Steganography is the science of hiding secret data inside another data type as image and text. This data is known as carrier data; it lets people interconnect secretly. This suggested paper aims to design a Steganography Biometric Imaging System (SBIS). The system is constructed in a hybridization manner between image processing, steganography, and artificial intelligence techniques. During image processing techniques the system receives RGB foot-tip images and preprocesses the images to get foot-template images. Then a chain code is illustrated for personal information within the foot-template image by Least Significant Bit (LSB). Accurate recognition operation is performed by artificial bee colony optimization (ABC). The automated system was tested on a live-took about ninety RGB foot-tip images known as the cover image and clustered to nine clusters that authorized visual database. The Least Significant Bit method transforms the foot template to a stego image and is stored on a stego visual database for further use. Features database was constructed for each stego footprint template. This step converts the image to quantities data and stored in an Excel feature database file. The quantities data was used at the recognition stage to produce either a notification of rejection or acceptance. At the acceptance choice, the corresponding stego foot-tip template occurrence was retrieved, it is corresponding individual data were extracted and cluster position on the stego template visual database. Indeed, the foot-tip template is displayed. The suggested work consequence is affected by the optimum feature selection via the artificial bee colony optimization usage and clustering, which declined the complication and subsequently raised the recognition rate to 93.65 %. This rate competes out the technique over others' techniques in the field of biometric recognition

Keywords: steganography, foot-tip template, hybridization, stego image, cover image, clustering, biometrics

UDC 004
DOI: 10.15587/1729-4061.2021.225371

LSB STEGANOGRAPHY STRENGTHEN FOOTPRINT BIOMETRIC TEMPLATE

Israa Mohammed Khudher
PhD, Assistant Professor,
Head of Department
Department of Computer Science
College of Education for Pure Sciences
University of Mosul
Alsediq Queue str., 213,
House No. 803, Mosul, Iraq
E-mail: israa.alhamdani@uomosul.edu.iq

Received date 04.01.2020
Accepted date 04.02.2021
Published date 26.02.2021

1. Introduction

The progress of communication technologies mainly the Internet supports the transfer of vast data in minimum time. This fast communication capability requires fast data preparation, which requires securing against unauthorized access. The need for data security is thus an important concern for communication applications. The two major techniques used for data security are encryption and steganography. The real data will be kept hidden inside a cover item. The cover item or medium (digital image, digital audio, network protocol, etc.) can differ based on the application. The human brain acknowledges and orders objects, individuals, or places in an effective, rapid, and easy manner. Since the recognition method takes place so flexible and fast, it is hard to translate this behavior into a laptop algorithm as best as the human being [1]. The computerized system is required and reproduces improved security values even with the practical limits, but a waste of individuality theft by the criminals' hints at risks in the society [1, 2]. Certainly, biometrics is a sensitive record and therefore must be properly protected, to ensure their confidentiality and to maintain the biometric system. There exist approaches that could be used to enhance the sanctuary of biometric information by applying the steganography technique biometric. The system can enhance user comfort and boost security; it is also protected from more than a few types of dangers [3, 4]. The steganography system requires embedding and extracting information. The central advantage of image steganography is the image within which the secret is determined does not interest the consideration of an attacker. During the embedding process image steganography usually deals with preserving the visible quality of an image and encoding a covert message inside it to construct a stego image [5]. In the extracting process, the hidden message was extracted based on the stego image with the flexible biometric to extract [5].

Foot-tip recognition draws a lot of studies from many branches such as digital image processing, deep learning, big data, forensic studying, biomedical. This study is very important for major problems that affect the industries such as visual observation. Also, it is important at checkpoints to accurately identify fraudsters and terrorists, and with the increase in fraud and impersonation nowadays. Security on the other hand represented by steganography manner is very important in biometric recognition systems. Various attacks portend the privacy of whole biometric applications and trial the current anti-deceiving methods. Recently, with the leak of biometrics data nowadays, confidentiality concerns are increasing. Some data about the person's individuality/age/name may be decoded in their images. Research on visible steganography to protect users privations on saved biometrics category are crucial for addressing public concern on privations.

Recently, swarm intelligent optimization merged with another technique. A solution to the problems for both the manufacturing and the technical world has been offered. The perfect results are shown in real-world optimization problems such as flow scheduling industrial establishment. As train scheduling and booking schedule, satellite network project and strategies to clear up the trouble of city garbage collection to minimize the total cost. Also, swarm intelligence solved problems in the technical world such as physics, image processing, biology and so. Indeed in practical terms, the results obtained from the study gave that they add improvements to this type of research by reducing the complications in the time consumed and cost directions. Increasing the privacy of information and preserving it from the abusers and the possibility of using it in transmission operations over networks.

