Measurement: Sensors 24 (2022) 100511

Contents lists available at ScienceDirect

Measurement: Sensors

journal homepage: www.sciencedirect.com/journal/measurement-sensors

Privacy preserving steganography based biometric authentication system for cloud computing environment

D. Prabhu *, S. Vijay Bhanu, S. Suthir

Department of Computer Science and Engineering, Annamalai University, India

ARTICLE INFO

KeywordsTerms:
About authentication
Biometrics
Cloud computing
Eye retina image
Fingerprint
Privacy
Security
Steganography

ABSTRACT

Recently, cloud computing (CC) received significant interest among organizations and individuals. Despite the significant benefits of CC, security and privacy are considered as the major issue. Biometric authentication is commonly employed for authentication purposes and has gained attention among several researchers due to its stable and high recognition rate. Amongst the several biometric authentication models, fingerprint is treated as an effective one to achieve security and privacy. Besides, image steganographic approaches are applied in order to enhance the security of the biometric data. The state of art biometric data hiding techniques generally performs the data embedding on the region which does not encompass key features of the biometrics. With this motivation, this paper presents a privacy preserving steganography based biometric authentication system (PPS-BAS) for cloud environments. The goal of the PPS-BAS model is to hide the fingerprint image (secret image) into the eye retina image (cover image) and transmits it to the cloud in an encrypted way. The proposed PPS-BAS model involves multilevel discrete wavelet transform (DWT) technique to split the cover image in order to identify the pixel location. Besides, continuous pigeon inspired optimizer (CPIO) algorithm is applied to determine the optimal pixel points in the cover image. At the same time, a Q-learning technique is employed to extract the minutiae from the fingerprint image and is then hidden into the optimal pixel locations in the cover image. In order to further increase security, double-logistic chaotic map (DLCM) model is applied for encrypting the stego image which is then transmitted to the cloud server. After the reconstruction of the original fingerprint image (secret image), the biometric recognition process takes place using the Scaled Conjugate Gradient (SCG) based back propagation neural network (BPNN) model. A detailed simulation analysis is performed to highlight the enhanced outcomes of the proposed PPS-BAS model and the comparative results analysis ensured the betterment of the PPS-BAS model over the recent state of art biometric authentication systems.

1. Introduction

IN recent times, biometrics-based detection system has received significant attention because of its inherent benefits. It effectively offers the privacy preserving of cloud users and security of saved confidential data on the cloud server [1]. Therefore, the current development focuses to address the problems of growth management, maintenance of user privacy, and data integrity of cloud data. Together with the privacy preserving of users, maintaining and processing the data integrity, this technique plays a major part in data management in the CC. In past few decades, efficient and advanced methods to achieve security and privacy of the biometric data have been developed. Besides, biometrics based detection systems were also greatly investigated [2], which provide client verification by authenticating the person. Biometric authentication is one of the common and consistent access control methods and becomes a regular feature in smartphones [3,4]. This application requires securely storing the biometrics features in digital databases for matching consequent biometric templates. The storage of this confidential data, thus, requires effective encryption for ensuring secrecy. In the transmission of encrypted data, steganography is utilized for enhancing the privacy of the biometric validation scheme. These measures could be in the form of embedded biometric data to carrier objects, like facial images, whether unrelated/related to the user authentication [5]. Biometric data, with other personal information, could be used by cyber criminals for conducting identity thefts, and its monetary value creates it a commodity which is exported in underground marketplaces like dark web. The dark web contains a hidden network of websites that could be opened by a specific browser which

* Corresponding author.
E-mail address: dprabhume@gmail.com (D. Prabhu).

https://doi.org/10.1016/j.measen.2022.100511
Received 15 July 2022; Accepted 5 October 2022
Available online 13 October 2022

provides anonymizing feature for helping obfuscate client recognition.

In recent years, the utilization of biometric information like iris, fingerprints, and faces are utilized for verification purposes. Permitting several organizations like government and bank agencies, access to biometric templates presented by a central and trusted entity would be beneficial in several features [6]. Initially, it permits organizations that presently have no direct access to a freely available database. Next, this organization doesn't want to invest in the framework needed for enrolling novel users and stores raw biometric databases of their personal. It will decrease the threat of significant data breaches. Lastly, a client should register one time with the confidential entity for accessing services given by several organizations. Singapore's SingPass face authentication and India's Aadhaar project are the 2 current instances, whereas the organization subscribes to the national biometric database for enabling verification service to their user. Biometric access control system provides a security layer nearby safe resources [7]. Steganography techniques employed to the biometric data provides distinct and separate security layers. It has the benefits of combining biometrics with steganography like augmenting the security of sensitive biometric data in transmission, and acceptance in real time application must be continued.

This paper presents privacy preserving steganography based biometric authentication system (PPS-BAS) for cloud environment to hide the fingerprints image (secret image) into the eye retina image (cover image). The proposed PPS-BAS model involves multilevel discrete wavelet transform (DWT) technique with continuous pigeon inspired optimizer (CPIO) algorithm for the identification and optimal pixel point selection in the cover image. Besides, a Q-learning technique is employed for the minutiae extraction from the fingerprint image and is then hidden into the optimal pixel locations in the cover image. Moreover, the double-logistic chaotic map (DLCM) model is utilized for encryption process. At last, the reconstruction of the original fingerprint image (secret image) takes place followed by Scaled Conjugate Gradient (SCG) based back propagation neural network (BPNN) model for biometric recognition. For examining the betterment of the proposed PPS-BAS model, a series of simulations take place on benchmark test images and investigated the outcomes in terms of different measures.

