Nature inspired hybrid algorithms for binding shared key with user trait

P. Suresh* and K.R. Radhika

Department of Information Science and Engineering,
BMS College of Engineering,
Visvesvaraya Technological University, India
Email: sureshpad@rediffmail.com
Email: rkr.ise@bmsce.ac.in
*Corresponding author

Abstract: Increased digital transactions accentuate the need for secure communication over open channels. Confidentiality and safe distribution of shared key is a mandatory requirement in symmetric key-based systems. The work proposes a novel nature inspired optimisation technique for binding secret key with user traits extracted from iris biometrics. Validation of key binding is demonstrated by ensuring that successful decryption happens by authorised user alone. Nature inspired swarm and population algorithms are used to extract optimal feature vectors from user trait. Chicken swarm optimisation and deer hunting optimisation algorithms have been used for the first time with iris traits to achieve optimal key binding. Experiments for different shared key lengths have been carried out with IIT Delhi and Multimedia University iris datasets. Accuracy of the proposed model is 7% better than whale optimisation algorithm and 4% better than grey wolf optimisation.

Keywords: symmetric key; iris biometric; nature inspired algorithms; neural network.

Reference to this paper should be made as follows: Suresh, P. and Radhika, K.R. (2021) ‘Nature inspired hybrid algorithms for binding shared key with user trait’, *Int. J. Applied Pattern Recognition*, Vol. 6, No. 3, pp.217–231.

Biographical notes: P. Suresh is a Research Scholar with deep interest in pattern recognition, biometrics and identity management systems. He has worked on dynamic signature, fingerprint, iris and facial emotions. He received his Bachelor of Engineering in Electronics and Communication from the College of Engineering, Guindy and Master of Technology in Computer Science and Engineering from IIT, Delhi. He is currently a PhD scholar from the VTU and has been exploring nature inspired algorithms for extracting optimal feature traits from user biometrics.

K.R. Radhika is an academician by choice, presumes in dedicated service towards teaching, research and academic activities. She has a rich experience of 24 years in teaching a wide spectrum of subjects in the areas of information technology at the BMSCE. She has about 50 publications to her credit with Google Scholar citations greater than 140. One of the noteworthy publications is in Elsevier journal, *Pattern Recognition* with an impact factor of 5.898. Other significant publications worth mentioning are in a book chapter, *Pattern Recognition, Machine Intelligence and Biometrics – Expanding Frontiers*, Springer and *Applied Soft Computing*, Elsevier with impact factor 4.873.

1 Introduction

Cryptography ensures confidentiality of messages transmitted across open communication channels. Security of messages exchanged is ensured by encrypting messages with keys. Encryption keys are symmetric or asymmetric. Shared keys score over public-private keys as they are more efficient and faster (Chandra et al., 2014; Assiri et al., 2019). Proliferation of cloud-based applications and services has increased online transactions leading to stringent demands for more secure and efficient cryptography (Yassein et al., 2017; Chen et al., 2020). Security of message and data depends on secrecy of shared key. Larger and more complex keys ensure improved security. Shared keys are most vulnerable while at storage and during distribution. Symmetric key-based cryptographic interactions establish start of session protocol by sharing key. Systems overcome vulnerable phase of key distribution by initiating session with public-private key and then switching over to shared session key (Arora and Hussain, 2018).

Biometric features capture behavioural and physical characteristics of a user. User traits are intrinsically bound to a person and hence establish identity of a person with high degree of confidence. Traits observed as characteristics present in body are termed as physiological traits while those exhibited by users are termed as behavioural traits. Physiological traits include face, fingerprint, iris, hand geometry, vascular structure, EEG, ECG while speech, handwriting, dynamic signature, gait, key stroke patterns, eyeball movements, hand gestures are categorised as behavioural traits. Feature vectors extracted from different traits possess varying characteristics in terms of inter-user and intra-user variations, ease of acquisition, vulnerability to sensor or environmental variations, user comfort, privacy and ethical issues. A conventional biometric system comprises of two phases: enrolment and recognition. User features such as fingerprint, iris, voice, etc. are captured through dedicated sensors and subjected to multiple algorithms to help identify optimal and consistent features. The pruned feature set is stored in a template as a fixed dimension vector as in case of iris. The stored feature vector template forms the basis of comparison while verifying identity of a user. A new sample of user is extracted, compared with stored template and the feature vector that satisfies closest proximity conditions is verified as identity of user. Feature vectors from certain traits such as face, speech and gait are more easily acquirable and require minimum cooperation from user. Behavioural traits such as handwritten signature, conventionally used for identity authentication in legal and financial transactions, provide high distinctiveness and are difficult to impersonate. Iris trait produces feature sets that are stable and consistent due to lower intra-user variation.

Integration of user specific traits with cryptographic systems greatly enhances security of symmetric key-based transactions. Biometrics is good at identity verification with better protection against repudiation. Cryptography provides enhanced security, privacy and anonymity while requiring better verification mechanisms. The common verification mechanisms used in cryptography are based on passwords and/or tokens which are vulnerable due to weak link between identity of person and associated cryptographic keys. Cryptographic principles can assist incorporation of revocability, privacy and template diversity in biometric systems, while biometrics-based cryptographic systems provide keys strongly linked to user identity.

Key binding, release and generation from user traits have been researched to achieve integration of cryptographic systems and biometrics (Rathgeb and Uhl, 2011). Features extracted from dynamic signatures and iris has been explored for key generation with limited success (Suresh and Radhika, 2018). Keys used in cryptography require an exact match between encryption and decryption stage. Biometric traits inherently expose both intra-user and inter-user variations. Intra-user variations in feature set additionally occur due to sensor variation, aging, environmental aspects such as lighting, dust, humidity and other similar factors. Binding user specific features with keys require higher inter-user variations and minimal intra-user variations. Iris trait of a user shows minimal intra-user variation and higher accuracy (Jain et al., 2016).