2. Literature review and problem statement

In this section, a brief discussion about the traditional footprint system and approaches will be reviewed due to the lack of artificial style in this branch of biometric. The paper [6] evaluates the recognition rate to 85 %. This rate was based on the peak and mass of a person from the size of the foot tip by the bits of help of the physical science laws. However, there was an unresolved issue related to this study it was the features calculated the reason that is the standing position. Their values may be changed through gait, also it is difficult to determine each of the features under dynamic conditions. The paper [7] presents a precision of 12.0 % for FRR and 1.0 % for FAR. The attributes of the core of foot stress were gained with sensors. But there were unresolved issues related to the use of a small set of participants. The reason for that is that they were from one term and disregards age. The study [8] presents experimental accuracy of about 92 %. The study used the person's walking and stepping category. But this paper shows unresolved problems related to the recognition rate, the reason is that it is inversely proportionate to the visual database size. When the size increases, the recognition rate decreases and vice versa. In [9], the whole recognized results illustrated a 92.80 % rate, shown that the geometric features were extracted from a foot shape and fuzzy neural networks. Despite the perfect experimental results, there exist unresolved issues related to time-consuming and complex computation requirements related to the fuzzy neural networks. The paper [10] presents reasonable results, it suggests using a Discrete Wavelet Transform with a steganography scheme based on the fingerprint (i. e. minutia). However, there was an unresolved issue related to making relevant research impractical due to the DWT complexity. In [11], the result produced approximately 90.56 %. The paper showed the use of deep learning by a convolutional neural network, which was applied on a sixty-five footprint dataset. But, there were unresolved issues related to the use of a few datasets. The reason for that is the objective difficulty associated with fewer participants. In [12], perfect recognition results with the least error were presented. This study showed a footprint biometric recognition based on fuzzy logic and the neural network. Seven attributes set for footprint were defined. Despite the perfect results, there is a related unresolved issue that the method has a boring process for important data. Due to that, the fuzzy scheme depends on a single element so that it has a problem when it is used with vast data. The paper [13] presents a hundred percentage outcome produced from robustness merged techniques based on intelligent image processing via ant swarm optimization and image analysis techniques to recognize human footprint. The related unresolved issue is the system slowness because it depends on ant swarm optimization for recognition which is slow for convergence to the ideal solution.

To overcome the difficulties and limitations from the previous discussion in the related works. All this suggests that it is advisable to conduct a study on foot-tip with significant, easy, and accurate results. So that a decision to create the proposed study is performed. The suggested system exceeds the previous limitations. It is based on bee swarm optimization that has the following abilities. It uses fewer control factors, its speedy convergence to the most satisfying solution. Also, the results reflect the character of its optimization, which chooses the superlative skills in a small and precise feature set.

3. The aim and objectives of the study

This study aims to design the steganography biometric image system named (SBIS). The system is based on image processing techniques, steganography via LSB, and artificial bee colony procedure. The system technique is to enforce security and to maintain data privacy from unauthorized attack.

To achieve the aim, the following objectives were set:

– to hide the message which it is (name and age) of a person, by LSB in the template biometric foot-tip image (stego image);

– to compute the chain code foot-tip features to construct a feature database;

– to estimate the recognition accuracy of the proposed method by artificial bee colony procedure, as well as the overall system accuracy;

– to extract the hidden data from the template stego image.

4. Materials and methods

4. 1. Image database arrangement method

The automated system was tested on live-took about ninety colored foot tip images collected by a digital scanner [14]. During visual database creation, each ten-foot-tip image per individual with various angles was classified in one cluster. First, the visual database images were preprocessed. The RGB images were transformed to the monochrome scale and the morphology filter (thin) for segmentation operation is performed where the foot tip is isolated. The proposed work had been written in Matlab version (R2018b) language and applied by Intel(R) Core(TM) 1.70 GHz (4 CPUs), ~1.7 GHz. The block diagram in Fig. 1 describes the stages of the proposed work.

