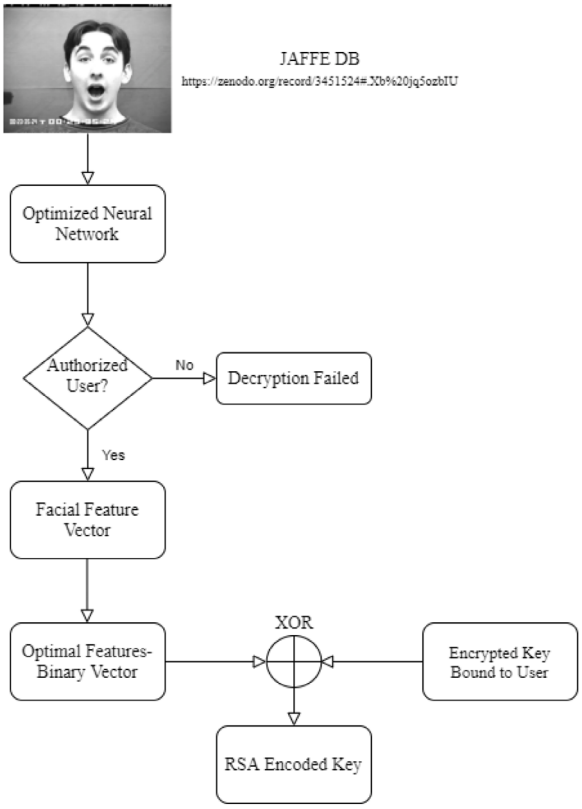



**Fig. 4.** Decryption process.

(b) *Yale Face Database:* Data has been downloaded from URL http://vision.ucsd.edu/datasets/yale_face_dataset_original/. The database contains 165 greyscale images in GIF format of 15 individuals. There are 11 images per subject, one per different facial expression.

Key lengths are varied as 36, 43, 64, 78 and 99 for performance analysis. A total of 25 iterations were performed for optimal feature selection. User detection system using FDHOA-RU was compared over models without optimization, Grey Wolf Optimization (GWO), Whale Optimization Algorithm (WOA), DHOA and CSO-based models [39,40]. Performance metrics used for evaluation include accuracy, sensitivity, specificity, and precision, False Positive Rate (FPR), False Negative Rate (FNR), Negative Predictive Value (NPV), False Discovery Rate (FDR), F1-score, and Matthews Correlation Coefficient (MCC).

### 7.2. Performance metrics

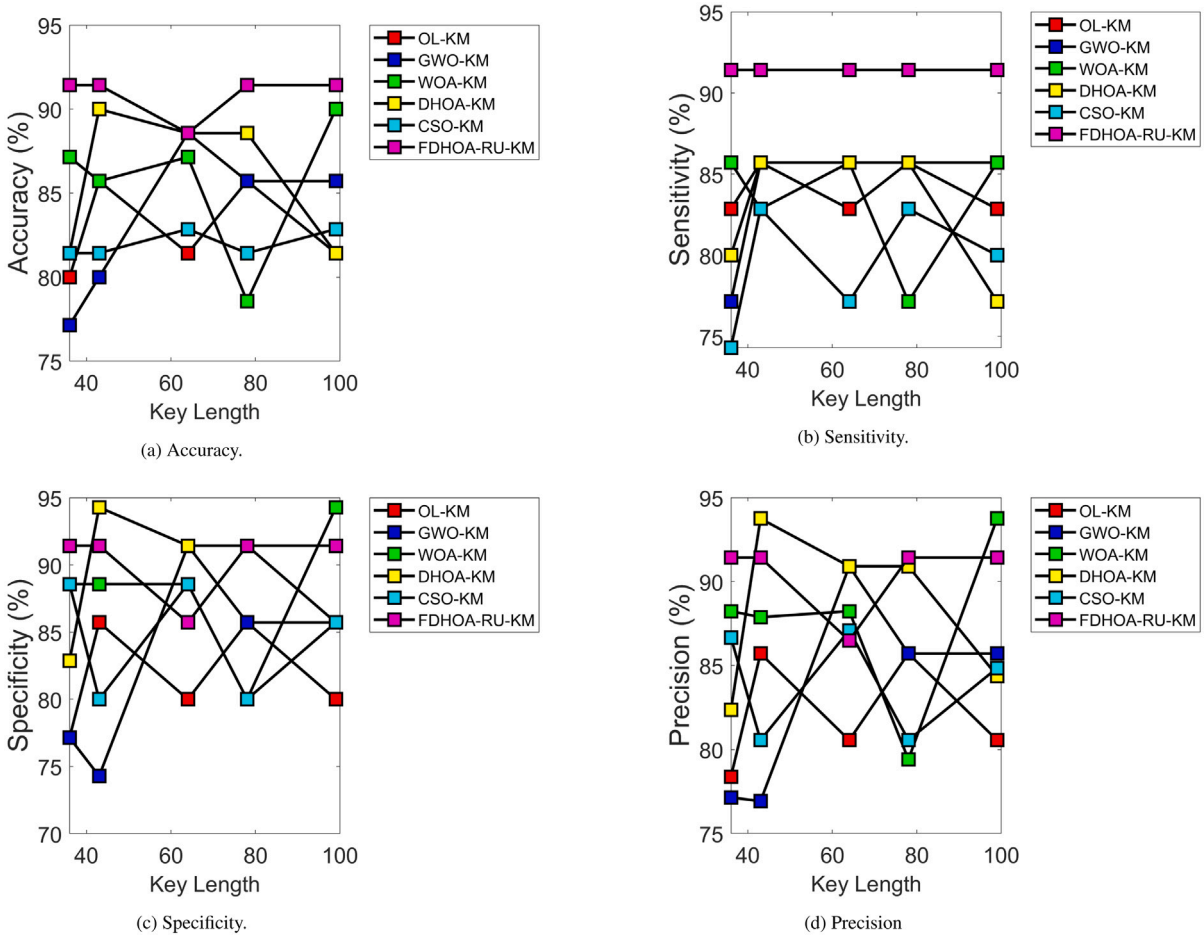
Ten performance measures are considered for image encryption using facial biometrics.