Extraction of consistent reproducible feature vectors from user traits remains a challenge in integrating biometrics with crypto-systems (Singh and Sinha, 2018). Extraction of optimal feature vectors from user traits requires use of novel algorithms, in addition to conventional feature extraction methods. Researchers are exploring innovative algorithms from spectrum of genetic, memetic and other nature inspired metaheuristic techniques to extract features from user specific traits with minimal intra-user variation (Sheng et al., 2015). Deep learning methods are being utilised to augment algorithmic techniques for improving accuracy of user trait-based authentication systems (Ríos-Sánchez et al., 2020; Kuzu et al., 2020).

The overall contributions of current research work are:

- extraction of feature vectors from iris trait
- selection of optimal feature vector using hybrid metaheuristics technique
- to train a neural network for enabling authentication based on optimal features
- binding optimal feature vector set with encrypted symmetric key
- demonstration of retrieval of symmetric key from user linked encrypted symmetric key.

2 Related work

2.1 Iris feature extraction

Researchers have shown that iris feature vector sets display a high degree of inter-user variability with minimal intra-user variations. Accurate and consistent code vectors extractable from iris traits make them ideal candidates for fusion with cryptographic keys. Iris code generation involves capture of image, pre-processing, image segmentation, normalisation and encoding (Suresh and Radhika, 2019). Figure 1 depicts primary steps involved in extraction of feature vectors from iris traits. Wavelet encoding, Gabor filters, log-Gabor filters, Haar wavelet, Laplacian of Gaussian filters and Legendre wavelet filter-based techniques have been employed to generate codes (Danlami et al., 2020). Detection of iris portion from image of an eye requires segmenting and marking of concentric circles, highlighting the iris portion while eliminating eyelashes, eyelids and specular reflections. Techniques for segmentation, encoding and matching iris traits are listed in Table 1. Steps involved in extraction of features from iris are shown in Figure 2.

Figure 1 Iris analysis and feature extraction

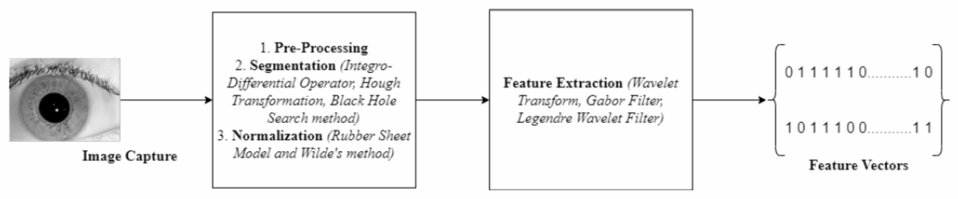
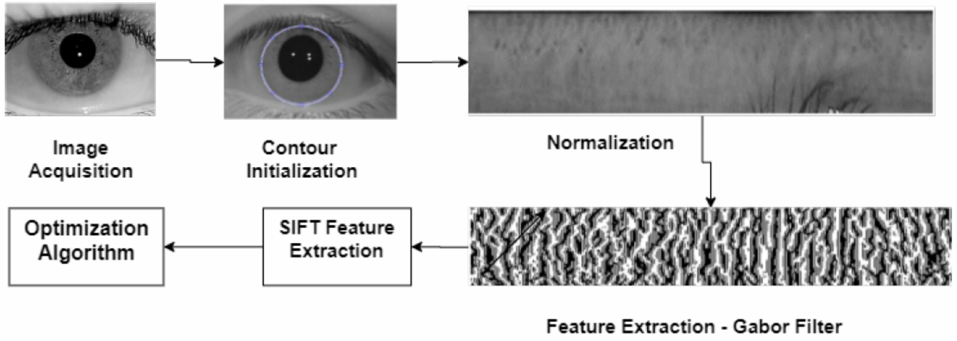


Image Capture
1. Pre-Processing
2. Segmentation (Integro-Differential Operator, Hough Transformation, Black Hole Search method)
3. Normalization (Rubber Sheet Model and Wilde's method)
Feature Extraction (Wavelet Transform, Gabor Filter, Legendre Wavelet Filter)
0 1 1 1 1 1 0..........1 0
1 0 1 1 1 0 0..........1 1
Feature Vectors

Table 1 Iris segmentation, encoding and matching

Process		*Technique*	*Authors*
Segmentation	1	Integro-differential operator	Daugman (1995), Huang et al. (2004), Danlami et al. (2018), Wang et al. (2020), Jalilian et al. (2020), Rafik and Boubaker (2020)
	2	Hough transform	
	3	Black hole search	
	4	Active shape models	
	5	Deep learning-based	
	6	CNN-based models	
	7	Metaheuristic models	
Encoding	1	2-D Gabor wavelet coefficients	Noruzi et al. (2006), Lim et al. (2001), Dorairaj et al. (2005), Ma and Sham (2019), Koç et al. (2019)
	2	Laplacian of Gaussian filter	
	3	Wavelet transform	
	4	Gabor filters	
	5	Haar wavelet transform	
	6	PCA	
	7	Error correction codes	
Matching	1	Hamming distance	Shah and Ross (2009), Păvăloi et al. (2019), Iglesias et al. (2019)
	2	Normalised correlation	
	3	Euclidean distance	
	4	SIFT-based	
	5	Optical flow-based	

Figure 2 Feature extraction – steps (see online version for colours)



Feature vectors extracted from iris are unique to user and exhibit high degree of permanence, performance and collectability. Image of iris from a user is obtained in a non-invasive manner, making acceptability of acquisition process higher (Dharanesh et al., 2017). Advent of smartphones with iris-based identification systems has further increased applicability of the user trait. Constraint of camera capability and variations in light intensity are challenges to iris image capture by mobile phones. Deep learning with optimal feature fusion techniques is being explored by researchers to overcome this constraint (Zhang et al., 2018). Improved camera technology, smarter phones with higher computing capability and employment of deep learning algorithms is resulting in increased use of iris-based biometric authentication systems. Acceptability of iris-based system is higher due to consistency of feature vectors produced by feature extraction techniques. Feature vectors produced from iris trait are highly suitable for use in closed authentication systems but are found wanting when used for open authentication systems (Eastwood et al., 2016), necessitating further research for extraction of stable features. Optimisation techniques are being researched to improve stability of feature vectors obtained through conventional binarisation methods (Hu et al., 2017).