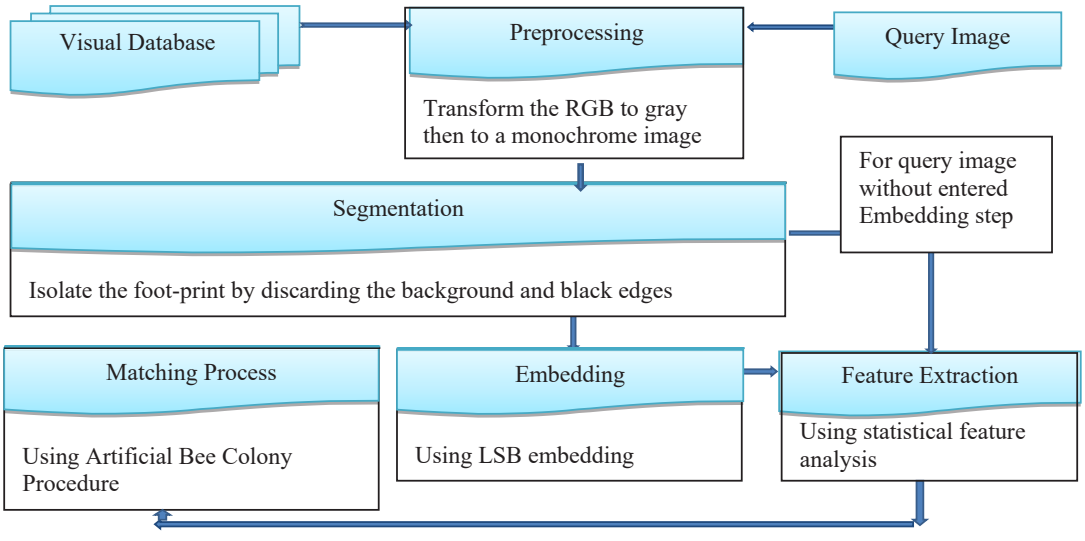

Fig. 1. Block diagram of the proposed work

4. 2. Steganography

Steganography is a Greek phrase that means covered writing. Thus, steganography is used artificially for hiding information, in other words the message as well as the methods to send the data via the cover image. Steganography hides the secret data in an extra file in a way that only the receiver knows the received message. In the olden time, the information was hidden in many ways, but recently the data are transmitted in the form of text or multimedia form over multimedia medium [15, 16]. The types of steganography are text, multimedia that has an image, video, and audio steganography also protocol steganography [17, 18].

4. 2. 1. Image steganography

The four concepts that construct the image steganography are shown in Fig. 2.

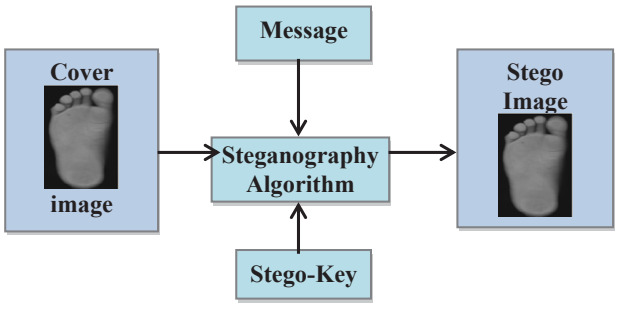

Fig. 2. Steganography concept

They are the cover image, it is the original image used as a carrier for a message. The message could be a simple text or another image. The stego-image is the media that carry the message after hiding it into the cover image. Stego-Key is utilized for embedding and extracting the messages from a stego image [19, 20].

4. 3. Least significant bit method (LSB) [5, 17]

This technique is most commonly used for hiding information. In this strategy, the installing is finished by replacing the least real bits of image pixels with the bits of secret information. In the LSB method, the message is hidden within the least significant bits of the cover mean's digital data. In this paper, the LSB substitution method was used, where the bits of the raw image are replaced with the bits of the secret message.

4. 3. 1. Embedding message pseudo code [21]

The LSB substitution method uses embedding and extraction procedures. It is noticeably hard for the human eye to distinguish between the raw and the embedded image. The standard encryption (embed) and decryption (extraction) for LSB are shown below:

Input: Cover image and Message

Output: Stego image

Begin

Read the cover image; Message=1000011

Convert each character of the cover image from decimal to binary number, e. g. 10000110 10011110 11101111 10010111 10011111

Convert each character of the message to 8 bits

1 0 0 0 0 0 1 1→1 0 0 0 0 0 1 1

Substitute the LSB bit in each byte from the cover image by one bit from the message to be hidden as shown below:

First byte from the Cover Image 10000110

The first bit from the message is 1

After substitution with XOR, the byte will be 10000111

Repeat substitution for all words of the cover image and write the Stego Image

end

4. 3. 1. Extracting message pseudo code [22]

Input: Stego image.

Output: The retrieved image and the message (name).

Read the stego image, calculate the LSB of each pixel of the stego image.

Retrieve bits and convert each 8 bit into character to display the message.

4. 4. Artificial bee colony algorithm

The artificial bee colony (ABC) technique is a commonly known optimization technique that represents the intelligent search behavior of bees. A group of honey bees has been named a swarm, which might successfully complete tasks via cooperation. The colony is similar to a unit and its members

are mutually dependent on each other. The artificial bee colony technique used three kinds of bees. They are the active bees, observer bees, and scout bees. The active bees search for nectar around the food supply, they share the knowledge of the food supply with the observer bees. The food supply with a greater quality (fitness) may be selected by the observer bees than other of lower quality. The scout bees are translated from a few active bees that expired their food place and find new ones. A mathematical model was established to enable bees to adopt compliant or direct employment of food sources.

The artificial bee colony is shown in equation (1) by initializing *NS* food supply, this supply is a vector containing the values to be optimized, that is ranged between *X*max*k*, *X*min*l* limits.

$$Xkl = X\min l + \text{rand}(0, 1)(X\max k - X\min l), \quad (1)$$

for $l=[1, D]$ and $k=[1, NS]$.

The observer bee evaluates the food source taken from all active bees and chooses a food source with a probability value that corresponds to its nectar amount, which is evaluated in equation (2). This probabilistic selection is a roulette wheel selection mechanism.

$$P_i = \frac{fit_i}{\sum_{i=1}^{SN} fit_j}, \quad (2)$$

where fit_i is the fitness value of the i^{th} solution in the swarm. As can be seen, the higher the probability the better the food source selected. The efficiency and easiness of the full process are possible due to the control in decision-making tactics and regular method of self-organization in bee colonies [22].