(a) *Accuracy:* Accuracy is computed as ratio of observation of exactly predicted to total observations. Expression for accuracy is shown in Eq. (39), in which Tr $P$ is true positive, Tr $N$ is true negative, $FaP$ is false positives and $FaN$ is false negatives.

$$Accuracy(Acc) = \frac{\text{Tr } P + \text{Tr } N}{\text{Tr } P + \text{Tr } N + FaP + FaN} \tag{39}$$

(b) *Sensitivity:* Measured as the number of true positives recognized. Mathematically represented in Eq. (40)

$$\text{Sen} = \frac{\text{Tr } P}{\text{Tr } P + FaN} \tag{40}$$




(a) Accuracy.

(b) Sensitivity.

(c) Specificity.

(d) Precision

**Fig. 5.** Accuracy, Sensitivity, Specificity, Precision.

(c) *Specificity:* Measured as number of true negatives determined precisely. Specificity is formulated as in Eq. (41).

$$\text{Spe} = \frac{\text{Tr}\ N}{FaP} \tag{41}$$

(d) *Precision:* Computed as ratio of true positive observations predicted to total number of observations positively predicted. It is depicted in Eq. (42).

$$\text{Pr}\ e = \frac{\text{Tr}\ P}{\text{Tr}\ P + FaP} \tag{42}$$

(e) *FPR:* Computed as ratio of count of false positive predictions to total count of negative predictions. FPR is numerically represented in Eq. (43).

$$FPR = \frac{FaP}{FaP + \text{Tr}\ N} \tag{43}$$

(f) *FNR:* Proportion of positives that yield negative test outcomes with the test. Numerically denoted in Eq. (44).

$$FNR = \frac{FaN}{FaN + TrP} \tag{44}$$

(g) *NPV:* Probability that subjects with a negative screening test are truly negative. Represented in Eq. (45)

$$NPV = \frac{FaN}{FaN + \text{Tr}\ N} \tag{45}$$

(h) *FDR:* Number of false positives in all rejected hypotheses. FDR is shown in Eq. (46).

$$FDR = \frac{FaP}{FaP + TrP} \tag{46}$$

(i) *F1 Score:* Harmonic mean between precision and sensitivity. Numerically shown in Eq. (47).

$$F1\ \text{score} = \frac{\text{Sen} \times \text{Pr}\ e}{\text{Pr}\ e + \text{Sen}} \tag{47}$$

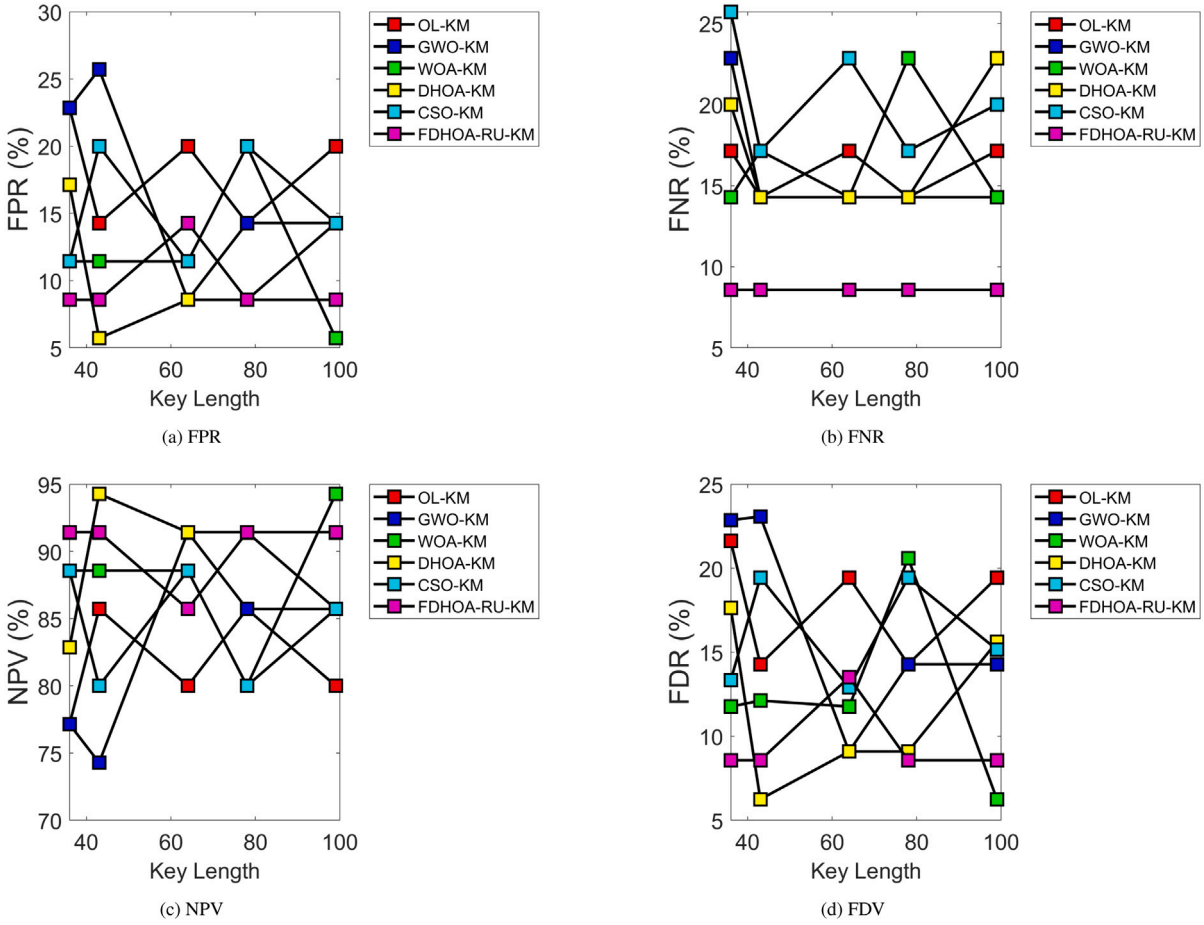
(j) *MCC:* Correlation coefficient computed as denoted in Eq. (48).