2.2 Nature inspired metaheuristics algorithms

Metaheuristic techniques are nature inspired algorithms and are being explored by researchers to solve numerous real world optimisation problems. Nature inspired methods perform well under uncertain conditions and provide effective solutions within defined constraints. Performance of metaheuristics techniques is lower than exact solutions but much better than random approaches. Techniques involving metaheuristic methods adopt a trade-off approach between local maxima and global exploration. Efficiency of these algorithms is realised in scenarios where brute force search for exact solution would be computationally expensive. Metaheuristic techniques aim to obtain an efficient and practical solution to complex problems with quality solutions (Aktel et al., 2016; Tsai and Rodrigues, 2014). The techniques are problem agnostic and hence find applicability in multiple domains. Metaheuristic techniques are categorised as single point search and population-based algorithms. Popular metaheuristic techniques include ant colony optimisation, evolutionary computation, physics-based methods and particle swarm optimisation. A further category is hybrid algorithms that comprise a mix of nature-based algorithms with other similar or exact techniques.

Meng et al. (2014) proposed a technique called chicken swarm optimisation (CSO) by imitating hierarchical behaviour in chicken swarm. CSO is divided into *ro*, *he*, *ch* and *mh*, indicating roosters, hens, chicks and mother hens. Positional update and pattern of movement of hens while searching for food depends upon fitness capability of each entity of swarm. CSO has been improved by considering an aggregate function based on social hierarchy of chicken population resulting in reduced convergence time of CSO (Zouache et al., 2019). Mirjalili and Lewis (2016) proposed an algorithm termed as whale optimisation algorithm (WOA), based on hunting behaviour of hump-back whales. The technique mimicking the manner of search, encircling and foraging pattern by whales has been tested on various structural engineering domain problems. Grey wolf optimisation (GWO) is a class of technique based on leadership hierarchy and hunting pattern exhibited by wolves. Leadership hierarchy of wolves is divided and ranked into categories – alpha, beta, delta and omega, in descending order of hierarchy. Optimisation technique is mathematically simulated by patterns of tracking, pursuing and attack of prey by wolves in hierarchy. The algorithm has been applied to optimisation problems in domain of optical engineering with encouraging results (Mirjalili et al., 2014). Deer hunting optimisation algorithm (DHOA) proposed by Brammya et al. (2019) is based on hunting pattern of human beings while attacking a buck/deer. A set of two hunters comprising of a leader and successor are defined. Task of hunters is to track and hunt a deer. Search space, motion dynamics and capabilities of deer as against that of hunters is used to define boundary conditions and constraints of problem. Hunting algorithm involves encircling of deer taking into account additional parameters like wind angle, positional update of deer, lead hunter and successor. Mathematical model of technique factors in aspects related to cooperation and interaction of contributing factors. Hunting-based techniques are further optimised by using adaptive boundaries for area of search and adjusting rate of separation distance between hunter and prey (Zhao et al., 2019).

2.3 Symmetric key management

Use of symmetric key for encryption and security of communication is an active area of interest for researchers working towards defining a rugged identity management system. Shared keys possess lot of advantages over public-private key systems though key distribution in a distributed open communication network remains a challenge. Diffie-Hellman key exchange protocol, Lamport scheme, time stamped passwords are some solutions for overcoming vulnerabilities of key distribution (Anikin et al., 2016). Existing solutions face threats due to man-in-middle attacks forcing need for further strengthening of key distribution mechanism. Key distribution over large wireless distributed networks result in increased overheads (Gu et al., 2009). Integration of user traits extracted from physiological or behavioural features is a solution to optimising key distribution (Barman et al., 2014).

3 Proposed methodology

The work proposes a novel key binding mechanism to attain secure and reliable key distribution. User traits are bound to an encrypted shared key. The encrypted key is retrievable only by authorised user to whose trait the key is bound to. Steps involved in proposed methodology are explained in detail.

3.1 Key binding and encryption – training

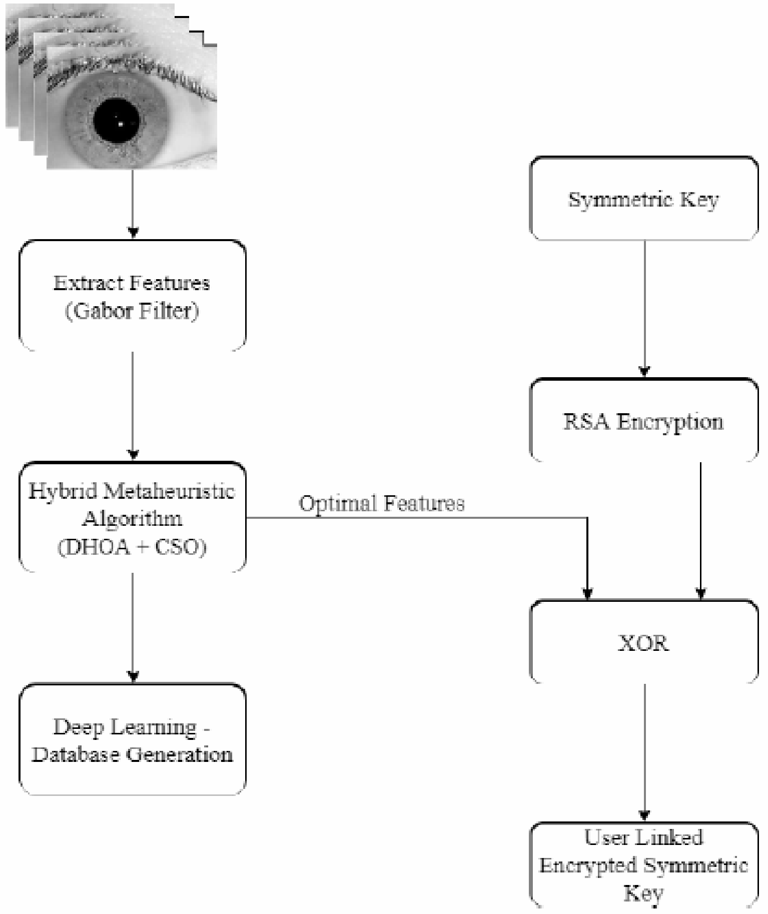
Figure 3 shows architectural layout for key binding and encryption. The schema includes training of a neural network for generating a user specific database comprising of optimal features. Symmetric key required to be shared over open communication channel is encrypted and bound to user. Encryption provides an additional layer of security while binding of key to user ensures that only authorised user is able to decrypt and retrieve key. RSA encryption is used for encrypting shared key. Encrypted key is bound to optimal feature vector extracted from iris of user through an XOR operation. Gabor filters are used to extract encoded feature vectors from iris of each user. Encoded bits are obtained by convolving normalised image with Gabor function [equation (1)].