2. Literature review

This section surveys the existing biometric based authentication systems developed to achieve security. Venkatraman and Geetha [8] focused on hiding images by specialized steganographic image authentication (SSIA) method in cluster based cloud systems. The SSIA technique is employed for virtual elastic clusters in the public cloud environment. Now, the SSIA method embeds the image data by genetic operator and blowfish technique. At first, the blowfish approach is employed on the image and later the genetic operator is employed to reencrypt the image data. The presented method gives enhanced security compared to traditional blowfish method in a cluster based cloud scheme. Khudher [9] designed a Steganography Biometric Imaging System (SBIS). This scheme obtains RGB foot tip image and pre-process it to get foot templates. Later, chain code is demonstrated for individual data with the foot template image by Least Significant Bit (LSB). The precise identification process is executed by artificial bee colony optimization (ABC).

Sudhakar and Gavrilova [10] proposed a cancellable biometric architecture depending upon deep learning (DL) method on the cloud. They determine that cloud is a better resolution for biometric system whereas quick response times, intensive computation, and higher accurateness is needed. In Banerjee et al. [11], a novel security method was determined by creating the scheme more secure using steganography together with biometric security. domain of an image.

Das et al. [12] presented an effective and secured lip biometric architecture. Different from the conventional biometric architecture, which emphasis on the identification accurateness only, but they concentrate on both detection rate together with secured template stored in the biometric scheme. It involves preprocessing to improve the local feature of the lip image. The local interest point is identified by Scale Invariant Feature Transform (SIFT) that is utilized to extract the lip feature. AL-Kateeb and AL-Bazaz [13] proposed a method for hiding private data in colourful images depending upon the features of engineering dimension of the human hand as all kinds of biometrics; they extract several features and process them to create a matrix which states the mapping of distribution of private data in the cover image. The presented technique was employed for several images to hide a group of private messages and visual quality of the cover image wasn't influenced afterward the concealment. The real-world result explains the performance of this technique that was measured base on relation among the original image after and before concealments.

Kayode et al. [14] proposed a method for securing eye retina template by steganography. The research analysis was performed on matrix laboratory (MATLABR2015A) platform. The segmented eye retina region was standardized to reduce the dimension variations among eye retina regions using Hough transform (HT). The feature of the eye retina has been encoded by convolving the standardized eye retina region with 1D Log Gabor filters to create a bitwise biometric template. Later, LSB was utilized for securing the eye retina template. The Hamming distance was selected as a matching metric that provides the measure of several bits disagreed among the templates of eye retina. Abikoye et al. [15] integrate Cryptography (Two fish and Triple data decryption (3DES)) method and Steganography LSB for solving the challenge of hacking/attacking biometric template for a malicious act that becomes a major challenge in the eye retina detection scheme. In this study, HT, Log Gabor filter, and Daugman rubber sheet model have been utilized to normalization feature extraction, and eye retina image segmentation as well as the eye retina template created was encrypted by Two fish and 3DES methods. The cipher image is later embedded into a cover image for producing stego image by LSB. Atighehchi et al. [16] proposed a transformation based biometric template protection system as an enhancement of BioHashing method whereas the projection matrix is made by integrating the biometric and secret data. Study outcomes on 3 biometric modules like hands vein images, digital fingerprint, and finger knuckle print display the advantage of the presented technique faces to an attack when maintaining a better performance.

3. The proposed PPS-BAM model

3.1. Overall system architecture

The working process involved in the PPS-BAM model is depicted in Fig. 1. The proposed PPS-BAM model involves different processes such as color channel separation, multi-level DWT based transformation, CPIO based optimal pixel selection, Q-learning based minutiae extraction, DLCM based encryption, and SCG-BPNN based biometric

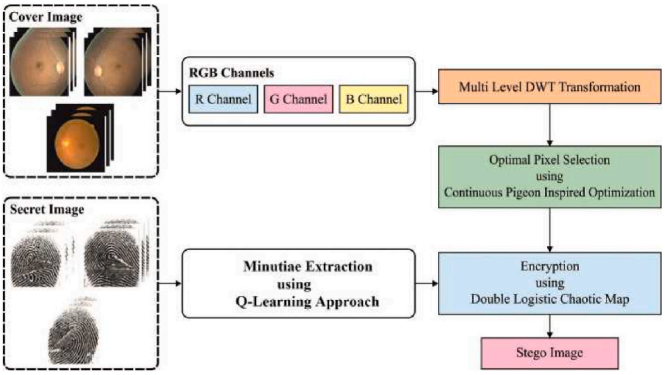


Fig. 1. Working process of PPS-BAM model.

recognition. Initially, the PPS-BAM model enables the channel separation of the RGB cover image (eye retina image), and then multi-level DWT based decomposition process takes place to split the image for the identification of pixel points. Then, the optimum pixels in the cover image are selected by the CPIO algorithm. Afterward, the minutiae from the fingerprint image are extracted and are hidden into the cover image. Followed by, the encryption of the stego image takes place using the DLCM technique and is transmitted to the cloud server for authentication process. On the cloud server side, the decryption and reconstruction of the stego image are carried out and the original fingerprint image is obtained. Finally, fingerprint image is fed into the SCG-BPNN model for the effectual recognition of biometrics, and then authenticated user will be identified. The detailed working of these processes is offered in the subsequent sections.

3.2. Multi-level DWT based transformation

The RGB cover eye retina image is divided into HH, LL, HL, and LH bands to detect the pixel position. The 2D DWT is a significant spatial to frequency domain transformation method. The separation is made by Vertical and Horizontal operations. The Horizontal operation decomposes an image to High (H) and Low (L) frequency bands. Next, the vertical operations decompose an image to HH_1, LL_1, HL_1, and LH_1 frequency bands. For secondary level of decomposition, LL_1 band is decomposed to HH_2 LL_2, HL_2, and LH_2. Consider the image size as 'M*N' [20]. Initially, to filter and down sample, the horizontal decomposition decreases the image to $M \times \frac{N}{2}$ size. The vertical reduction undergoes downsampling the image to $\frac{M}{2} \times \frac{N}{2}$. The single level decomposed outcome is made by Ref. [17]:

$$[C_1 C_2 C_3 C_4] = \mathrm{DWT}(C) \tag{1}$$

Where 'C_1', 'C_2', 'C_3', and 'C_4' denotes coefficient values. 'C_1' indicates low-level frequency band that is decomposed for extracting the subbands by:

$$\left[C_1^{\mathrm{LL1}} C_1^{\mathrm{LH1}} C_1^{\mathrm{HL1}} C_1^{\mathrm{HH1}}\right] = \mathrm{DWT}(C_1) \tag{2}$$

The succeeding level of decomposition is executed on low band LL_1. The decomposed form of frequency band is provided by:

$$\left[C_1^{\mathrm{LL2}} C_1^{\mathrm{LH2}} C_1^{\mathrm{HL2}} C_1^{\mathrm{HH2}}\right] = \mathrm{DWT}(\mathrm{LL}_1) \tag{3}$$

Where C_1^{LL2} indicates low-level frequency band of the 2nd level decomposition.

