Research Article

Design and implementation of secure ATM system using machine learning and crypto–stego methodology

Indrajit Das[1] · Shalini Singh[1] · Sonali Gupta[1] · Amogh Banerjee[1] · Md Golam Mohiuddin[1] · Shubham Tiwary[1]

© Springer Nature Switzerland AG 2019

Abstract
The crucial prerequisite in these days is to get rid of various forms of attacks. Nowadays, for financial transaction, automated teller machines (ATMs) are the mostly used gadgets in which personal identification numbers (PINs) are generally used for transaction. But personal identification numbers (PINs) are not secured from many types of threats (spoofing, eavesdropping, man-in-the middle attack etc.), which can affect the security of the confidential and private information. Due to this reason, different biometric systems gain popularity worldwide for their behavioral and physiological features. However, the current biometric systems, for example, iris, palm, faces fingerprints or voice are extremely complex to use and have different disadvantages. In order to overcome these disadvantages a new concept has been introduced in this paper, for authentication in ATM a finger vein authentication method and for information (finger vein image) transfer a combined approach of steganography and cryptography scheme is used. Finger vein authentication system is implemented by the combination of machine learning and image processing procedure. For the purpose of information (finger vein image) transfer, a combined approach of light-weight cryptography and steganography (variable MSB–LSB algorithm) has been proposed. For finger-vein authentication system, the experiment shows that in proposed classification procedure (one-versus-one and one-versus-all) the average recognition accuracy is 98.75% and 97.92% and the execution time is 0.168 s and 0.187 s respectively. For transferring finger vein image, light-weight cryptography and variable MSB–LSB algorithm are proposed, because light weight cryptography is superior to traditional cryptography in terms of time consumption and variable MSB–LSB algorithm is superior to simple LSB in different aspects such as randomness, security and amount of space consumed.

Keywords Finger vein detection · Contrast limited adaptive histogram equalization · Gabor filter · Support vector machine · Fractal dimension · Lacunae · Variable MSB–LSB algorithm · Light weight cryptography · Automated teller machines

1 Introduction

With an increase in technology, the need for the security of individual's information is also becoming a major concern. Automated teller machines (ATMs) are a common gadget which is highly used by humans to perform financial and banking related transactions. It has become worldwide famous within the public due to its features like accessibility and user-friendliness. Access of private information in ATM is possible by using passwords or personal identification numbers (PINs) as they are easy to use, but still it's defenseless against the various types of attack (Phishing attack, Spoofing attack, Sniffing etc.). So as an alternative method i.e. biometrics are being employed. Biometrics utilizes human physiological or behavioral features for individual authentication and provides higher concern to information security, due to which it is being emerged as one of the most popular alternatives to the traditional password or PIN based authentication systems. But some biometrics authentication system like

✉ Indrajit Das, indrajitdas1979@hotmail.com | [1]Meghnad Saha Institute of Technology, Kolkata, India.

SN Applied Sciences (2019) 1:976 | https://doi.org/10.1007/s42452-019-0988-0

Received: 21 May 2019 / Accepted: 25 July 2019 / Published online: 3 August 2019

fingerprints, iris, faces, voice or palm have several disadvantages for example the patterns can be forged due to their physical appearance thus making it unprotected against attackers.

Unique finger print authentication also has few disadvantages. As, it can smoothly be ripped off by utilizing a fake finger and can be unrecognized due to presence of injuries or dirts in finger. Since Iris recognition relies on the intensity of the light, its recognition rate is less accurate [1]. The light condition, expression of the face and camera position etc. makes issue in the face identification process. Another biometric process is voice recognition which has some issues like spoofing attack by recorded voice. Henceforth, more secure biometric authentication framework is required. Finger vein recognition strategy is a solution for it.

The primary favorable thing of utilizing finger vein patterns for safety and reliability purpose is that it lies under the skin and is unique. It demonstrates a couple of other advantages and these include:

- It gives extraordinary distinction between individuals as it incorporates indistinguishable twins and its characteristic is static.
- Its patterns can't be effectively duplicated, harmed, or hidden like fingerprints, iris, faces, voice or palm.
- Other fingers can be utilized as an option for authentication, if one finger of individual gets injured due to accident or something [2].