Convolution results in real and imaginary parts, resulting in four possible combinations for each complex number. Coding convention results in a 20 × 480 matrix for the iris.

$$f\left(x, y, \omega, \theta, \sigma_x, \sigma_y\right) = \frac{1}{2\pi\sigma_x\sigma_y} \exp\left[\frac{-1}{2}\left(\left(\frac{x}{\sigma_x}\right)^2 + \left(\frac{y}{\sigma_y}\right)^2\right) + j\omega(x\cos\theta + y\sin\theta)\right] \quad (1)$$

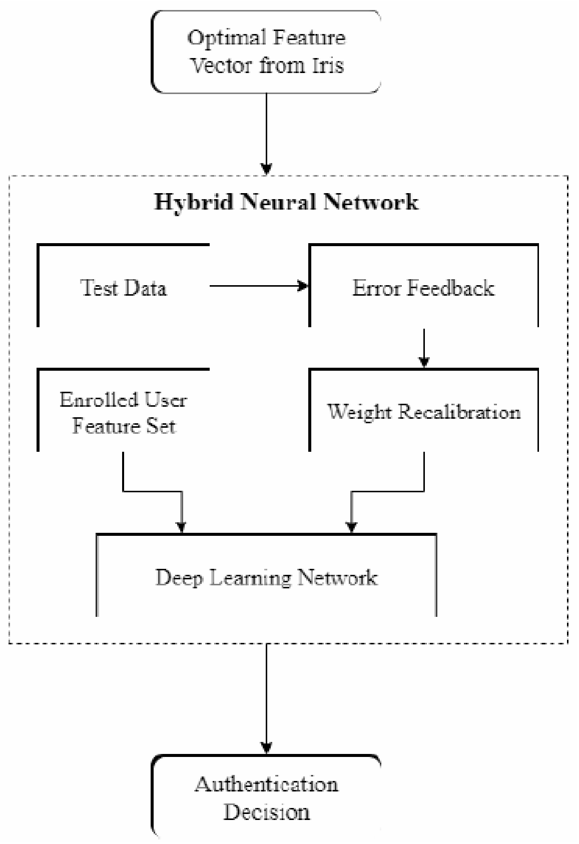
σ is spatial spread, ω is frequency and θ is the orientation.

Figure 3 Binding symmetric key to user


Symmetric Key
Extract Features (Gabor Filter)
RSA Encryption
Hybrid Metaheuristic Algorithm (DHOA + CSO)
Optimal Features
XOR
Deep Learning - Database Generation
User Linked Encrypted Symmetric Key

A hybrid metaheuristic algorithm combining DHOA and CSO algorithms is applied on extracted features to identify optimal features, which in turn is used to train a neural network as depicted in Figure 4.

Figure 4 Training of neural network



3.1.1 Chicken swarm optimisation

Chicken population is ordered as per fitness value. Roosters have highest fitness, chicks the worst and hens have fitness level in between. Roosters with higher fitness levels search food over larger areas as compared to these with lower levels of fitness. Movement of roosters is represented by locations $P_{x,y}^{t_s}(x \in [1, \mathrm{L}\ , M], y \in [1, \mathrm{L}\ , d_s])$ at time steps t_s in dimensional space d_s, as given in equation (2). $Rnd(0, \sigma^2)$ is a Gaussian distribution function with standard deviation σ^2 as shown in equation (3). ft is the fitness value of rooster. ε is utilised to prevent zero-division error while c denotes rooster index.

$$P_{x,y}^{t_s+1} = P_{x,y}^{t_s} * \left(1 + Rnd\left(0, \sigma^2\right)\right) \tag{2}$$

$$\sigma^2 = \begin{cases} 1, & \text{if } ft_x \le ft_c \\ \exp\left(\dfrac{\left(ft_c - ft_x\right)}{\left|ft_x\right| + \varepsilon}\right), & \text{otherwise, } c \in [1, M], c \ne x \end{cases} \tag{3}$$

Hens tag along the rooster of their group in search of food. Position of hens is updated as per equation (4):

$$P_{x,y}^{ts+1} = P_{x,y}^{ts} + B1 * Rd * \left(P_{rs1,y}^{ts} - P_{x,y}^{ts}\right) + B2 * Rd * \left(P_{rs2,y}^{ts} - P_{x,y}^{ts}\right) \tag{4}$$

$$B1 = \exp\left(\frac{\left(ft_x - ft_{rs1}\right)}{\left(abs\left(ft_x\right) + \varepsilon\right)}\right) \tag{5}$$

$$B2 = \exp\left(ft_{rs2} - ft_x\right) \tag{6}$$

Rd is a random number, *rs*1 is index of rooster belonging to x^{th} hen group and *rs*2 is index of rooster selected randomly from swarm such that $rs1 \neq rs2$. $ft_x > ft_{rs1}$ and $ft_x > ft_{rs2}$, therefore $B2 < 1 < B1$.