5. Results of designing the steganography biometric image system

The research results had been arranged into four sections gradually, each output result of the section would be an input to the following one as described below.

5. 1. Embedding data within footprint template

This suggested system hides the name and age of a person as a message within his/her foot template image (cover image) via the (LSB) approach. This step produced the stego image. Fig. 3 shows a sample from the cover and the stego image. A preprocessing procedure was performed to transform the RGB foot-tip image to the intensity scale and at last to the monochrome image. The binary image was denoted after successive morphological operations. Indeed, the foot template was isolated by segmentation operation from the background. Chain code for foot tip template was denoted and its histogram is extracted [23–25] to be used for the next steps.

The person data as name and age is preprocessed by each character conversion from decimal to a binary number, then processed by the Least Significant Bit procedure in the cover image. The stego image is produced now.

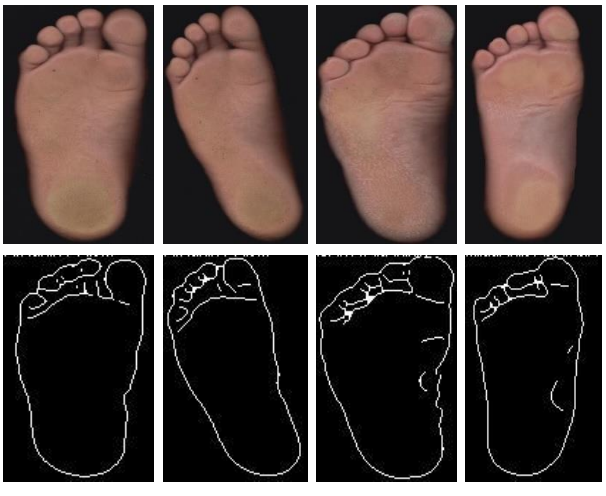

Fig. 3. A sample from the cover and the embedded image

The encryption and decryption operations affect image quality. To ensure quality, we have applied the metrics such as MSE, Structural Similarity Index Measure (SSIM), and Normalized Cross-Correlation. Table 1 shows the mathematical equations for these metrics as shown from (3)–(5). Table 1 records the mathematical equation numbered from (3)–(5) for these metrics.

The smaller the MSE value, the better the image quality. SSIM ranged between 0 and 1, of course, the best value when it reaches value one. NCC value is limited between [–1, 1]. Fig. 4 shows the similarity between the covered and the stego image.

The performance of the steganography operation is measured via the quality difference measure between the cover and the stego image. Their values were calculated, the value of MSE is equal to zero, SSIM is equal to 0.9988, and Norm. Xcor is equal to 1.

Table 1

Metric measures

Accuracy Measure	Equation	Parameter
MSE	$\text{MSE} = \frac{1}{\mu}\sum_{i=1}^{n}\sum_{j=1}^{m}\left(x_{ij} - y_{ij}\right)$ (3)	Where *X* represents the stego image and *Y* denotes the retrieved image, μ denotes the mean [21, 26]
Structural Similarity Index (SSIM)	$\text{SSIM}(x,y) = \frac{(2\mu x\mu y + c1)(2\sigma xy + c2)}{(\mu^2 x + \mu^2 y + c1)(\sigma^2 x + \sigma^2 y + c2)}$ (4)	*X*, *Y* are the cover and stego images. μx, μy are *x*, *y* mean, σ_X^2 and σ_Y^2 are the variance of *x* and *y*, σxy is the co-variance of *x* and *y*, and *c*1, *c*2 are the absolute values for stabilization [5, 26]
Normalized-Cross Correlation (NCC)	$\text{NCC} = \left(\frac{1}{N}\right)\sum_{i=1}^{N}\left((x-\mu x)(y-\mu y)\right)\Big/\sqrt[2]{\sigma(x)\sigma(y)}$ (5)	*x*, *y* is the cover and stego image. μ_x and μ_y are the mean, σx, σy is the variance *of x* and *y* [5]

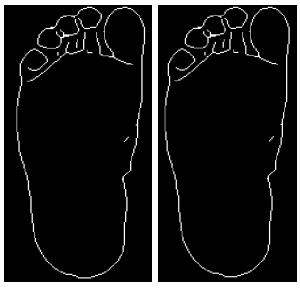

Fig. 4. The stego image (embedded) and the covered image

5. 2. Chain code evaluation

The chain code of the stego template was calculated by truncates of the black portion from the template. When the binary image is obtained, the start point of the code is defined and the chain code was found. The right, left diagonal and vertical directions of the image are calculated. Also, the center angle was found.

5. 3. Recognition techniques

Template stego image features were extracted, these features are shown in Table 3. These features are the Normalized Standard Deviation, entropy, covariance, third central moment as well as the mean of chain code histogram and bwarea. I have used the statistical moments to represent the foot-tip characteristic for their importance in the reduction of memory storage. Also their speed and high precise consequence [27]. The outcome from the feature extraction process is a feature set EXCEL file named "stgfoot-tip.xls" that represents the feature database. Table 2 shows the proposed work features as shown in equation (6)–(9).