3.3. Optimal pixel selection using CPIO algorithm

The multilevel DWT transformation process offers the vector coefficients of the cover image. Amongst the different vector coefficients, the optimum pixels are chosen by the use of CPIO algorithm in such a way that the PSNR gets maximized. The objective function of the CPIO algorithm is determined using the fitness function. The objective is to develop a steganography approach that reduces the error level (MSE) and improves the PSNR. It can be defined as follows

$$F = \{min(MSE), max(PSNR)\} \tag{4}$$

The desirable lower and higher values are achieved using the CPIO algorithm. The PIO is an advanced bio inspired SI method, which is inspired by the homing behavior of pigeons. The pigeons acquired their homing characteristics based on 2 key operators: compass and landmark and map operators. Few researches of pigeon homing skill explained that the pigeon's capabilities for navigating its homeland come from small magnetic particles are placed at its peak [18]. It is mathematically stated by altering the location X_i and velocity V_i of pigeon i in every iteration. The values of X_i and V_i are upgraded for the subsequent iteration $(t+1)^{th}$ based on the value of present iteration t*'hin* Eqs. (5) and (6).

$$V_i(t+1) = V_i(t).e^{-Rt} + rand.\left(X_g - X_i(t)\right) \tag{5}$$

$$X_i(t+1) = X_i(t) + V_i(t+1) \tag{6}$$

Where R indicates map and compass factor when *rand* denotes uniform arbitrary number in the range zero and one , X_g represents global optimum solution, $X_i(t)$ indicates present location of pigeon at instance t, and $V_i(t)$ represents present velocity of pigeon at iteration t.

Every pigeon alters their flying location based on map and compass operator via next optimum pigeon location. The entire pigeon's location is estimated through a certain objective function. The optimum pigeon is denoted using black pigeon, another pigeon would follow this pigeon based on Eq. (5), whereas the initial portion of the formula denotes present pigeon direction and is given by using thin straight arrow when the next portion of Eq. (5) denotes an optimum pigeon direction and stated by using thick arrow. The summary of these 2 vectors is the following flying course for the pigeon. Every pigeon would alter their location based on novel direction evaluated by Eqs. (5) and (6). In landmark operators, every pigeon is ranked based on fitness value. In every generation, the pigeon count is upgraded in Eq. (7), whereas only half number of pigeons is assumed to estimate the desirable location of the central pigeon when other pigeons alter their end by next the desired end location. The location of the desirable end is estimated using Eq. (8) when other pigeons upgrade their location using Eq. (9). The desired end location is denoted using black pigeon when the pigeons in the circle are 50% of pigeons are estimated using Eq. (7).

$$N_p(t+1) = \frac{N_p(t)}{2} \tag{7}$$

Where N_p denotes number of pigeons in present iteration t.

$$X_c(t+1) = \frac{\sum X_i(t+1).Firness(X_i(t+1))}{N_p \sum Fitness\left(X_i(t+1)\right)} \tag{8}$$

Where X_c indicates location of the center pigeon (desirable end), when X_i indicates present location of every pigeon.

$$X_i(t+1) = X_i(t) + rand.(X_c(t+1) - X_i(t)) \tag{9}$$

3.4. Q-learning based minutiae extraction

For extracting the minutiae from the fingerprint images, Q-learning technique is employed. It is an active reinforcement technique in which it creates and enhances the agent's policy on the fly. They place an agent onto the fingerprint image. This agent follows the ridge by grey scale values and choosing a state from reward structure. To attain the reward structure, they take a fingerprint image and employ diminishing to the image up to single pixel value. They scan the image with the help of 3 × 3 filter and greyscale values. A single intermediate neighbor is considered as end point, 2 neighbor of central is considering as a bifurcation. Once the entire image is scanned, they attain whole end points and bifurcation. Then, they estimate Euclidean distance of these points and takes this distance as reward structure R. Besides, the states are chosen. They take variation of rows in reward structure and choose the initial state. Here, they detect whole non-negative values from R and takes variation of these non-negative values. This nonnegative value is preserved as action [19]. Hence, they choose an action that has highest non-negative value and estimate Q [state, action]. The select action would be their novel state, reiterate the process till the process gets terminated.

3.5. Encryption using DLCM technique

During the encryption process, the stego image which is generated from the cover image and extracted minutiae are encrypted using the DLCM technique. Based on present cryptosystem, the encryption and decryption procedures are understood by the conversion process of the decryption and encryption keys. The encryption target is the plaintext space, and the decryption target is the cipher text space. For the cryptographic architecture of the digital images, the plain text space P equivalent to the group of pixels of the input image which should be encrypted, and the cipher text space C equivalent to the group of image pixels later the encryption. The cipher text space C attained using plain text space P afterward encryption is transferred via unsecured network. The key K is a key to perform encryption and decryption convert operations [20]. A similar key might be utilized to various decryption and encryption keys based on chosen encryption technique, or various keys might be utilized. In key space $\{K\}$, the control design of the encryption method is understood that is a space consist of the fundamental data grabbed by cipher text and plain text spaces. The key flow is depending upon double chaotic image encryption technique. The 2 chaotic series creators involved in decryption and encryption procedure are the main components of the encryption method. It is in charge of understanding the image encryption method. It is executed by 2 chaotic mappings; hence it is named a double chaotic digital image encryption scheme, and other components are mostly involved encryption, decryption, and transmission modules.