Chicks search their food by moving around their mother. $P_{cm,y}^{ts}$ is position of x^{th} chick's mother ($cm \in [1, M]$). Parameter C_M ($C_M \in (0, 2)$) implies that chick follows mother in search of food. C_M of every chick is selected randomly from 0 to 2 to denote speed at which the chick follows its mother hen. Movement of chicks about their mother for searching food is modelled in equation (7).

$$P_{x,y}^{ts+1} = P_{x,y}^{ts} + C_M * \left(P_{cm,y}^{ts} - P_{x,y}^{ts}\right). \tag{7}$$

3.1.2 Deer hunting optimisation algorithm

Population of hunters is initialised. *N* is total number of hunters with P_o as population. *Rand* is a random number ranging 0 to 1. θ_{ts} is the wind angle along the circular search area as given in equation (9). Position of prey is denoted in equation (10). Position of leader (P^{ld}) and successor (P^{Su}) are two best solutions. Position update is dependent on position of successor and is updated every iteration till best solution is obtained. Angle of visualisation of prey, *va*, is calculated as in equation (11). The encircling behaviour and position update of each hunter is based on position of successor and is modelled as per equation (12).

$$P_o = \left\{P_1, P_2, \ldots, P_N\right\} \quad 1 < i < N \tag{8}$$

$$\theta_{ts} = 2\pi Rand \tag{9}$$

$$\phi = \theta + \pi \tag{10}$$

$$va_{ts} = \frac{\Pi}{8} \times Rand \tag{11}$$

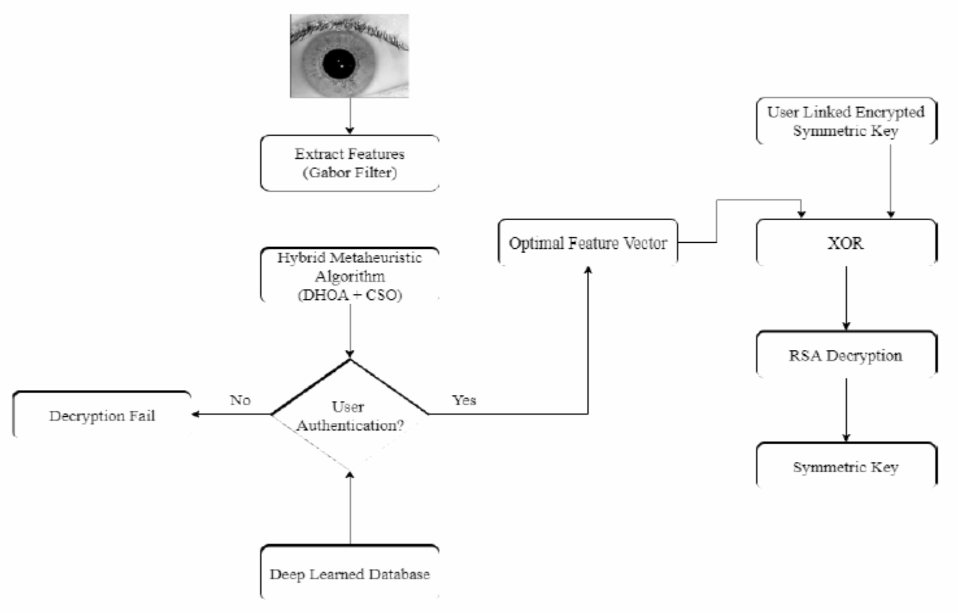
$$P_{ts+1} = P^{Su} - C \cdot g \cdot \left|D \times P^{Su} - P_{ts}\right| \tag{12}$$

where P_{ts} is position at current iteration, P_{ts+1} is position at next iteration, *C* and *D* are coefficient vectors.

3.2 Key retrieval and decryption – testing

Figure 5 shows architectural layout for key decryption. Gabor filter and DHOA-CSO metaheuristic techniques are used to extract optimal features of user. Extracted optimal feature set is compared with assistance of trained neural network to ascertain identity of user. Users that pass authentication criterion by neural network evaluation alone are authorised for extracting shared key from input encrypted stream. Optimal features of authenticated users are XORed with RSA encrypted user linked key to extract the RSA encrypted key. RSA decryption finally reveals the symmetric key distributed over the network.

Figure 5 Key retrieval



4 Results and discussion

4.1 Experimental setup

Selection of optimal features from iris dataset, training of neural network and key binding has been implemented in MATLAB 2018a. The work has used Indian Institute of Delhi (IITD) and Multimedia University (MMU) iris databases for experiments.

- *IITD database:* The dataset consists of images captured using JIRIS JPC1000 digital CMOS camera from 224 users in bitmap format. A total of 1,120 images from 176 males and 48 females form the database. All images are at resolution of 320 × 240 pixels acquired indoors.
- *MMU database:* The dataset comprises of 1,445 bitmap images at a resolution of 320 × 240 pixels.