Although it has several advantages, some disadvantages also persist which needs to be handle for attaining higher efficiency in the today's world.

- During the acquisition process the small distance between finger and camera deteriorates the quality of image and create optical blurring [3].
- The intensity of light at the capturing device may affect image darkness and brightness [4].
- If position of the finger is not properly maintained, the recognition rate decreases [5].
- Different thicknesses of skin layer, bones and noise can affect the light scattering, which can decrease the recognition rate [6, 7].

Since finger vein authentication systems are associated with the Internet during transaction from ATM, security threats issues arises. In this paper a finger vein identification system is created by Image acquisition device (built in house) and is utilized in ATM with higher accuracy rate. After that the acquired finger vein image is sent to the ATM server. For securely transferring this image through internet to the central server for classification, a more secured method is employed which uses combined approach of light-weight cryptography and steganography [proposed variable most significant bit–least significant bit (MSB–LSB)] techniques. In central server firstly the captured image is passed through thresholding for extracting the region of interest, and then contrast limited adaptive histogram equalization (CLAHE) is used for the intensification of the captured image. Afterwards, it is transformed to black and white image and edge, texture and feature extraction is done by Gabor filter, fractal dimension and Lacunae. Finally the learning and classification is done by support vector machine.

The consecutive portion of the paper describes literature survey, proposed methodology and conclusion respectively.

2 Literature survey

Since many years, different researchers all through the world have just been researching in the area of finger vein authentication system and its information exchange security. Additionally, some surveys of this type of ongoing research and its relating efficiency and measuring estimation time are explained in this section.

Researcher Wu and Liu [8] have described neural network and component analysis methodology used in finger vein authentication method. In this paper, finger vein patterns are captured by near infrared radiation (NIR) light and charge-coupled device (CCD) camera, after that feature extraction is done by principal component analysis (PCA) and classification is done by using two algorithm back propagation (BP) neural network and adaptive neuro-fuzzy inference system (ANFIS) respectively. To verify the effect of the proposed ANFIS, the BP neural network is compared with ANFIS. The experimental results demonstrated by the proposed architecture using ANFIS has better performance than BP neural network and its classification accuracy reaches to 99%.

Researcher Zhang et al. [9] highlighted the problems of extracting vein patterns from an infrared finger-vein image due to low light conditions, noise and irregular shading, which can seriously weaken the capability of a finger-vein recognition system in practical application. To overcome this problem, in this paper proposed local Radon transform which depends on robust vein pattern extraction procedure is used. For this purpose primarily calculate the values along six directions in the neighborhood of the pixel using local Radon transform. Then on basis of the values along six directions, the primary vein orientation and its normal vector can be determined. Further to reduce the impact of noise, the curvature along the normal vector and verify whether the pixel belongs

to vein patterns by certain rules. Finally, a local binarization method is employed for extracting vein patterns and is matched by the template method. This experiment revealed that the suggested approach is better in terms of performance than any another algorithm as its result is 92.46% on database A and 97.55% on database B.

Researcher Khanam et al. [10] observed discriminant analysis method better in terms of space requirement and time complexity and the K-nearest neighbor (KNN) algorithm of machine learning method determines the accuracy of the features of the finger-vein images. Hence the resulting accuracy from KNN is 55.84% while the discriminant analysis method gives the accuracy of 92.21% which makes it more accurate from KNN technique.

Researcher Fairuz et al. [11] explained that the development of finger vein identification method depends on transfer learning of AlexNet model which is then tested by plotting true positive rate and false positive rate by receiver operating characteristic (ROC) curve which is the curve of probability to examine the experiments results where the appropriate result is 95%. Area under the curve (AUC) is used to give the measure of quality of ROC curve which is 0.99 for this test that means 99% of times this experiment is capable to differentiate between positive and negative classes.

Researcher Buchmann et al. [12] have proposed a lightweight cryptographic authentication protocol. It is XOR scheme in radio frequency identification (RFID) tags and readers that effectively opposes any unapproachable assaults propelled in smart environment. Lightweight cryptography strategies are represented considerable in compelled conditions where RFID tags, sensors, contactless smart vehicles and medicinal services gadgets are importantly utilized since such calculations require small code and random access memory (RAM) estimate.