3.6. Biometric recognition using SCG-BPNN model

At the cloud server side, the decryption process followed by the reconstruction process takes place to get back the original fingerprint image, which is then fed into the SCG-BPNN model for authentication purposes. BP is a multilayer FFNN, which is based on error inverse propagation method [21]. Based on incomplete statistics, 80–90% of the NN modules are utilized via persons accept BP network or few forms of modification. It contains weight correction among neurons, forward calculation, calculation of the total mean squared error, and feedback calculation of local gradient, (Eq. (10)). A sigmoidal (Eq. (11)) function is considered as the transfer function, as given in the following:

$$E_{AV} = \frac{1}{2N}\sum_{j=1}^{N}\sum_{j\in c}^{N} e_j^2(n) \tag{10}$$

$$f(x) = \frac{1}{1+e^{-ex}} \tag{11}$$

Where, N indicates the number of instances and c denotes the set of entire output units. For the effective training process of the BPNN model, the SCG technique is employed. The SCG method is depending upon conjugate direction, however, this method doesn't execute a line search at every round varying from another conjugate gradient method that needs a line search at every round to make the system computation costly. SCG was implemented for avoiding time consuming line search [22]. It could train other networks as its net input; transfer function and weight have derived function. In SCG method, the step size is an operation of quadratic estimate of the error functions that creates it strong and autonomous of user determined variables. The step size is approximating by various methods. The second order term is estimated by,

$$s_k^- = \frac{E'(\overline{w}+\sigma_k\overline{p}_k) - E'(\overline{w}_k)}{\sigma_k} + \lambda_k\overline{p}_k \tag{12}$$

where, λ_k denotes scalar and altered every time based on sign of δ_k. The step size is given as follows,

$$\alpha_k = \frac{\mu_k}{\delta_k} = \frac{-\overline{p}_j^T E'_{qw}(\overline{y}_1)}{\overline{p}_j^T E''(\overline{w})\overline{p}_j} \tag{13}$$

where W denotes weight vector in space $R^n, E(W)$ indicates global error function, $E'(\overline{w})$ represents gradient of error, $E'_{qw}(\overline{y}_1)$ denotes quadratic approximation of error function, $\overline{p}_1, \overline{p}_2 \ldots \overline{p}_k$ indicates collection of non-zero weight vectors, and λ_k represents upgraded thus,

$$\overline{\lambda}_k = 2\left(\lambda_k - \frac{\delta_k}{|p_k^-|^2}\right) \tag{14}$$

If $\Delta_k > 0.75$, then $\lambda_k = \lambda_k/4$

If $\Delta_k < 0.25$, then $\lambda_k = \lambda_k + \frac{\delta_k(1-\Delta_k)}{|p_k^-|^2}$Where, Δ_k denotes comparison variable and as follows,

$$\Delta_k = 2\delta_k[E(\overline{w}) - E(\overline{w}+\alpha_k\overline{p}_k)] \,/\, \mu_k^2 \tag{15}$$

4. Performance validation

This section validates the performance analysis of the PPS-BAS model. Fig. 2 shows some of the sample eye retina and fingerprint images used for experimentation. Some of the sample processes involved in the presented model is provided in Appendix. A sample visualization results analysis of the PPS-BAS model on sample test images is given in Table 1. The first column in the table indicates the cover eye retina image and the second column shows the secret fingerprint image. Besides, the encrypted image is displayed in column and the decrypted fingerprint image is depicted in last column. The figures showcased that the encrypted image does not reveal information about the secret image and the reconstructed image quality of the decrypted image is high.

A brief comparison study of the proposed PPS-BAS model with other methods interms of MSE and PSNR in Table 2. Fig. 3 demonstrates the MSE examination of the PPS-BAS model with other techniques under different images. The proposed PPS-BAS technique has accomplished superior performance with the minimum MSE values. For instance, on

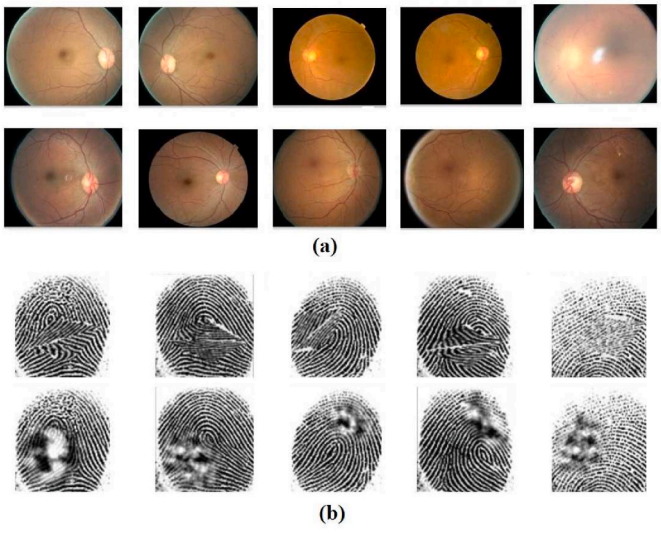


Fig. 2. Sample Images a) Eye Retina b) Fingerprint.

Table 1
Visualization of Proposed PPS-BAS method on Sample Images.