A query image is entered into the system, it is preprocessed there, the features were mined online via the system works. These features were compared parallel within the feature database by the artificial bee colony (ABC) algorithm. The artificial bee colony procedure applied feature selection algorithm within foot tip clusters via fitness function calculation with the smallest alteration (min) between query and database features.

Table 2

Features description

Features	Formula		Parameter
Normalized Standard Deviation	$\frac{\sigma(hist(chain))}{\mu(hist(chain))}$	(6)	Where σ denotes the standard deviation and μ denotes the mean [28]
Entropy	$H(X)=-\sum_{i=1}^{n}P(xi)\log_b P(xi)$	(7)	$P(x)$ denotes the image probability [27]
Bwarea of image	bwarea(BW)		Estimate the number of pixels in the monochrome image [27]
Covariance	$\mathrm{cov}(x,y)=\frac{1}{N-1}\sum_{i=1}^{n}(x_i-\mu_x)(y_i-\mu_y)$	(8)	X and Y are image features and μ_x are μ_y their mean [28]
Third-order central moment	$\mu_3=E\left[(X-\mu)^3\right]$	(9)	[27]

5. 4. Extracting data from footprint template

After the recognition operation is performed, the suggested system extracts a message from his/her foot template image (stego image). The extraction is done by displaying the stego image and loads it, then the stego image is transformed into a byte array. From the first byte: transform the lsb into a vector and change them to digit. Change the LSB digit value into a vector of size 8. Change the vector to a byte value and save it in the corresponding index of the created array, then change the array value into a text message. Indeed, the retrieved image and the message (name) are displayed.

6. Recognition evaluation results

The ninety image features database was stored in the "stgfoot-tip.xls" file. A query foot-tip image is entered into the system, after the features extraction process on-line these features are recorded in Table 3, every query feature was compared with the ninety image database features via the (ABC) procedure function.

Table 3

Query features

Img. Name	Norm. Std	Entropy	Covariance	Bwarea of Image	3'rd moment of chain histogram
QTp1	37.02784	4.835546	80.53905	0.721928	1.058607
QTp2	85.23763	2.886259	28.94677	0.881291	2.086411
QTp3	83.43518	3.089991	31.22897	0.970951	2.153216
QTp4	149.2323	4.454545	331.6625	0.721928	2.857176
QTp5	88.88666	3.384365	32.90895	0.970951	1.983012
QTp6	100.7746	4.997991	44.31625	1	1.8647
QTp7	102.3274	5.119448	45.34992	1	1.838154
QTp8	79.31932	5.121223	49.31503	1	1.348677
QTp9	145.3986	10.16327	132.3825	0.790951	1.836609
QTp10	56.31582	5.989065	66.62688	0.8812	1. 036798

The outcome from this step is shown in Table 4.

From Table 4, a required image named QTmplt1 was entered into the system, the occurrence image is (1) and its Cluster is (1) within the database. QTmplt2 was entered into the system, the occurrence image is (10) and its Cluster is (1) within the database and so on. But the shaded rows show the error result from its clusters should be five and six. The efficiency of the (ABC) method shows the acceleration of the consequence in finding the precise indication and compact the respect time that ranged between times (0.0001) to (0.0004) in millisecond recursively. The fitness function value determines the outcome of the system that is represented by the Bestres value. The Bestres value is compared with a corresponding threshold, a positive matching is gained if the Bestres is small, otherwise a negative matching is notified. Where the entry of this table was transformed into a figure as shown in Fig. 5, which represents the positive and two message boxes, the first box has the template footprint, its occurrence, and its corresponding cluster within the visual database. Another box shows the extracted data from the stego template, personal information, as well as his/her age, is then recovered.

The overall system performance was determined in Table 4. It is drawn in Fig. 6, which shows the relation between image number and its cluster.