Researcher Boughaci et al. [13] have proposed an uncommon steganographic strategy where confidential information is covered with an image to assure secret communication. The stochastic local search (SLS) which is a local search based-algorithm adopts an initial random solution. Here certain diversification and intensification strategies are associated to locate good quality solutions. A fitness function is evaluated for each and every block. During the position search process, if an image block is found identical to block message, then the process is stopped for this block and is continued for other remaining blocks. The combined approach of steganography only with LSB is not effective as the image size increases with the insertion of information due to which discovery of hidden information gets possible. So to improve it, metaheuristic is added to LSB.

The successive segment describes the proposed approach.

3 Proposed methodology

For secure financial transaction through ATM, a biometrics authentication system is used and the combined approach of cryptography and steganography is proposed for the transfer of finger vein information. The proposed model is broadly divided into two categories, i.e. finger vein authentication system and secure finger vein information transfer. In this paper, for secure information (finger vein image) transfer a lightweight cryptography and proposed variable MSB–LSB algorithm is used, as depicted in Fig. 1. For authentication purpose consolidated methodology of machine learning and image processing is used as shown in Fig. 2.

3.1 Finger vein authentication system

3.1.1 Image acquisition

Finger vein patterns are undetectable to normal eye but are seen by near infrared light (where wavelength varies between 700 and 1000 nm) [6, 14]. 850 nm near infrared radiation (NIR) are utilized for capturing finger vein pictures in this paper as it is the cheapest way to visualize finger vein with highest accuracy since, it passes through fingers to capture the images and is impeded by the hemoglobin and melanin by which dark line of the vein is shown up.

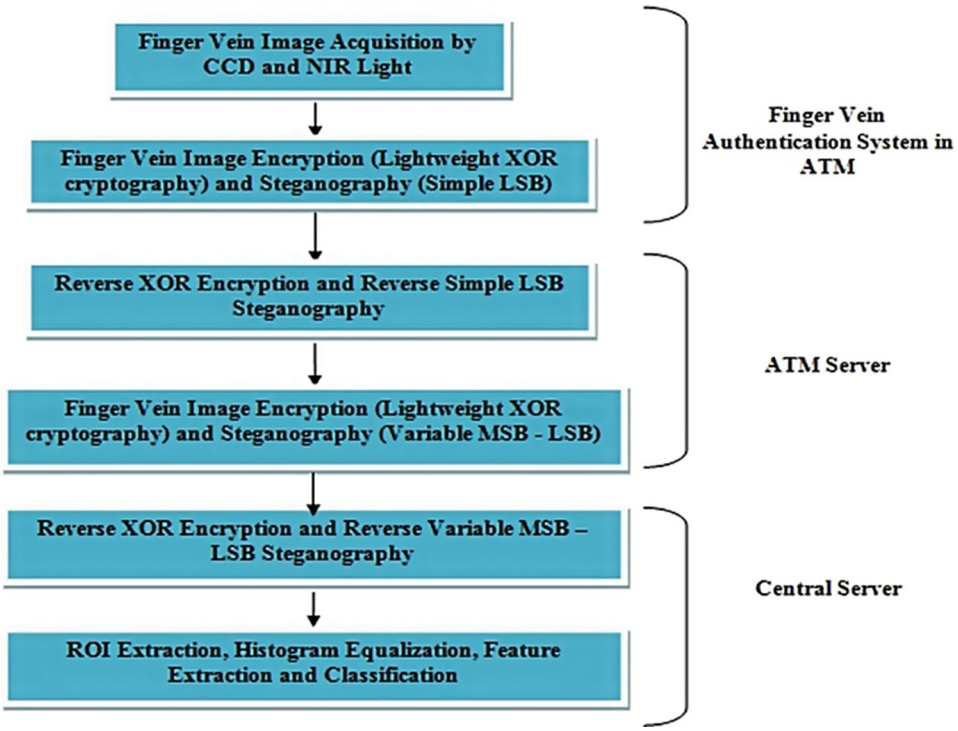
For capturing the finger vein pattern 2 methods are commonly used i.e. "light reflection" and "light transmission" as depicted in Figs. 3 and 4.