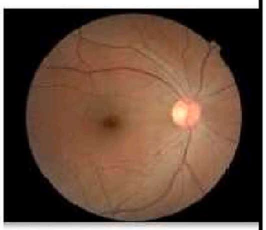
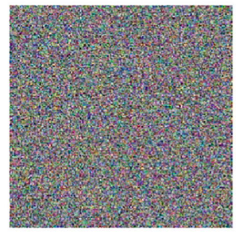
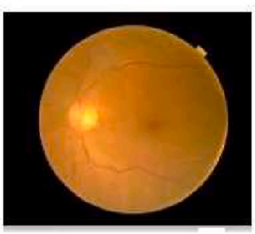
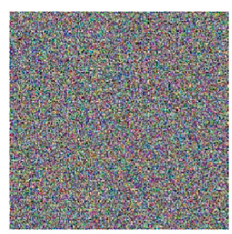
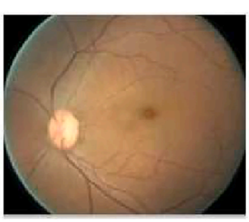
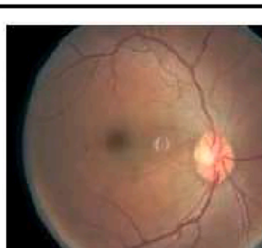
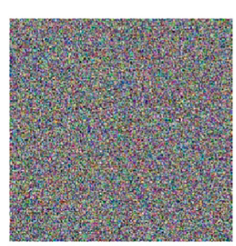
Cover Images	Secret Images	Encrypted Images	Decrypted Images
			
			
			
			
			

Table 2
MSE and PSNR analysis of Proposed PPS-BAS Method.

Test Images	PPS-BAS		DLCM-WOA		DLCM-GWO		DLCM-PSO	
	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
Image_1	0.090	58.59	0.176	55.68	0.298	53.39	1.679	45.88
Image_2	0.123	57.23	0.187	55.41	0.309	53.23	2.321	44.47
Image_3	0.098	58.22	0.256	54.05	0.267	53.87	2.690	43.83
Image_4	0.078	59.21	0.221	54.69	0.209	54.93	2.124	44.86
Image_5	0.105	57.92	0.198	55.16	0.266	53.88	2.569	44.03

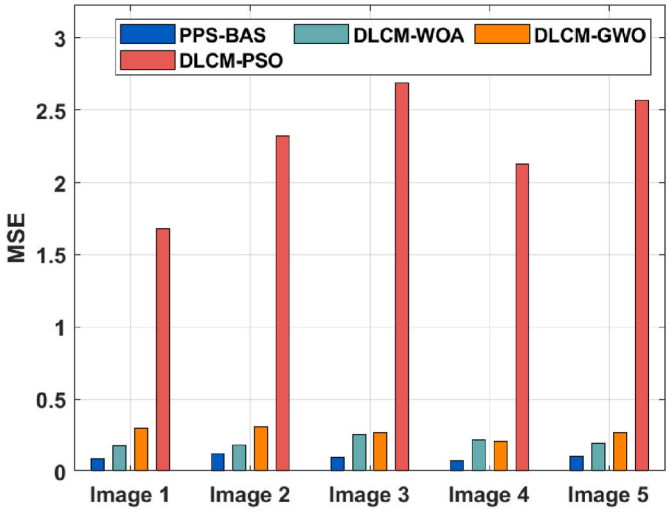


Fig. 3. MSE analysis of PPS-BAS model with existing methods.

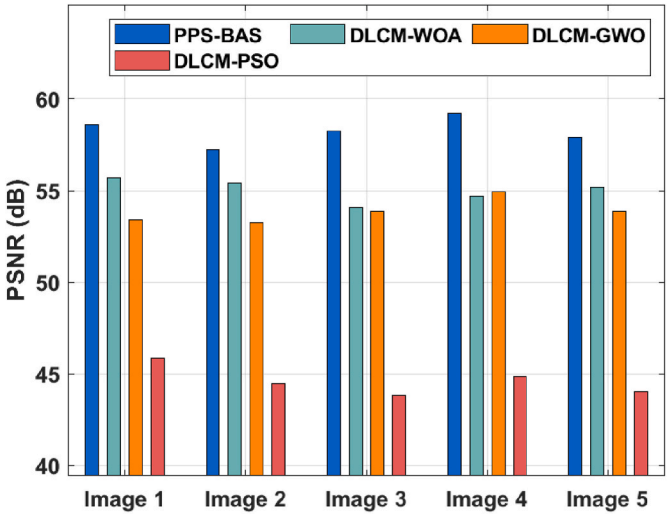


Fig. 4. PSNR analysis of PPS-BAS model with existing methods.

test image_1, the proposed PPS-BAS model has offered least MSE of 0.090 whereas the DLCM-WOA, DLCM-GWO, and DLCM-PSO algorithms have obtained a higher CT of 0.176, 0.298, and 1.679 respectively. Eventually, on test image_3, the presented PPS-BAS technique has offered minimum MSE of 0.098 whereas the DLCM-WOA, DLCM-GWO, and DLCM-PSO methodologies have obtained a superior CT of 0.256, 0.267, and 2.690 correspondingly. Meanwhile, on test image_5, the projected PPS-BAS model has offered least MSE of 0.105 whereas the DLCM-WOA, DLCM-GWO, and DLCM-PSO approaches have obtained a maximum CT of 0.198, 0.266, and 2.569 correspondingly.

Fig. 4 exhibits the PSNR investigation of the PPS-BAS method with existing approaches under different images. The figure demonstrated that the proposed PPS-BAS model has accomplished superior performance with the minimum PSNR values. For instance, on test image_1, the proposed PPS-BAS technique has gained better performance with the PSNR of 58.59 dB whereas the DLCM-WOA, DLCM-GWO, and DLCM-PSO algorithms have demonstrated a minimum PSNR of 55.68 dB, 53.39 dB, and 45.88 dB correspondingly. Simultaneously, on test image_3, the proposed PPS-BAS approach has gained better performance with the PSNR of 58.22 dB whereas the DLCM-WOA, DLCM-GWO, and DLCM-PSO algorithms have demonstrated a lesser PSNR of 54.05 dB, 53.87 dB, and 43.83 dB respectively. Concurrently, on test image_5, the PPS-BAS technique has gained optimal performance with the PSNR of 57.92 dB whereas the DLCM-WOA, DLCM-GWO, and DLCM-PSO algorithms have demonstrated a reduced PSNR of 55.16 dB, 53.88 dB, and 44.03 dB correspondingly.