$$MCC = \frac{\text{Tr}\ P \times \text{Tr}\ N - FaP \times FaN}{\sqrt{(\text{Tr}\ P + FaP)(\text{Tr}\ P + \text{FaN})(\text{Tr}\ N + \text{FaP})(\text{Tr}\ N + \text{FaN})}} \tag{48}$$

### 7.3. Performance analysis on IMS

A detailed analysis of user detection with optimal features is carried out. Performance of proposed FDHOA-RU-KM is compared over conventional approaches based on different performance metrics for different key lengths varying from 36 to 99. The results are plotted in Fig. 5, Fig. 6, and Fig. 7. The plots shows that accuracy of the implemented FDHOA-RU-KM model is 2.2% better than DHOA, 6.4% better than GWO, 12.3% better than CSO, and 15.1% better than WOA-based KM at key length 80. Sensitivity of developed FDHOA-RU-KM is depicted. A key length of 99 implemented with FDHOA-RU-KM is 6.4% superior to WOA, 9.6% superior to OL, 13.7% superior to CSO, and 18.1% superior to DHOA-KM.

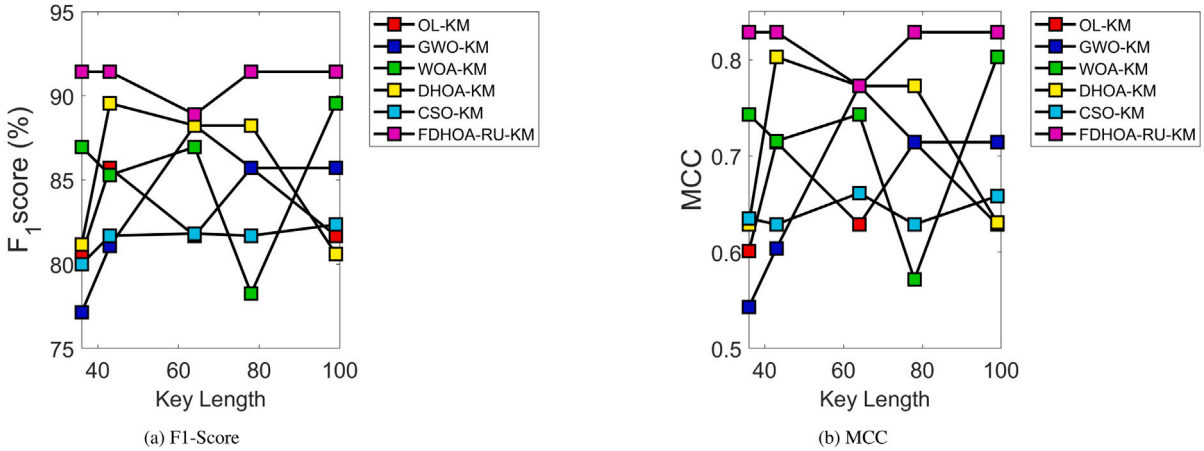
Specificity of FDHOA-RU-KM is 7% improved over GWO and 13.7% improved than CSO-KM for a key length of 80. Precision of modified FDHOA-RU-KM for a key length of 35 is 3.4%, 5.2%, 10.3%, 8.3%, and 18.1% enhanced over WOA, CSO, DHOA, OL, and GWO-KM, respectively. The plots depict that FPR of recommended FDHOA-RU-KM is




(a) FPR (b) FNR

(c) NPV (d) FDV

**Fig. 6.** FPR,FNR,NPV, FDV.




(a) F1-Score (b) MCC

**Fig. 7.** F1-Score, MCC.

39.5% better than GWO and 55% better than CSO-KM for a key length of 80. For a key length of 80, NPV for FDHOA-RU-KM is 6.4% superior to GWO, and 13.7% superior to CSO-KM. The proposed FDHOA-RU-KM is superior to conventional algorithms for all performance metrics and hence suitable for efficient employment in IMS.