In this paper a high contrast image is captured using the light transmission procedure in which the finger is situated between NIR light and charge-coupled device (CCD) camera, where the light passes in between the finger and the CCD camera catches the image, therefore most of finger vein imaging device employ this.

3.1.2 Region of interest extraction

However, in image acquisition process, there are some problems, like lower contrast and noise due to light fluctuation and finger rotation and translation problem occurs, so to solve these problems, in this paper region of interest process and histogram equalization is used. Region of interest i.e. image region extraction is done by thresholding of the image, for that purpose multidimensional filtering is used [15]. By using this methodology a better quality of finger vein image is produce without noise, shades and low contrast.

Fig. 1 Proposed architecture



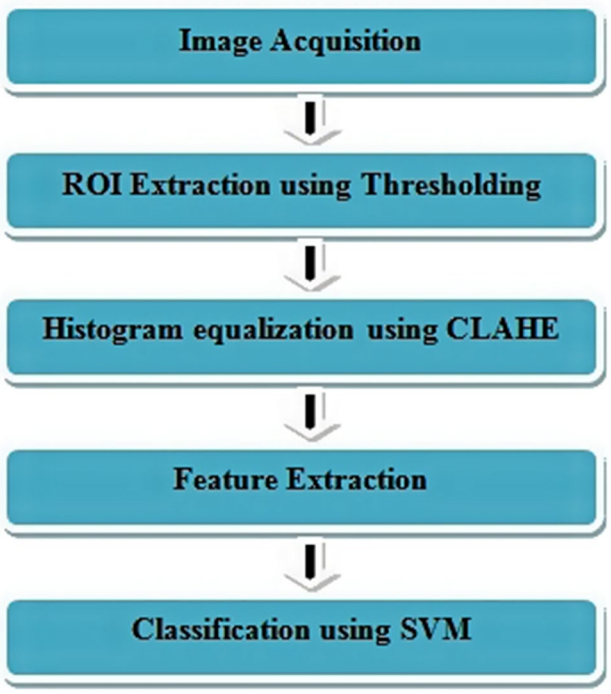


Fig. 2 Finger vein identification system

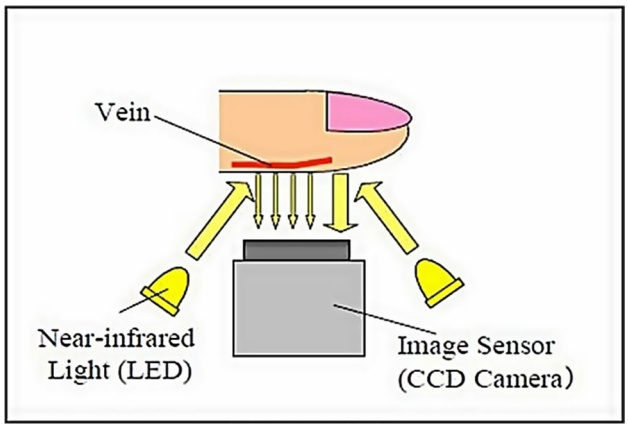


Fig. 3 Light reflection method

3.1.3 Histogram equalization

Histogram equalization is used for enhancing the finger vein image quality after region of interest procedure. Adaptive histogram equalization is used to adjust the dark and bright region. One weakness of this technique is noise amplification. For this purpose contrast limited adaptive histogram equalization (CLAHE) is utilized. It minimizes the amplification by using cumulative distribution function (CDF) and redistribution is done by cutting the limit of histogram and its neighborhood area. The process is repeated until additional value goes to minimum.