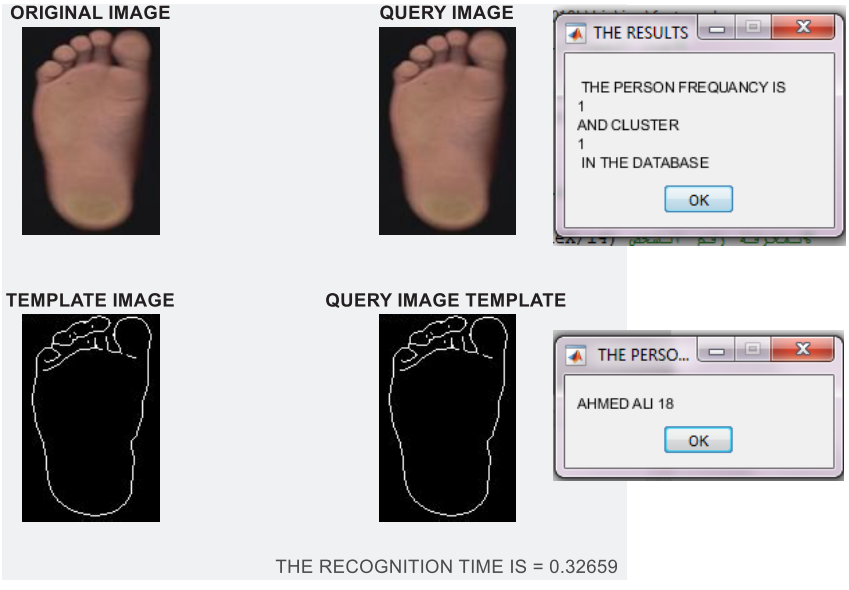

Fig. 5. Outcome results

Table 4

System outcomes

Img. Name	Bestres	Img. Freq. in the DB.	Cluster No.	Elapsed time
QTmplt1	0	1	1	0.0004
QTmplt2	0	10	1	0.0004
QTmplt3	0	13	2	0.0002
QTmplt4	1.3147	21	3	0.0002
QTmplt5	0	33	4	0.0002
QTmplt6	0	42	6	0.0001
QTmplt7	0	52	7	0.0001
QTmplt8	0.0019	61	7	0.0001
QTmplt9	0	82	9	0.0001
QTmplt10	0	83	9	0.0001

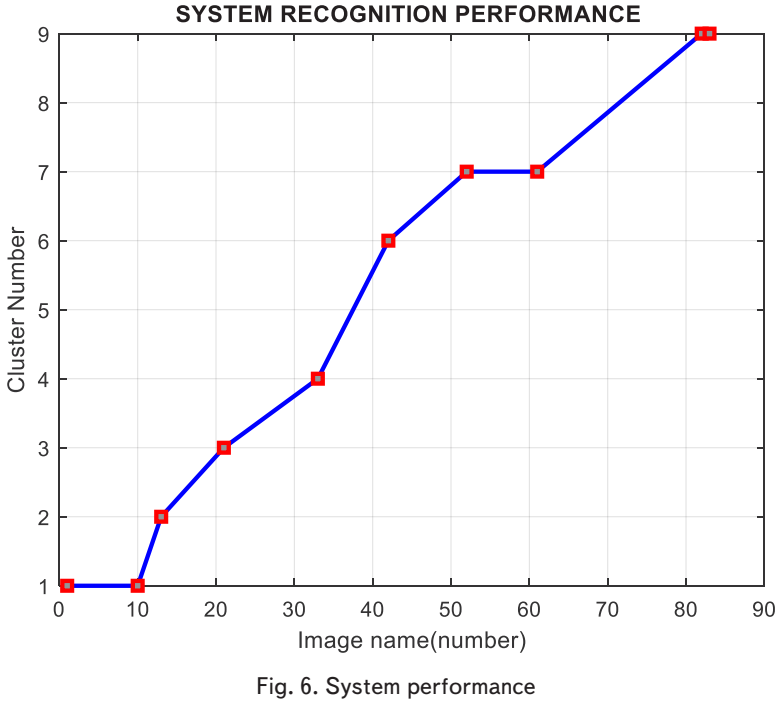

Fig. 6. System performance

The enhancement of the recognition rate shown relates to the database foot-tip image found from the recognition process with its extracted corresponding cluster.

7. System performance

The system performance and enhancement were measured by many metric measures as shown and discussed. For overall system quantitative criteria, we used to calculate the algorithm performance, it is balanced by the F-score that combines precision and recall. It approximates the average of the two when their values are nearer. The function of the F-score is the harmonic average of precision and recall [29], their equations are recorded from (10)–(12) as follows:

$$Recall=Tpos/(Tpos+Fneg), \quad (10)$$

where *Tpos* denotes the appropriate image and *Fneg* denotes the inappropriate image retrieved.

$$Precision=Tpos/(Tpos+Fpos), \quad (11)$$

where *Tpos* denotes the appropriate image and *Fpos* denotes the appropriate false image retrieved:

$$\text{F-score}=2*(Precision*recall)/(Precision+recall). \quad (12)$$

From the collected results in Table 4, the results are evaluated for the overall system as follows:

$$Recall=8/(8+1)=0.88,$$

$$Precision=8/(8+0)=1,$$

$$\text{F-score}=(2*1*0.88)/(1+0.88)=93.63.$$

The recognition rate represented by F-score is equal to 93.63, which reflects excellent results, as well as the perfect accuracy method. Table 5 records the related studies' performance, as well as the proposed work enhancement.

Table 5

Related work comparison

Technique	Performance, %
Fuzzy neural network	90–92.80 [30]
Neural Network	92 [8]
Morphological and statistical features	83.38–89.52 [1]
Modified Sequential Haar Energy Transform (MSHET)	92.37 [31]
The proposed work	93.32

The proposed work reflects reasonable results in comparison with other traditional and intelligent works of foot-tip biometrics. Their performance values ranged from 83.38 to 92.80. I did not use a statistical method such as the Pearson correlation coefficient despite its perfect results in the matching operation. Due to that, it is one of the types of traditional methods, and my study is based on the intelligent approach in the matching operation.