### *7.4. Overall user detection*

Overall performance in user detection of proposed FDHOA-RU-KM model as against conventional models for IMS using facial emotion biometrics is tabulated in Table 2. FDHOA-RU-KM records improved performance characteristics over conventional optimization techniques in detecting users for image encryption using face biometrics.

### *7.5. ROC curve analysis*

Receiver Operating Curve (ROC) for the proposed system for a key length of 64 is plotted in Fig. 8. Each point on the ROC plot indicates a sensitivity (or) specificity pair related to specific decision threshold. The plotted figure shows that proposed FDHOA-RU-KM outperforms

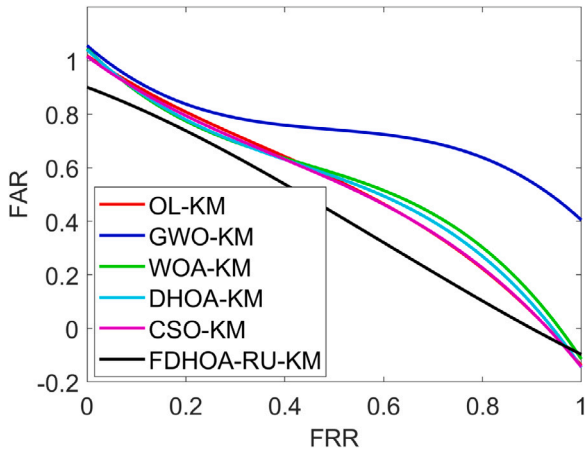



**Fig. 8.** ROC analysis of the proposed and conventional models based on FAR with respect to FRR.

**Table 2**
Overall performance of user detection in proposed biometric key management-based IMS.

| Measure | OL-KM | GWO-KM | WOA-KM | DHOA-KM | CSO-KM | FDHOA-RU-KM |
|---|---|---|---|---|---|---|
| Accuracy | 0.7142 | 0.4285 | 0.8571 | 0.9 | 0.8714 | 0.9285 |
| Sensitivity | 0.6857 | 0.8571 | 0.8571 | 0.8857 | 0.8 | 0.9428 |
| Specificity | 0.7428 | 0 | 0.8571 | 0.9142 | 0.9428 | 0.9142 |
| Precision | 0.7272 | 0.4615 | 0.8571 | 0.9117 | 0.9333 | 0.9167 |
| FPR | 0.2571 | 1 | 0.1428 | 0.0857 | 0.0571 | 0.08571 |
| FNR | 0.3142 | 0.14286 | 0.1428 | 0.1142 | 0.2 | 0.05714 |
| NPV | 0.7428 | 0 | 0.8571 | 0.9142 | 0.9428 | 0.9142 |
| FDR | 0.2727 | 0.5384 | 0.1428 | 0.0882 | 0.0667 | 0.08333 |
| F1-score | 0.7058 | 0.6 | 0.85714 | 0.8985 | 0.8615 | 0.9295 |
| MCC | 0.4292 | −0.27 | 0.7142 | 0.8003 | 0.7505 | 0.8574 |

conventional models at all FRRs. The implemented FDHOA-RU-KM is suitable for biometric key management in IMS using facial biometrics.

### 7.6. Effect of key length on ROC

Effect of key length on ROC for implemented FDHOA-RU-KM model and conventional models is shown in Fig. 9, which consists of varied key lengths. In Fig. 9(a), with key length 36, FAR by GWO-KM in terms of 0.2 FRR is minimum, followed by WOA-KM, DHOA-KM. The proposed FDHOA-RU is occupying the next position in showing the minimum result. Later, CSO and OL are having minimum value. At 0.4 FRR, FAR by developed FDHOA-RU is minimum. Next, CSO, DHOA, WOA, and GWO are occupying rest of the positions, respectively in providing the minimum values. On the basis of degree of improvement, FAR by developed FDHOA-RU with respect to 0.8 FRR is 33.3% better than CSO, 41.1% better than OL, 50% better than DHOA and WOA, and 73.6% better than GWO-KM. At key length 43, from Fig. 9(b), FAR by implemented FDHOA-RU-KM is showing minimum from 0.4 FRR. Initially, GWO is showing minimum output but finally it is exhibiting maximum FAR. By considering the FRR as 0.6, FAR by developed FDHOA-RU-KM is 2.4% enhanced than CSO, 4.7% enhanced than OL, 11.1% enhanced than WOA, 13% enhanced than DHOA, and 20% enhanced than GWO. From Fig. 9(c), for a key length of 64, FAR with presented FDHOA-RU-KM is minimum at 0 FRR. Later, the proposed model is increasing the FAR with respect to FRR. After a certain period, from 0.4 FRR, again the FAR by offered FDHOA-RU-KM is minimum. Based on the degree of improvement, FAR with improved FDHOA-RU-KM regarding 0.4 FRR is 20% improved than CSO, 23% improved than OL, 24.5% improved than DHOA, and 27.2% improved than WOA-KM. Fig. 9(d), depicts that FAR by proffered FDHOA-RU-KM is minimum at 0 FRR, later it increases slowly with respect to FRR