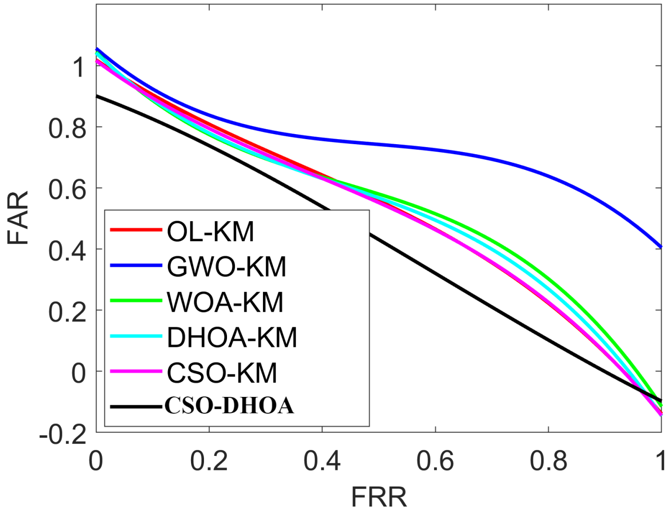
4.2 Discussion of results

Experiments for analysis of performance have been carried out for different key lengths – 36, 43, 64, 78 and 99. Optimal features are selected over 25 iterations. Performance of proposed hybrid optimisation approach is compared with an approach without optimisation and with state-of-art optimisation models GWO, WOA, DHOA and CSO. The hybrid technique combining CSO and DHOA is evaluated for ten metrics, i.e., accuracy, sensitivity, specificity, precision, false positive rate (FPR), false negative rate (FNR), negative predictive value (NPV), false discovery rate (FDR), F1-score and Matthews correlation coefficient (MCC). Results are shown in Table 2. Hybrid combination of CSO and DHOA shows an improved performance over compared algorithms.

Table 2 Performance of hybrid algorithm

Measure	*Without optimisation*	*GWO*	*WOA*	*DHOA*	*CSO*	*CSO-DHOA*
Accuracy	0.937	0.894	0.84	0.846	0.894	0.952
Sensitivity	0.965	0.973	0.91	0.876	0.905	0.968
Specificity	0.909	0.79	0.749	0.807	0.879	0.931
Precision	0.9	0.858	0.826	0.856	0.907	0.948
FPR	0.07	0.209	0.25	0.192	0.12	0.068
FNR	0.024	0.26	0.089	0.123	0.094	0.031
NPV	0.911	0.79	0.749	0.807	0.879	0.931
FDR	0.073	0.141	0.173	0.143	0.092	0.051
F1-score	0.902	0.912	0.86	0.86	0.906	0.958
MCC	0.901	0.79	0.675	0.686	0.784	0.902

Figure 6 ROC analysis (see online version for colours)



Receiver operating curve (ROC) for a key length of 64 is plotted in Figure 6. Each point on the ROC plot indicates a sensitivity (or) specificity pair related to specific decision threshold. Figure 6 shows that the implemented hybrid metaheurisitc technique outperforms conventional models at all FRRs.

Combination of two optimisation techniques for selection of optimal features and training neural network has yielded encouraging results for all metrics considered. Iris trait of users yields distinct feature vectors and is suited for extraction of consistent optimal feature vectors. Variation of metrics over different key lengths is due to the reason that in case of key decryption, there has to be a complete match for all bits.

4.3 Computational complexity

The computational complexity of feature selection in proposed iris-based system is shown in Table 3. The computational speed of the proposed hybrid 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 methodology is 38.04%, 2.42%, 3.83%, 2.67%, and 1.73% superior to without optimisation, GWO, WOA, DHOA and CSO, respectively.

Table 3 Computation complexity

<table>
<tr><th colspan="6"><i>Feature selection (sec)</i></th></tr>
<tr><td colspan="2"><i>GWO</i></td><td><i>WOA</i></td><td><i>DHOA</i></td><td><i>CSO</i></td><td><i>CSO-DHOA</i></td></tr>
<tr><td colspan="2">413.41</td><td>419.03</td><td>433.50</td><td>461.62</td><td>397.16</td></tr>
<tr><td colspan="6"><i>Encryption and decryption (sec))</i></td></tr>
<tr><td><i>Without optimisation</i></td><td><i>GWO</i></td><td><i>WOA</i></td><td><i>DHOA</i></td><td><i>CSO</i></td><td><i>CSO-DHOA</i></td></tr>
<tr><td>10.2474</td><td>6.5061</td><td>6.6014</td><td>6.5229</td><td>6.4602</td><td>6.3484</td></tr>
</table>

4.4 Applications

Proposed work finds application in secure distribution of shared key in symmetric key-based systems. Identity management systems using symmetric keys over distributed open networks face major vulnerability while distribution of keys. The methodology proposed and demonstrated can be used gainfully for linking user traits optimally to a shared key. Authorised users alone would be able to access, decrypt and use shared key. Authentication is invariably the first step while accessing user directed services. The integration of iris biometric trait with shared key management exploits the complementary benefits of user features and cryptography and finds applicability in both central and federated identity management systems. Cryptographic principles assist incorporation of revocability, privacy and template diversity while linking keys to iris trait provide keys strongly linked to user identity. The non-invasive and stable feature codes extractable from iris make the system robust and easy to deploy. The difficulty of user linked authentication systems arise when excessive intra user variations occur due to extraneous factors such as poor sensor, data corruption and degradation resulting from environmental factors.

5 Conclusions

A novel methodology to link shared keys with user traits has been proposed, demonstrated and evaluated. Key binding has been achieved by linking shared key with optimal features extracted from iris biometric. The work has adopted a unique metaheuristic approach by combining CSO and DHOAs to extract optimal user features and train a neural network. Experimental results show that proposed methodology is performant and yields better results as compared to state-of-art optimisation techniques. Results of experiments carried out show that accuracy of hybrid combination of CSO and DHOA algorithms is 6% and 11% better than individually selected CSO and DHOA algorithms, respectively. The proposed system provides an efficient means to share keys in addition to catering for authentication of users. A detailed study has been conducted with iris biometric. As part of future work, newer metaheuristic techniques including genetic and memetic algorithms on multi-modal biometric feature sets including larger iris datasets will be carried out to further improve the system.

References

Aktel, A., Yagmahan, B., Ozcan, T., Yenisey, M.M. and Sansarc, E. (2016) 'The comparison of the metaheuristic algorithms performances on airport gate assignment problem', in *19th EURO Working Group Transportation Meeting, EWGT2016*, Elsevier, 5–7 September, DOI: 10.1016/ j.trpro.2017.03.061.