Table 3 and Fig. 5 demonstrate the CC analysis of the proposed model under distinct test images. From the obtained result, it is exhibited that the PPS-BAS technique has achieved superior performance with the maximum CC value over the other existing models. For instance, on test image_1, the proposed PPS-BAS technqiue has gained better performance with the CC of 0.998 whereas the DLCM-WOA, DLCM-GWO, and DLCM-PSO algorithms have portrayed a reduced CC of 0.994, 0.992, and 0.986 respectively. Simultaneously, on test image_3, the proposed PPS-BAS model has gained better performance with the CC of 0.995 whereas the DLCM-WOA, DLCM-GWO, and DLCM-PSO algorithms have demonstrated a lesser CC of 0.992, 0.989, and 0.984 respectively. Concurrently, on test image_5, the PPS-BAS model has gained better performance with the CC of 0.995 whereas the DLCM-WOA, DLCM-GWO, and DLCM-PSO algorithms have demonstrated a minimum CC of 0.991, 0.990, and 0.982 respectively.

Table 4 and Fig. 6 examine the computation time (CT) analysis of the PPS-BAS model with other approaches. The results demonstrated that the proposed PPS-BAS model has achieved effectual outcome with minimal CT. For instance, on test image_1, the PPA-BAS model has demonstrated lower CT of 1.291s whereas the DLCM-WOA, DLCM-GWO, and DLCM-PSO algorithms have obtained a higher CT of 1.717s,

Table 3
Result Analysis of Proposed PPS-BAS Method in terms of CC.

Test Images	PPS-BAS	DLCM-WOA	DLCM-GWO	DLCM-PSO
Image_1	0.998	0.994	0.992	0.986
Image_2	0.996	0.993	0.992	0.989
Image_3	0.995	0.992	0.989	0.984
Image_4	0.996	0.994	0.987	0.983
Image_5	0.995	0.991	0.990	0.982

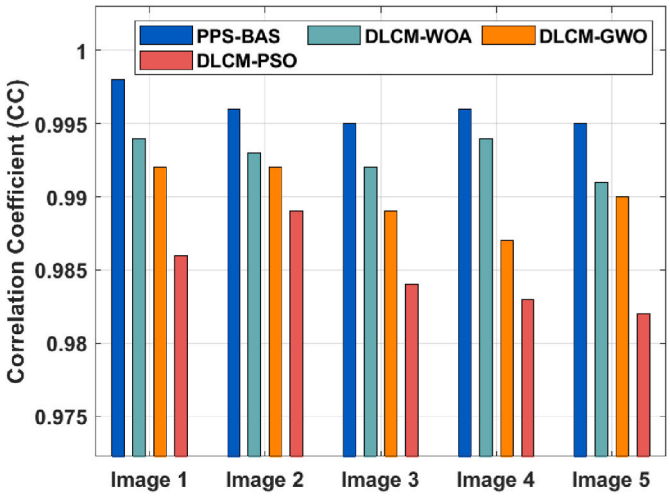


Fig. 5. CC analysis of PPS-BAS model with existing methods.

Table 4
Result Analysis of Proposed PPS-BAS Method with Existing Methods in terms of Computation Time (s).

Test Images	PPS-BAS	DLCM-WOA	DLCM-GWO	DLCM-PSO
Image_1	1.291	1.717	2.202	2.924
Image_2	1.382	1.547	1.879	2.355
Image_3	1.641	1.871	2.022	2.445
Image_4	1.217	1.745	2.297	2.256
Image_5	1.309	1.819	2.012	2.254

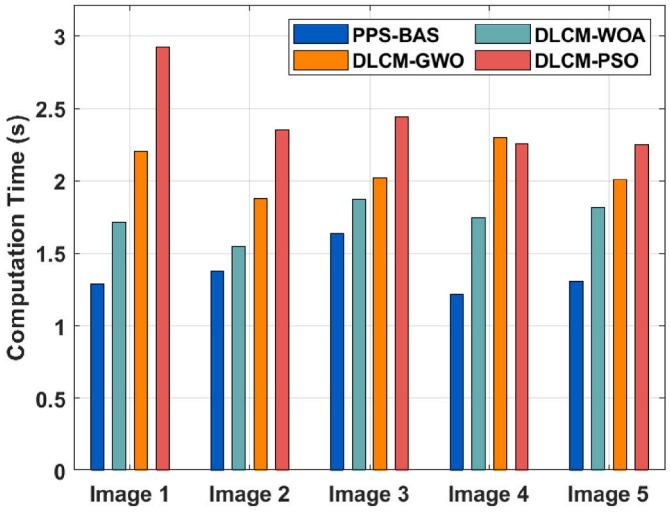


Fig. 6. CT analysis of PPS-BAS model with existing methods.

Table 5
Result Analysis of Proposed PPS-BAS Method with Existing Methods in terms of Recognition Rate (%).

Methods	PPS-BAS	KELM	ELM	SVM
Recognition Rate	96.78	95.98	93.21	92.07

2.202s, and 2.924s correspondingly. Besides, on test image_3, the PPA-BAS method has outperformed lower CT of 1.641s whereas the DLCM-WOA, DLCM-GWO, and DLCM-PSO algorithms have obtained a higher CT of 1.871s, 2.202s, and 2.445s respectively. At last, on test image_5, the PPA-BAS approach has demonstrated lower CT of 1.309s whereas the DLCM-WOA, DLCM-GWO, and DLCM-PSO techniques have obtained a higher CT of 1.819s, 2.202s, and 2.254s correspondingly.

Finally, a biometric recognition rate analysis of the proposed PPS-BAS model with existing methods takes place in Table 5. From the resultant values, it is evident that the SVM model has accomplished insignificant outcomes with the least recognition rate of 92.07%. At the same time, the ELM model has gained slightly enhanced performance with a recognition rate of 93.21% whereas further increased outcomes are offered by the KELM model with a recognition rate of 95.08%. However, the proposed PPS-BAS model has accomplished superior results with a recognition rate of 96.78%.