**Table 3**
Computation complexity.

| Feature selection (s) | | | | |
|---|---|---|---|---|
| GWO | WOA | DHOA | CSO | FDHOA-RU-KM |
| 413.41 | 419.03 | 433.50 | 461.62 | 397.16 |

| Encryption and decryption for IMS (s)) | | | | | |
|---|---|---|---|---|---|
| OL-KM | GWO-KM | WOA-KM | DHOA-KM | CSO-KM | FDHOA-RU-KM |
| 10.2474 | 6.5061 | 6.6014 | 6.5229 | 6.4602 | 6.3484 |

**Table 4**
Performance comparison over state-of-art-methods.

| Performance metrics | Panchal and Samanta [20] | Wu et al. [22] | Jin et al. [26] | Proposed FDHOA-RU-KM |
|---|---|---|---|---|
| TPR | 91.27 | 93.6 | 89 | 94.28 |
| FPR | 0.14 | 0.1502 | 0.16 | 0.08571 |

until 0.4. From 0.4 FRR, the proposed model started decreasing and providing minimum FAR. FAR by implemented FDHOA-RU KM with respect to 1 FRR is 90% better than GWO, and 97% better than OL-KM. In addition, from Fig. 10(a), FAR by modified FDHOA-RU-KM started providing minimum values from 0.4 FRR. At 0.8 FRR, FAR by improved FDHOA-RU-KM is 50% superior to WOA, 58.3% superior to OL, 75% superior to CSO, 77.2% superior to DHOA, and 80% superior to GWO-KM. It is confirmed that proposed FDHOARU-KM model outperforms conventional models in IMS using facial emotion biometrics.

### 7.7. Computational complexity

The computational complexity of feature selection in proposed facial emotion biometric-based IMS is shown in Table 3. The computational speed of the proposed FDHOA-RU-based feature selection is 3.93%, 5.21%, 8.38%, and 13.96% better than GWO, WOA, DHOA, and CSO, respectively. The computational time of encryption and decryption is given in Table 3, in which, the speed of the proposed FDHOA-RU-KM is 38.04%, 2.42%, 3.83%, 2.67%, and 1.73% superior to OL-KM, GWO-KM, WOA-KM, DHOA-KM, and CSO-KM, respectively.

### 7.8. Performance comparison over state-of-art-methods

Performance of proposed FDHOA-RU model against other state-of-art methods is tabulated in Table 4, in terms of TPR and FPR. The tabulated values show that FDHOA-RU approach has higher TPR and lower FPR values as compared to surveyed state-of-art methods. TPR and FPR give a measure of acceptance and the rejection rate respectively of the biometric system. Higher TPR and lower FPR values obtained from proposed FDHOA-RU model indicate better performance. The proposed FDHOA-RU has TPR higher than Panchal and Samanta [20] by 3.3%, Wu et al. [22] by 0.72%, Jin et al. [26] by 5.9%. The proposed scheme has lower FPR than Panchal and Samanta [20] by 38.7%, Wu et al. [22] by 42.8%, Jin et al. [26] by 46.3%.

### 7.9. Practical applications

Proposed biometric-based key management system ensures secure authentication in online transactions. The work identifies an approach to generate biometric enabled encryption and decryption across multiple sessions. The methodology enables sharing of symmetric keys across communication channels thereby enhancing security of IMS. Use of biometrics ensures security of key while additionally ensuring that authentication occurs only when authorized user is present. The emotion based facial biometric ensures ease of use and ease of integration with multitude of mobile devices used to access digital services.