8. Discussion of experimental results

As discussed, the system had been constructed in a hybridization manner between image processing techniques, steganography by least significant bit, and artificial bee colony procedure. To overcome the drawbacks of the three algorithms when they were applied separately and to exploit them sufficiently. Mainly, the artificial bee colony (ABC) algorithm accelerates the solution, as well as records the perfect outcomes. Due to that, ABC is applied to data clusters, which work on a small data set in such a manner of feature selection. The intermediate results were discussed with each section previously, but the main results were obtained as shown in Fig. 5 and the relation diagram discussed in Fig. 6. The recognition outcome over the whole system is calculated by the F-score value that approximates to 93.63, which balances the precision and recall values. The results are reasonable in comparison with other works depending on various techniques shown in Table 5. The performance of this system is based on presentation and obligations, which are stringency, precision, power of authentication, and the probability of usage to distinguish numerous users. Also, decrease the complication aspect of time and the honesty of the solution of this system.

The limitation of this study is the limited size of the database used, an idea for the future is to increase the number of participants with different ages, gender, and resources. The drawback of this work is that the solution for the matching operation may diverge with the artificial bee procedure, so a specific threshold should be selected accurately to get precise results. Also, the artificial bee may only move to nearby food sources. This characteristic may restrict the zones which the bees can move on and may become a drawback of the ABC. A solution to these problems is to accelerate and enhance it, there should be a modification for the ABC such as supervised learning via classification. The stego-message may be lost if we use image operations as an image crop or resize. To solve this problem, we can use other steganography methods. The direction to develop this study by the idea to use multi-biometric features could be obtained.

9. Conclusions

1. Quantitative indicators of research results in embed the message which it is (name and age), by LSB in the foot-tip template image (stego image). LSB procedure was used due to fewer amounts of information required to cover any personal data by interchanging those bits using message bits.

2. Research results in extracts of the personal data by LSB procedure by reading the stego image. Each recovered eight bits illustrated from this procedure were converted specifically into character to construct the message.

3. Extracting important features with an indication of qualitative values produced from chain code foot-tip template image. This stage shows significant results that affect the matching operation efficiently.

4. The quantitative indicators of research results clarified that the system effectiveness was measured in aspects of robustness and efficiency. Robustness is shown in the precise matching between the tested and the visual database images. Efficiency is shown in the form of measures during the steganography procedure, while the other was applied at the end of the recognition operation. The overall efficiency of the system is measured by the F-score measure, which approximates 93.63.

Acknowledgments

The author is appreciative to the University of Mosul to associate this scientific paper. Additionally, big thanks to the volunteers who helped to collect the foot-tip images to construct the visual database.

References

1. Nagwanshi, K. K. (2019). Cyber-Forensic Review of Human Footprint and Gait for Personal Identification. IAENG International Journal of Computer Science, 46 (4), 645–661.
2. McAteer, I., Ibrahim, A., Zheng, G., Yang, W., Valli, C. (2019). Integration of biometrics and steganography: A comprehensive review. Technologies, 7 (2), 34. doi: https://doi.org/10.3390/technologies7020034
3. Kant, C., Nath, R., Chaudhary, S. (2008). Biometrics security using steganography. International Journal of Security, 2 (1), 1–5. Available at: https://www.cscjournals.org/manuscript/Journals/IJS/Volume2/Issue1/IJS-5.pdf
4. Johnson, N. F., Jajodia, S. (1998). Steganalysis of Images Created Using Current Steganography Software. Lecture Notes in Computer Science, 273–289. doi: https://doi.org/10.1007/3-540-49380-8_19
5. Chandran, S., Bhattacharyya, K. (2015). Performance analysis of LSB, DCT, and DWT for digital watermarking application using steganography. 2015 International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO). doi: https://doi.org/10.1109/eesco.2015.7253657
6. Khokher, R., Chandra Singh, R. (2016). Footprint-Based Personal Recognition using Scanning Technique. Indian Journal of Science and Technology, 9 (44). doi: https://doi.org/10.17485/ijst/2016/v9i44/105167
7. Ye, H., Kobashi, S., Hata, Y., Taniguchi, K., Asari, K. (2009). Biometric System by Foot Pressure Change Based on Neural Network. 2009 39th International Symposium on Multiple-Valued Logic. doi: https://doi.org/10.1109/ismvl.2009.16