Anikin, I.V., Makhmutova, A.Z. and Gadelshin, O.E. (2016) 'Symmetric encryption with key distribution based on neural networks', *2016 2nd International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM)*, Chelyabinsk, pp.1–4, DOI: 10.1109/ ICIEAM.2016.7911640.

Arora, S. and Hussain, M. (2018) 'Secure session key sharing using symmetric key cryptography', *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Bangalore, pp.850–855, DOI: 10.1109/ICACCI.2018.8554553.

Assiri, S., Cambou, B., Booher, D.D., Miandoab, D.G. and Mohammadinodoushan, M. (2019) 'Key exchange using ternary system to enhance security', *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA, pp.488–492, DOI: 10.1109/CCWC.2019.8666511.

Barman, S., Chattopadhyay, S. and Samanta, D. (2014) 'An approach to cryptographic key distribution through fingerprint based key distribution center', *2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, New Delhi, pp.1629–1635, DOI: 10.1109/ICACCI.2014.6968299.

Brammya, G., Praveena, S., Preetha, N., Ramya, R., Rajakumar, B.R. and Binu, D. (2019) 'Deer hunting optimization algorithm: a new nature-inspired meta-heuristic paradigm', *The Computer Journal* [online] https://doi.org/10.1093/comjnl/bxy133.

Chandra, S., Paira, S., Alam, S.S. and Sanyal, G. (2014) 'A comparative survey of symmetric and asymmetric key cryptography', *2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE)*, Hosur, pp.83–93, DOI: 10.1109/ ICECCE.2014.7086640.

Chen, B., Wu, L., Li, L., Choo, K.R. and He, D. (2020) 'A parallel and forward private searchable public-key encryption for cloud-based data sharing', *IEEE Access*, Vol. 8, pp.28009–28020, DOI: 10.1109/ACCESS.2020.2971089.

Danlami, M. et al. (2018) 'An efficient iris image thresholding based on binarization threshold in black hole search method', *International Journal of Engineering & Technology*, December, Vol. 7, No. 4.31, pp.34–39, Sl, ISSN: 2227-524X, DOI: http://dx.doi.org/10.14419/ijet.v7i4. 31.23337 [online] https://www.sciencepubco.com/index.php/ijet/article/view/23337 (accessed 31 August 2020).

Danlami, M., Jamel, S., Ramli, S.N. and Azahari, S.R.M. (2020) 'Comparing the Legendre wavelet filter and the Gabor wavelet filter for feature extraction based on iris recognition system', *2020 IEEE 6th International Conference on Optimization and Applications (ICOA)*, Beni Mellal, Morocco, pp.1–6, DOI: 10.1109/ICOA49421.2020.9094465.

Daugman, J. (1995) 'High confidence recognition of persons by rapid video analysis of iris texture', *European Convention on Security and Detection*, Brighton, UK, pp.244–251, DOI: 10.1049/cp:19950506.

Dharanesh, C.M., Prasad, R. and Patil, C.M. (2017) 'Feature extraction classification for personal identification using iris', *2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC)*, Mysore, pp.431–435, DOI: 10.1109/CTCEEC.2017.8455060.

Dorairaj, V., Schmid, N.A. and Fahmy, G. (2005) 'Performance evaluation of iris-based recognition system implementing PCA and ICA encoding techniques', *Proc. SPIE 5779, Biometric Technology for Human Identification II*, 28 March [online] https://doi.org/10.1117/12.604201.

Eastwood, S.C., Shmerko, V.P., Yanushkevich, S.N., Drahansky, M. and Gorodnichy, D.O. (2016) 'Biometric-enabled authentication machines: a survey of open-set real-world applications, *IEEE Transactions on Human-Machine Systems*, April, Vol. 46, No. 2, pp.231–242, DOI: 10.1109/THMS.2015.2412944.

Gu, Q., Peng, L., Lee, W-C. and Chu, C-H. (2009) 'KTR: an efficient key management scheme for secure data access control in wireless broadcast services', *IEEE Transactions on Dependable and Secure Computing*, July–September, Vol. 6, No. 3, pp.188–201, DOI: 10.1109/TDSC.2008.12.

Hu, Y., Sirlantzis, K. and Howells, G. (2017) 'Optimal generation of iris codes for iris recognition', *IEEE Transactions on Information Forensics and Security*, January, Vol. 12, No. 1, pp.157–171, DOI: 10.1109/TIFS.2016.2606083.

Huang, J., Wang, Y., Tan, T. and Cui, J. (2004) 'A new iris segmentation method for recognition', *Proceedings of the 17th International Conference on Pattern Recognition, 2004. ICPR 2004*, Cambridge, Vol. 3, pp.554–557, DOI: 10.1109/ICPR.2004.1334589.

Iglesias, P., Hernández-García, R., Barrientos, R.J., Goncalves, E. and Mora, M. (2019) 'Iris recognition based on displacement information using a sparse matching technique', *2019 38th International Conference of the Chilean Computer Science Society (SCCC)*, Concepcion, Chile, pp.1–8, DOI: 10.1109/SCCC49216.2019.8966438.

Jain, A.K., Nandakuma, K. and Ross, A. (2016) '50 years of biometric research: accomplishments, challenges, and opportunities', *Pattern Recognition Letters*, Vol. 79, pp.80–105, Elsevier [online] http://dx.doi.org/10.1016/j.patrec.2015.12.013.

Jalilian, E., Karakaya, M. and Uhl, A. (2020) 'End-to-end off-angle iris recognition using CNN based iris segmentation', *2020 International Conference of the Biometrics Special Interest Group (BIOSIG)*, Darmstadt, Germany, pp.1–7.

Koç, O., Tosku, L., Hoxha, J., Topal, A.O., Ali, M. and Uka, A. (2019) 'Detailed analysis of iris recognition performance', *2019 International Conference on Computing, Electronics Communications Engineering (iCCECE)*, London, UK, pp.253–258, DOI: 10.1109/iCCECE46942.2019.8941784.