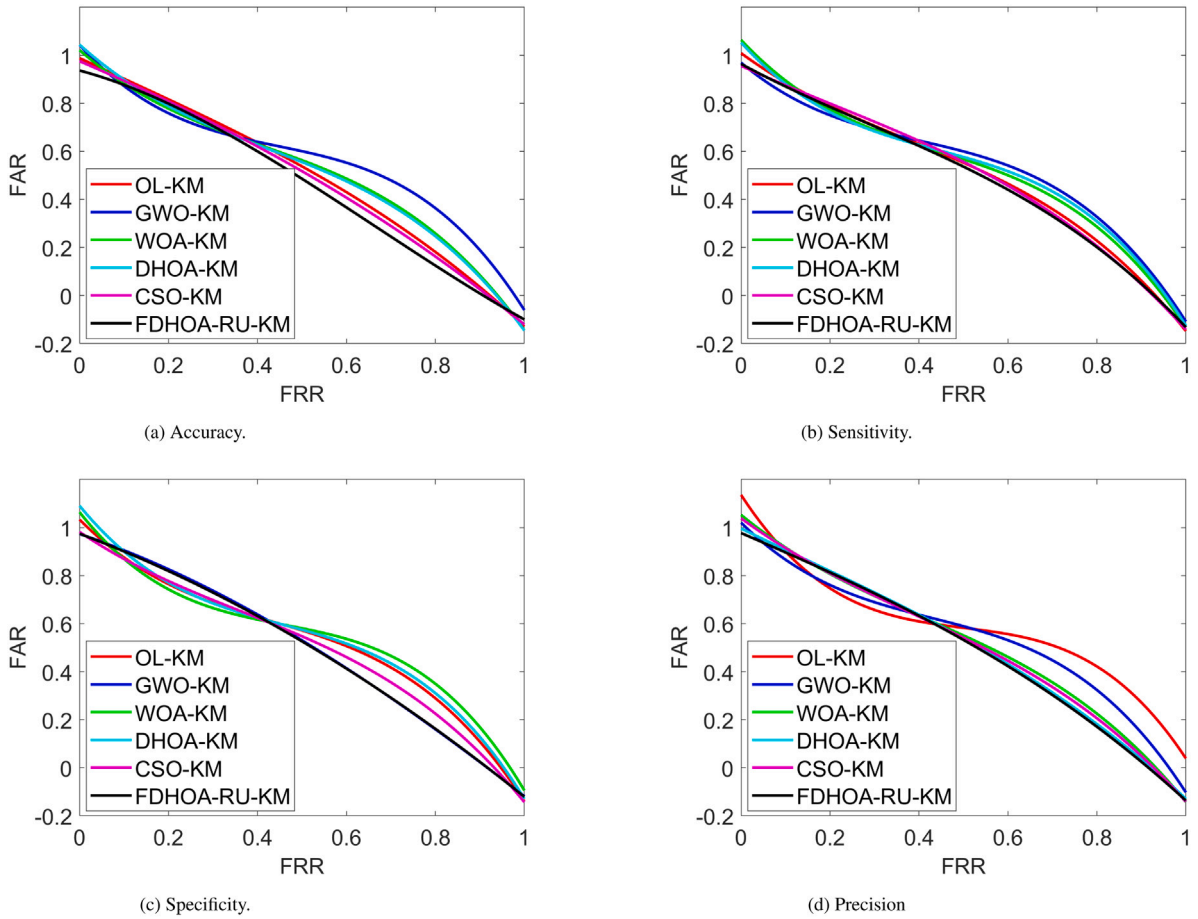



**Fig. 9.** Effect of Key Length on ROC for proposed and existing facial biometric-based key management models based on FAR with respect to FRR for varied key lengths (a) 36, (b) 43, (c) 64 and (d) 78.

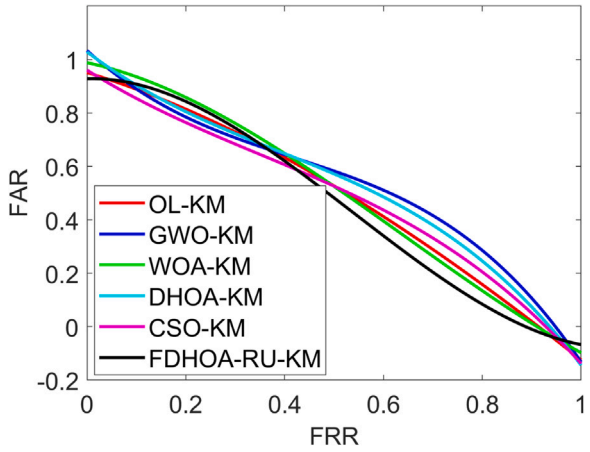



**Fig. 10.** Effect of Key Length on ROC for proposed and existing facial biometric-based key management models based on FAR with respect to FRR for varied key length 99.

## 8. Conclusion

A new IMS protocol has been demonstrated involving key extraction for encryption, feature extraction of different emotions, optimal feature selection, bit stream generation, and decryption process. The image is initially subjected to DRPE, wherein the key is created using CRPM and EFRT. Binary conversion, BCH encoding, shuffling and RSA encryption are performed on generated key, followed by extraction of features with different emotions of user facial biometric and optimal feature selection. Optimal feature selection has been achieved done by combining CSO and DHOA, thereby defining a new model named FDHOA-RU. User detection was done by an optimized neural network. Experiments and results have revealed that accuracy of implemented FDHOA-RU-KM model is 2.2% better than DHOA, 6.4% better than GWO, 12.3% better than CSO, and 15.1% better than WOA-based KM at key length 80. Precision of FDHOA-RU-KM has been found to be better than conventional algorithms. The implemented FDHOA-RU-KM methodology is found to be proficient for IMS using facial biometrics. The future scope of work would encompass further experiments with additional optimal features extracted from stable biometric traits such as iris. A multi-modal approach combining facial emotions and iris is an ideal candidate for further research.

## Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## References

[1] J. Torres, M. Nogueira, G. Pujolle, A survey on identity management for the future network, IEEE Commun. Surv. Tutor. 15 (2) (2013) 787–802, http://dx.doi.org/10.1109/SURV/2012.072412.00129, Second Quarter.

[2] S.C. Eastwood, V.P. Shmerko, S.N. Yanushkevich, M. Drahansky, D.O. Gorodnichy, Biometric-enabled authentication machines: A survey of open-set real-world applications, IEEE Trans. Hum.-Mach. Syst. 46 (2) (2016) 231–242, http://dx.doi.org/10.1109/THMS.2015.2412944.

[3] C. Li, J. Hu, A security-enhanced alignment-free fuzzy vault-based fingerprint cryptosystem using pair-polar minutiae structures, IEEE Trans. Inf. Forensics Secur. 11 (3) (2016) 543–555, http://dx.doi.org/10.1109/TIFS.2015.2505630.

[4] A.K. Jain, K. Nandakumar, Biometric authentication: System security and user privacy, Computer 45 (11) (2012) 87–92, http://dx.doi.org/10.1109/MC.2012.364.

[5] W. Sheng, S. Chen, G. Xiao, J. Mao, Y. Zheng, A biometric key generation method based on semisupervised data clustering, IEEE Trans. Syst. Man Cybern. 45 (9) (2015) 1205–1217, http://dx.doi.org/10.1109/TSMC.2015.2389768.