From the above-mentioned tables and figures, it is evident that the PPS-BAS model not only achieves improved security but also accomplishes maximum recognition performance. Therefore, it can be employed as an effective biometric authentication scheme for CC environment.

5. Conclusion

This paper has designed a novel PPS-BAS technique for effective biometric authentication in the CC platform. The proposed PPS-BAS model intends to hide the fingerprints image (secret image) into the eye retina image and then transmits the encrypted stego image into the cloud server. The proposed PPS-BAM model involves different processes such as color channel separation, multi-level DWT based transformation, CPIO based optimal pixel selection, Q-learning based minutiae extraction, DLCM based encryption, and SCG-BPNN based biometric recognition. For examining the betterment of the proposed PPS-BAS model, a series of simulations take place on benchmark test images and investigated the outcomes interms of different measures. The comprehensive comparison study validated the enhanced outcomes of the PPS-BAS technique compared to the recent state of art biometric authentication systems. Therefore, the PPS-BAS model can be employed as an effective biometric authentication tool. In future, the presented model can be enhanced by the use of multiple biometric based authentication system in real time applications.

CRediT authorship contribution statement

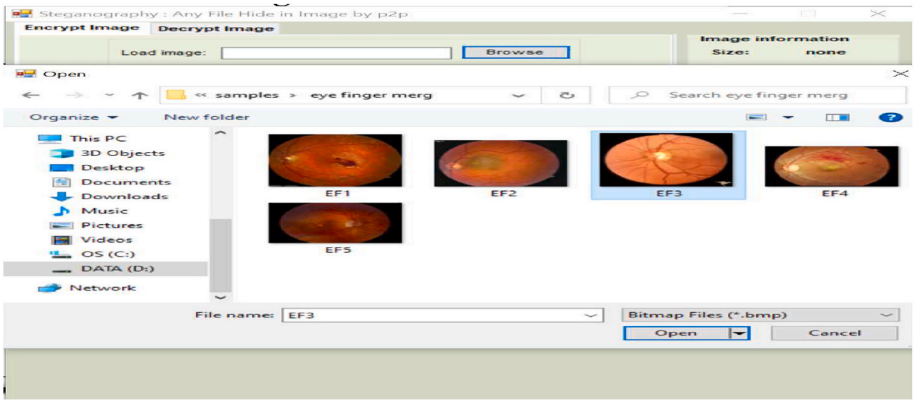
D. Prabhu: Conceptualization, Methodology, Software, Validation, Formal analysis, Investigation, Resources, Data curation, Writing – original draft, Writing – review & editing. **S. Vijay Bhanu:** Software, Investigation, Resources, Writing – review & editing, Visualization, Supervision, Project administration. **S. Suthir:** Software, Investigation, Resources, Supervision.

Declaration of competing interest

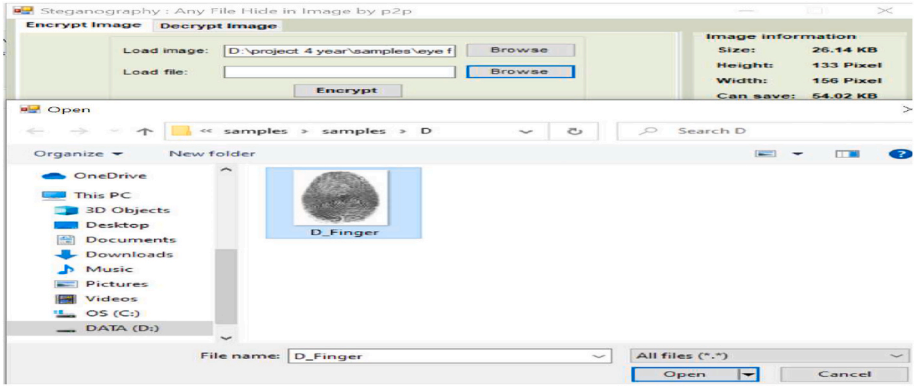
The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix

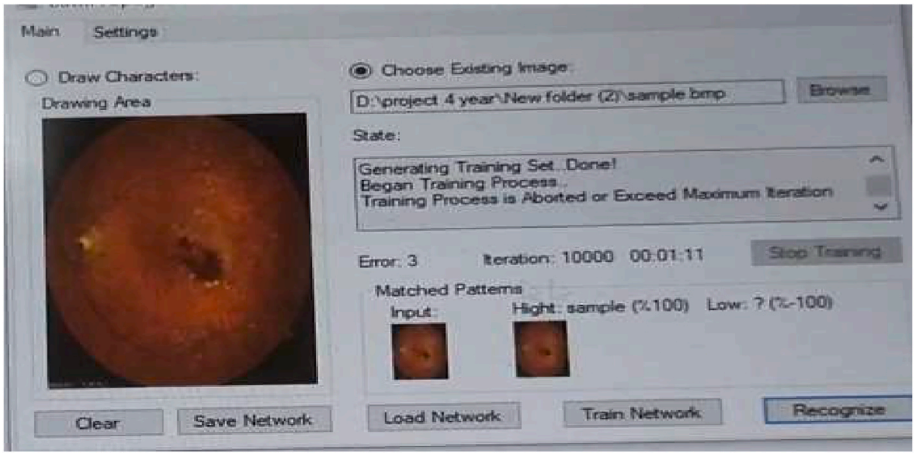
Load Cover Image.



Select Secret Image.



Testing Process.



References

[1] S. Kumar, S.K. Singh, A.K. Singh, S. Tiwari, R.S. Singh, Privacy preserving security using biometrics in cloud computing, Multimed. Tool. Appl. 77 (9) (2018) 11017–11039.

[2] A.K. Jain, A.A. Ross, K. Nandakumar, Introduction to Biometrics, Springer Science & Business Media, 2011.