Kuzu, R.S., Piciucco, E., Maiorana, E. and Campisi, P. (2020) 'On-the-fly finger-vein-based biometric recognition using deep neural networks', *IEEE Transactions on Information Forensics and Security*, Vol. 15, pp.2641–2654, DOI: 10.1109/TIFS.2020.2971144.

Lim, S., Lee, K., Byeon, O. and Kim, T. (2001) 'Efficient iris recognition through improvement of feature vector and classifier', *ETRI Journal*, Vol. 23, pp.61–70, DOI: 10.4218/etrij.01.0101.0203.

Ma, L. and Sham, C. (2019) 'SoC-FPGA-based implementation of iris recognition enhanced by QC-LDPC codes', *2019 International Conference on Field-Programmable Technology (ICFPT)*, Tianjin, China, pp.391–394, DOI: 10.1109/ICFPT47387.2019.00075.

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

Mirjalili, S. and Lewis, A. (2016) 'The whale optimization algorithm', *Advances in Engineering Software*, May, Vol. 95, pp.51–67 [online] https://doi.org/10.1016/j.advengsoft.2016.01.008.

Mirjalili, S., Mirjalili, S.M. and Lewis, A. (2014) 'Grey wolf optimizer', *Advances in Engineering Software*, March, Vol. 69, pp.46–61, Elsevier [online] https://doi.org/10.1016/j.advengsoft.2013.12.007.

Noruzi, M., Vafadoost, M. and Moin, M.S. (2006) 'Iris recognition: localization, segmentation and feature extraction based on Gabor transform', in Gavrilova, M. et al. (Eds.): *Computational Science and Its Applications – ICCSA 2006*.

Păvăloi, I., Niţă, C.D. and Lazăr, L.C. (2019) 'Novel matching method for automatic iris recognition using SIFT features', *2019 International Symposium on Signals, Circuits and Systems (ISSCS)*, Iasi, Romania, pp.1–4, DOI: 10.1109/ISSCS.2019.8801797.

Rafik, H.D. and Boubaker, M. (2020) 'Application of metaheuristic for optimization of iris image segmentation by using evaluation Hough transform and methods Daugman', *2020 1st International Conference on Communications, Control Systems and Signal Processing (CCSSP)*, El Oued, Algeria, pp.142–150, DOI: 10.1109/CCSSP49278.2020.9151617.

Rathgeb, C. and Uhl, A. (2011) 'A survey on biometric cryptosystem and cancelable biometrics', *EURASIP J. Info. Security*, Vol. 3 [online] https://doi.org/10.1186/1687-417X-2011-3.

Ríos-Sánchez, B., Silva, D.C., Martín-Yuste, N. and Sánchez-Ávila, C. (2020) 'Deep learning for face recognition on mobile devices', *IET Biometrics*, May, Vol. 9, No. 3, pp.109–117, DOI: 10.1049/iet-bmt.2019.0093.

Shah, S. and Ross, A. (2009) 'Iris segmentation using geodesic active contours', *IEEE Transactions on Information Forensics and Security*, December, Vol. 4, No. 4, pp.824–836, DOI: 10.1109/TIFS.2009.2033225.

Sheng, W., Chen, S., Xiao, G., Mao, J. and Zheng, Y. (2015) 'A biometric key generation method based on semisupervised data clustering', *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, September, Vol. 45, No. 9, pp.1205–1217, DOI: 10.1109/TSMC.2015.2389768.

Singh, S. and Sinha, M. (2018) 'Pattern recognition based on specific weights', *Int. J. Applied Pattern Recognition*, Vol. 5, No. 1, pp.1–10.

Suresh, P. and Radhika, K.R. (2018) 'Biometric based consistent key generation for IMS', *TENCON 2018 – 2018 IEEE Region 10 Conference*, Jeju, South Korea, pp.2175–2180, DOI: 10.1109/TENCON.2018.8650543.

Suresh, P. and Radhika, K.R. (2019) 'Integrated framework for anonymous biometrickey based identity management system', *International Journal of Recent Technology and Engineering (IJRTE)*, September, Vol. 8, No. 3, pp.4594–4601, ISSN: 2277-3878.

Tsai, C. and Rodrigues, J.J.P.C. (2014) 'Metaheuristic scheduling for cloud: a survey', *IEEE Systems Journal*, March, Vol. 8, No. 1, pp.279–291, DOI: 10.1109/JSYST.2013.2256731.

Wang, C., Muhammad, J., Wang, Y., He, Z. and Sun, Z. (2020) 'Towards complete and accurate iris segmentation using deep multi-task attention network for non-cooperative iris recognition', *IEEE Transactions on Information Forensics and Security*, Vol. 15, pp.2944–2959, DOI: 10.1109/TIFS.2020.2980791.

Yassein, M.B., Aljawarneh, S., Qawasmeh, E., Mardini, W. and Khamayseh, Y. (2017) 'Comprehensive study of symmetric key and asymmetric key encryption algorithms', *2017 International Conference on Engineering and Technology (ICET)*, Antalya, pp.1–7, DOI: 10.1109/ICEngTechnol.2017.8308215.

Zhang, Q., Li, H., Sun, Z. and Tan, T. (2018) 'Deep feature fusion for iris and periocular biomerics on mobile devices', *IEEE Transactions on Information Forensics and Security*, November, Vol. 13, No. 11, DOI: 10.1109/TIFS.2018.2833033.

Zhao, Z., Wang, X., Wu, C. and Lei, L. (2019) 'Hunting optimization: an new framework for single objective optimization problems', *IEEE Access*, Vol. 7, pp.31305–31320, DOI: 10.1109/ACCESS.2019.2900925.

Zouache, D., Arby, Y.O., Nouioua, F. and Ben Abdelaziz, F. (2019) 'Multi-objective chicken swarm optimization: a novel algorithm for solving multi-objective optimization problems', *Computers and Indeustrial Engineering*, March, Vol. 129, pp.377–391, Elsevier [online] https://doi.org/10.1016/j.cie.2019.01.055.