[6] C. Li, J. Hu, J. Pieprzyk, W. Susilo, A new biocryptosystem-oriented security analysis framework and implementation of multibiometric cryptosystems based on decision level fusion, IEEE Trans. Inf. Forensics Secur. 10 (6) (2015) 1193–1206, http://dx.doi.org/10.1109/TIFS.2015.2402593.

[7] Peng Li, Xin Yang, Kua Qiao, Kai Cao, Eryun Liu, Jie Tian, An effective biometric cryptosystem combining fingerprints with error correction codes, Expert Syst. Appl. 39 (7) (2012) 6562–6574.

[8] S. Li, A.C. Kot, Fingerprint combination for privacy protection, IEEE Trans. Inf. Forensics Secur. 8 (2) (2013) 350–360, http://dx.doi.org/10.1109/TIFS.2012.2234740.

[9] A.S. Andalib, M. Abdulla-Al-Shami, A novel key generation scheme for biometric cryptosystems using fingerprint minutiae, in: 2013 International Conference on Informatics, Electronics and Vision (ICIEV), Dhaka, 2013, pp. 1–6, http://dx.doi.org/10.1109/ICIEV.2013.6572670.

[10] A. Nagar, K. Nandakumar, A.K. Jain, Multibiometric cryptosystems based on feature-level fusion, IEEE Trans. Inf. Forensics Secur. 7 (1) (2012) 255–268, http://dx.doi.org/10.1109/TIFS.2011.2166545.

[11] T.H. Nguyen, Y. Wang, Y. Ha, R. Li, Performance and security-enhanced fuzzy vault scheme based on ridge features for distorted fingerprints, IET Biom. 4 (1) (2015) 29–39, http://dx.doi.org/10.1049/iet-bmt.2014.0026.

[12] L. Zhang, X. Yuan, K. Wang, D. Zhang, Multiple-image encryption mechanism based on ghost imaging and public key cryptography, IEEE Photonics J. 11 (4) (2019) 1–14, http://dx.doi.org/10.1109/JPHOT.2019.2923705, 7904014.

[13] G. Luan, A. Li, D. Zhang, D. Wang, Asymmetric image encryption and authentication based on equal modulus decomposition in the fresnel transform domain, IEEE Photonics J. 11 (1) (2019) 1–7, http://dx.doi.org/10.1109/JPHOT.2018.2886295, 6900207.

[14] Y. Song, Z. Zhu, W. Zhang, H. Yu, Y. Zhao, Efficient and secure image encryption algorithm using a novel key-substitution architecture, IEEE Access 7 (2019) 84386–84400, http://dx.doi.org/10.1109/ACCESS.2019.2923018.

[15] C. Rathgeb, A. Uhl, A survey on biometric cryptosystem and cancelable biometrics, EURASIP J Info. Secur. 2011 (3) (2011) http://dx.doi.org/10.1186/1687-417X-2011-3.

[16] E. Maiorana, H. Kalita, P. Campisi, Deepkey: Keystroke dynamics and CNN for biometric recognition on mobile devices, in: 2019 8th European Workshop on Visual Information Processing (EUVIP), Roma, Italy, 2019, pp. 181–186, http://dx.doi.org/10.1109/EUVIP47703.2019.8946206.

[17] B. Ríos-Sánchez, D.C. Silva, N. Martín-Yuste, C. Sánchez-Ávila, Deep learning for face recognition on mobile devices, IET Biom. 9 (3) (2020) 109–117, http://dx.doi.org/10.1049/iet-bmt.2019.0093.

[18] R.S. Kuzu, E. Piciucco, E. Maiorana, P. Campisi, On-the-fly finger-vein-based biometric recognition using deep neural networks, IEEE Trans. Inf. Forensics Secur. 15 (2020) 2641–2654, http://dx.doi.org/10.1109/TIFS.2020.2971144.

[19] Nirmala Saini, Aloka Sinha, Biometrics based key management of double random phase encoding scheme using error control codes, Opt. Lasers Eng. 51 (8) (2013) 1014–1022, http://dx.doi.org/10.1016/j.optlaseng.2013.03.006.

[20] Gaurang Panchal, Debasis Samanta, A novel approach to fingerprint biometric-based cryptographic key generation and its applications to storage security, Comput. Electr. Eng. 69 (2018) 461–478, http://dx.doi.org/10.1016/j.compeleceng.2018.01.028.

[21] A. Sarkar, B. Singh, A cancelable biometric based secure session key agreement protocol employing elliptic curve cryptography, Int. J. Syst. Assur. Eng. Manag. 10 (2019) 1023–1042, http://dx.doi.org/10.1007/s13198-019-00832-7.

[22] Zhendong Wu, Longwei Tian, Ping Li, Ting Wu, Ming Jiang, Chunming Wu, Generating stable biometric keys for flexible cloud computing authentication using finger vein, Inform. Sci. 433–434 (2018) 431–447, http://dx.doi.org/10.1016/j.ins.2016.12.048.

[23] Ngoc-Tu Nguyen, Chin-Chen Chang, A biometric-based authenticated key agreement scheme for session initiation protocol in ip-based multimedia networks, Multimedia Tools Appl. 77 (2018) 23909–23947, http://dx.doi.org/10.1007/s11042-018-5708-z.

[24] L. Zhang, S. Tang, S. Zhu, Privacy-preserving authenticated key agreement scheme based on biometrics for session initiation protocol, Wireless Netw. 23 (2017) 1901–1916, http://dx.doi.org/10.1007/s11276-016-1267-2.