8. Yun, J., Abowd, G., Woo, W., Ryu, J. (2007). Biometric User Identification with Dynamic Footprint. 2007 Second International Conference on Bio-Inspired Computing: Theories and Applications. doi: https://doi.org/10.1109/bicta.2007.4806456
9. Hashem, K. M., Ghali, F. (2016). Human Identification Using Foot Features. International Journal of Engineering and Manufacturing, 6 (4), 22–31. doi: https://doi.org/10.5815/ijem.2016.04.03
10. Douglas, M., Bailey, K., Leeney, M., Curran, K. (2017). An overview of steganography techniques applied to the protection of biometric data. Multimedia Tools and Applications, 77 (13), 17333–17373. doi: https://doi.org/10.1007/s11042-017-5308-3
11. Keatsamarn, T., Visitsattapongse, S., Pintavirooj, C. (2020). Footprint Pressure-Based Personal Recognition. International Journal of Pharma Medicine and Biological Sciences, 9 (2), 65–69. doi: https://doi.org/10.18178/ijpmbs.9.2.65-69
12. Nagwanshi, K. K., Dubey, S. (2018). Mathematical Modeling of Footprint Based Biometric Recognition. International Journal of Mathematics Trends and Technology, 54 (6), 500–507. doi: https://doi.org/10.14445/22315373/ijmtt-v54p560
13. Ibrahim, Y. I., Alhamdani, I. M. (2019). A hyprid technique for human footprint recognition. International Journal of Electrical and Computer Engineering (IJECE), 9 (5), 4060–4068. doi: https://doi.org/10.11591/ijece.v9i5.pp4060-4068
14. Alhamdani, I. M., Ibrahim, Y. I. (2020). Swarm intelligent hyperdization biometric. Indonesian Journal of Electrical Engineering and Computer Science, 18 (1), 385. doi: https://doi.org/10.11591/ijeecs.v18.i1.pp385-395
15. Kaur, N. I., Kaur, A. (2017). Art of Steganography. International Journal of Advanced Trends in Computer Applications (IJATCA), 4 (2), 30–33.
16. Ali, U. A. M. E., Sohrawordi, M., Uddin, M. P. (2019). A Robust and Secured Image Steganography using LSB and Random Bit Substitution. American Journal of Engineering Research (AJER), 8 (2), 39–44.
17. Mousa, S. M. A. (2017). LSBs Steganography Based on R-Indicator. The Islamic University Gaza, 73. Available at: https://iugspace.iugaza.edu.ps/bitstream/handle/20.500.12358/20075/file_1.pdf?sequence=1&isAllowed=y
18. Cheddad, A. (2009). Steganoflage: A New Image Steganography Algorithm. School of Computing & Intelligent Systems Faculty of Computing & Engineering, University of Ulster. Available at: https://theses.eurasip.org/media/theses/documents/cheddad-abbas-steganoflage-a-new-image-steganography-algorithm_1.pdf
19. Awadh, W. A., Hashim, A. S., Hamoud, A. K. (2019). A Review of Various Steganography Techniques in Cloud Computing. University of Thi-Qar Journal of Science, 7 (1), 113–119. doi: https://doi.org/10.32792/utq/utjsci/vol7/1/19
20. Hussain, Me., Hussain, Mu. (2013). A survey of image steganography techniques. International Journal of Advanced Science and Technology, 54, 113–124.
21. Chitradevi, B., Thinaharan, N., Vasanthi, M. (2017). Data Hiding Using Least Significant Bit Steganography in Digital Images. Statistical Approaches on Multidisciplinary Research, 143–150. Available at: https://zenodo.org/record/262996#.YCEyjHQzaUk
22. Kumar, A., Kumar, D., Jarial, S. K. (2017). A review on artificial bee colony algorithms and their applications to data clustering. Cybernetics and Information Technologies, 17 (3), 3–28. doi: https://doi.org/10.1515/cait-2017-0027
23. Baji, F., Mocanu, M. (2018). Chain Code Approach for Shape based Image Retrieval. Indian Journal of Science and Technology, 11 (3). doi: https://doi.org/10.17485/ijst/2018/v11i3/119998
24. Salem, A.-B. M., Sewisy, A. A., Elyan, U. A. (2005). A vertex chain code approach for image recognition. International Journal on Graphics, vision and Image processing, 5 (3).
25. Govindaraju, V., Shi, Z., Schneider, J. (2003). Feature Extraction Using a Chaincoded Contour Representation of Fingerprint Images. Audio- and Video-Based Biometric Person Authentication, 268–275. doi: https://doi.org/10.1007/3-540-44887-X_32
26. Al-Najjar, Y. A. Y., Soong, D. C. (2012). Comparison of Image Quality Assessment: PSNR, HVS, SSIM, UIQI. International Journal of Scientific & Engineering Research, 3 (3).
27. Gonzalez, R. C., Woods, R. E. (2002). Digital image processing. Prentice-Hall, 793.
28. Ambeth Kumar, V. D., Ramakrishnan, M. (2010). Footprint recognition using modified sequential haar energy transform (MSHET). IJCSI International Journal of Computer Science, 7 (3), 47–51.
29. De Oliveira, I. O., Laroca, R., Menotti, D., Fonseca, K. V. O., Minetto, R. (2019). Vehicle Re-identification: exploring feature fusion using multi-stream convolutional networks. arXiv.org. Available at: https://arxiv.org/pdf/1911.05541.pdf
30. Rusdi, N., Yahya, Z. R., Roslan, N., Azman, W. Z. (2018). Reconstruction of medical images using artificial bee colony algorithm. Mathematical Problems in Engineering. doi: https://doi.org/10.1155/2018/8024762
31. Abuqadumah, M. M. A., Ali, M. A. M., Almisreb, A. A., Durakovic, B. (2019). Deep transfer learning for human identification based on footprint: a comparative study. Periodicals of Engineering and Natural Scinces, 7 (3), 1300–1307. doi: http://dx.doi.org/10.21533/pen.v7i3.733