[3] I. McAteer, A. Ibrahim, G. Zheng, W. Yang, C. Valli, Integration of biometrics and steganography: a comprehensive review, Technologies 7 (2) (2019) 34.

[4] W. Meng, D.S. Wong, S. Furnell, J. Zhou, Surveying the development of biometric user authentication on mobile phones, IEEE Communications Surveys & Tutorials 17 (3) (2014) 1268–1293.

[5] I. Marqués, M. Graña, Image security and biometrics: a review, in: International Conference on *Hybrid Artificial Intelligence Systems*, Springer, Berlin, Heidelberg, 2012, March, pp. 436–447.
[6] Loh, J.C., Poh, G.S., Ying, J.H., Xu, J., Lim, H.W., Pan, J. and Wong, W., PBio: Enabling Cross-Organizational Biometric Authentication Service through Secure Sharing of Biometric Templates.
[7] S. Hillman, Physical Security 101: Evolving 'defense in Depth', InTech Magazine, May/June 2011.
[8] K. Venkatraman, K. Geetha, Dynamic virtual cluster cloud security using hybrid steganographic image authentication algorithm, Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije 60 (3) (2019) 314–321.
[9] I.M. Khudher, LSB steganography strengthen footprint biometric template, E. Eur. J. Enterprise Technol. 1 (9) (2021) 109.
[10] T. Sudhakar, M. Gavrilova, Cancelable biometrics using deep learning as a cloud service, IEEE Access 8 (2020) 112932–112943.
[11] I. Banerjee, S. Bhattacharyya, S. Mukherjee, G. Sanyal, Biometric steganography using face geometry, in: TENCON 2014-2014 IEEE Region 10 Conference, IEEE, 2014, October, pp. 1–6.
[12] S. Das, K. Muhammad, S. Bakshi, I. Mukherjee, P.K. Sa, A.K. Sangaiah, A. Bruno, Lip biometric template security framework using spatial steganography, Pattern Recogn. Lett. 126 (2019) 102–110.
[13] Z.N.J. AL-Kateeb, M.R.J.M. AL-Bazaz, Steganography in colored images based on biometrics, Tikrit Journal of Pure Science 24 (3) (2019) 111–117.
[14] S.Y. Kayode, A.S. Olaniyi, A.M. Olaolu, A.N. Babatunde, Development of eye retina biometric template security using steganography, Comput. Inf. Syst. 22 (3) (2018).
[15] O.C. Abikoye, U.A. Ojo, J.B. Awotunde, R.O. Ogundokun, A safe and secured eye retina template using steganography and cryptography, Multimed. Tool. Appl. 79 (31) (2020) 23483–23506.
[16] K. Atighehchi, L. Ghammam, M. Barbier, C. Rosenberger, GREYC-Hashing: combining biometrics and secret for enhancing the security of protected templates, Future Generat. Comput. Syst. 101 (2019) 819–830.
[17] Ambika, R.L. Biradar, V. Burkpalli, Encryption-based steganography of images by multiobjective whale optimal pixel selection, Int. J. Comput. Appl. (2019) 1–10.
[18] H. Alazzam, A. Sharieh, K.E. Sabri, A feature selection algorithm for intrusion detection system based on pigeon inspired optimizer, Expert Syst. Appl. 148 (2020), 113249.
[19] S. Tiwari, N. Sharma, Q-Learning approach for minutiae extraction from fingerprint image, Procedia Technology 6 (2012) 82–89.
[20] H. Pan, Y. Lei, C. Jian, Research on digital image encryption algorithm based on double logistic chaotic map, EURASIP Journal on Image and Video Processing 2018 (1) (2018) 1–10.
[21] J. Yan, Z. Xu, Y. Yu, H. Xu, K. Gao, Application of a hybrid optimized BP network model to estimate water quality parameters of Beihai Lake in Beijing, Appl. Sci. 9 (9) (2019) 1863.
[22] L. Babani, S. Jadhav, B. Chaudhari, Scaled conjugate gradient based adaptive ANN control for SVM-DTC induction motor drive, in: IFIP International Conference on *Artificial Intelligence Applications and Innovations*, Springer, Cham, 2016, September, pp. 384–395.

Mr. D. Prabhu (Prabhu Dorai) received B.E degree in EEE from Annamalai University, Annamalai Nagar, Chidambaram, Tamil Nādu in 2007. M.E Degree in CSE from Annamalai University, Annamalai Nagar, Chidambaram, Tamil Nādu in 2009. He is currently doing Ph.D. degree at the Department of Computer Science and Engineering, Annamalai University, Annamalai Nagar, Chidambaram, Tamil Nādu, India. Also working as Assistant Professor in Loyola Institute Of Technology. His research interests include Cloud Computing, Cyber Security, Share Creation, Signcryption, Optimal key generation, Email: dprabhume@gmail.com Ph.No. 9566092218

Dr. S.Vijay Bhanu (Vijay Bhanu Srinivasan) His Qualification is M.E., M.B.A., P.G. Dip. Mark. Mgmt. Ph.D. He is currently working as Research Supervisor in Department of Computer Science and Engineering, Annamalai University, Annamalai Nagar, Chidambaram, Tamil Nādu, India. His research interests include Computer Networks, Network Security and Cloud Computing, Email: svbhanu22@gmail.com, Contact number 9843133883

Dr. S. Suthir (Suthir Sriram) received B.Tech degree in IT from Anna University, Chennai, Tamil Nādu. M.Tech Degree in IT from Sathyabama University, Chennai, Tamil Nādu. Ph.D degree in CSE from MS University, Tamil Nadu, India. He is currently working as Research Co- Supervisor at the Department of Computer Science and Engineering, Annamalai University, Annamalai Nagar, Chidambaram, Tamil Nādu, India. His research interests include Artificial Intelligence, Machine Learning and Cloud Computing. Email: suthirsriram@gmail.com, Ph.No. 9944042932