[25] Qi Feng, Debiao He, Sherali Zeadally, Huaqun Wang, Anonymous biometrics-based authentication scheme with key distribution for mobile multi-server environment, Future Gener. Comput. Syst. 84 (2018) 239–251, http://dx.doi.org/10.1016/j.future.2017.07.040.

[26] Zhe Jin, Andrew Beng Jin Teah, Bok-Min Goi, Yong-Haur Tay, Biometric cryptosystems: A new biometric key binding and its implementation for fingerprint minutiae-based representation, Pattern Recognit. 56 (2016) 50–62, http://dx.doi.org/10.1016/j.patcog.2016.02.024.

[27] S. Li, W. Deng, Deep facial expression recognition: A survey, IEEE Trans. Affect. Comput. http://dx.doi.org/10.1109/TAFFC.2020.2981446.

[28] I.M. Revina, W.R. Sam Emmanuel, A survey on human face expression recognition techniques, 2018 J. King Saud Univ.-Compter Inf. Sci. https://doi.org/10.1016/j.jksuci2018.09.002.

[29] E. Sariyanidi, H. Gunes, A. Cavallaro, Automatic analysis of facial affect: A survey of registration, representation, and recognition, IEEE Trans. Pattern Anal. Mach. Intell. 37 (6) (2015) 1113–1133, http://dx.doi.org/10.1109/TPAMI.2014.2366127.

[30] M. Yuvaraju, K. Sheela, Sheela Sobana Rani, Extraction of real-time image using sift algorithm, Int. J. Res. Electr. Electron. Eng. 3, 1–7.

[31] D. Smeets, P. Claes, J. Hermans, D. Vandermeulen, P. Suetens, A comparative study of 3-D face recognition under expression variations, IEEE Trans. Syst. Man Cybern. C 42 (5) (2012) 710–727, http://dx.doi.org/10.1109/TSMCC.2011.2174221.

[32] E. Sariyanidi, H. Gunes, A. Cavallaro, Automatic analysis of facial affect: A survey of registration, representation, and recognition, IEEE Trans. Pattern Anal. Mach. Intell. 37 (6) (2015) 1113–1133, http://dx.doi.org/10.1109/TPAMI.2014.2366127.

[33] C.A. Corneanu, M.O. Simón, J.F. Cohn, S.E. Guerrero, Survey on RGB 3D thermal and multimodal approaches for facial expression recognition: History, trends, and affect-related applications, IEEE Trans. Pattern Anal. Mach. Intell. 38 (8) (2016) 1548–1568, http://dx.doi.org/10.1109/TPAMI.2016.2515606.

[34] Tansel Dokeroglu, Ender Sevinc, Tayfun Kucukyilmaz, Ahmet Cosar, A survey on new generation metaheuristic algorithms, Comput. Ind. Eng. 137 (2019) 106040, http://dx.doi.org/10.1016/j.cie.2019.106040.

[35] Ilhem Boussaid, Julien Lepagnot, Patrick Siarry, A survey on optimization metaheuristics, Inf. Sci. 237 (2013) 82–117, http://dx.doi.org/10.1016/j.ins.2013.02.041.

[36] X. Meng, Y. Liu, X. Gao, H. Zhang, A new bio-inspired algorithm: Chicken swarm optimization, in: Y. Tan, Y. Shi, C.A.C. Coello (Eds.), Advances in Swarm Intelligence, in: ICSI 2014. Lecture Notes in Computer Science, vol. 8794, Springer, Cham., 2014, http://dx.doi.org/10.1007/978-3-319-11857-4_10.

[37] G. Brammya, S. Praveena, N. Preetha, Rajakumar Ramya, D. Binu, Deer hunting optimization algorithm: A new nature-inspired meta-heuristic paradigm, Comput. J. https://doi.org/10.1093/comjnl/bxy133.

[38] Z. Zhao, X. Wang, C. Wu, L. Lei, Hunting optimization: An new framework for single objective optimization problems, IEEE Access 7 (2019) 31305–31320, http://dx.doi.org/10.1109/ACCESS.2019.2900925.

[39] Seyedali Mirjalili, Seyed Mohammad Mirjalili, Andre Lewis, Grey wolf optimizer, Adv. Eng. Softw. 69 (2014) 46–61, http://dx.doi.org/10.1016/j.advengsoft.2013.12.007.

[40] Seyedali Mirjalili, Andrew Lewis, The whale optimization algorithm, Adv. Eng. Softw. 95 (2016) 51–67, http://dx.doi.org/10.1016/j.advengsoft.2016.01.008.

[41] Bhagyashree Pandurangi, Shobha Hiremath, Meenakshi Patil, Image encryption based on chaos and fractional Fourier transform, 2020.

[42] B. Zhong, Y. Li, Image feature point matching based on improved SIFT algorithm, in: 2019 IEEE 4th International Conference on Image, Vision and Computing (ICIVC), Xiamen, China, 2019, pp. 489–493, http://dx.doi.org/10.1109/ICIVC47709.2019.8981329.

[43] F. Fernández-Navarro, M. Carbonero-Ruz, D. Becerra Alonso, M. Torres-Jiménez, Global sensitivity estimates for neural network classifiers, IEEE Trans. Neural Netw. Learn. Syst. 28 (11) (2017) 2592–2604, http://dx.doi.org/10.1109/TNNLS.2016.2598657.