3.1.4 Feature extraction

Enhancement of the precision of finger vein recognition is done by an efficient feature extraction technique. It

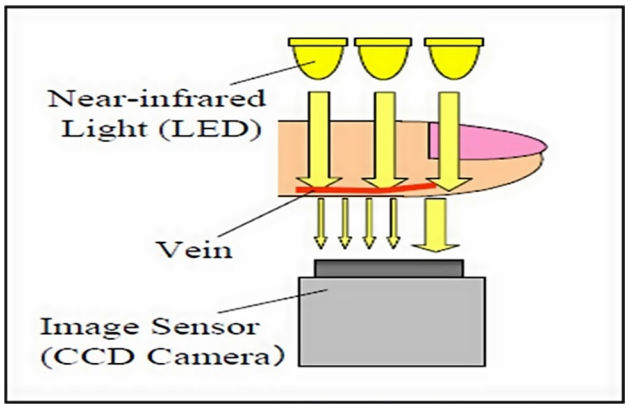


Fig. 4 Light transmission method

comprises of two section first is texture extraction later is edges extraction. These are done by three algorithms fractal dimension, Lacunae algorithms and Gabor filter.

3.1.5 Fractal dimension

It determines the quantifiable record of complexity present in fractal geometry and compares the differences minutely present in the scale where the complexity is measured. For measuring it a box counting procedure is used and three dimensional extended box checking procedures is used for determining 3D volumetric information. Similar concept is used to analyze fractal dimensions.

$$FD = \log(Nr)/\log(1/r) \quad (1)$$

In this process at first N copies of crude shape is created by the division of fractal object where each and every copy is scaled up to the factor of r and N and r have a logarithmic relation between them. The fractal value can be calculated determining the slope of line along with calculation of Nr for different calculation of r.

3.1.6 Lacunae

Lacunae are taken as gap which can measure intensity by differentiating from one point to another point. But a condition can also come when value of fractal dimensions will vary with varying images and then the lacunae algorithm is used for identifying different images [16].

3.1.7 Gabor filter

For different pattern recognition techniques Gabor filter is used for better feature extraction by using acuteness of direction, detect the feature component and tweaking the particular frequency, which grabs the texture attributes from the images.

It's determined by modulating a sinusoidal sign along with a Gaussian. Let's take a function f(x, y, θ, and ϕ) which define the Gabor filter. As θ and ϕ indicates the spatial frequency in the direction, Gabor filter is focused at the origin with θ and ϕ [17]. The Gabor filter can be seen as:

$$f(x, y, \theta, \phi) = \exp((-x^2 + y^2)/\sigma^2)\exp(2\pi\theta i(x\cos\phi + y\sin\phi)) \quad (2)$$

Here, σ is standard deviation which relies upon θ.

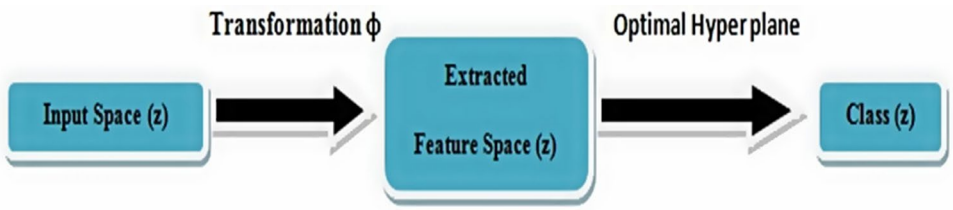
3.1.8 Classification

Everyday some new classification algorithms are being invented based on statistical theory of learning. Within these algorithms, support vector machine (SVM) is one of better classification algorithm. As it works with the boundary values unlike all the classifier thus it can classify between a larger ranges, so there is less chance of showing an odd result. SVM is a cluster of training methodology that can solve problems of discrimination and regression. For the purpose SVM uses linear classifiers [18]. Gaussian Kernel avoids non-linearity factors in SVM by changing data space depicted in Fig. 5.

3.2 Secure finger vein information transfer

For the transmission of biometric information (finger vein image) between finger vein authentication system in ATM and the ATM server, the combination of a lightweight cryptographic method (such as XOR operation) and steganography (simple LSB substitution technique) scheme is proposed. At the ATM server, the encrypted finger vein image is retrieved using reverse steganography and the original finger vein image is obtained by light weight decryption. During the transfer of the captured finger vein image from the ATM server to the central server through Internet, an integrated approach of steganography (proposed variable MSB–LSB substitution technique) scheme and a light

Fig. 5 SVM space



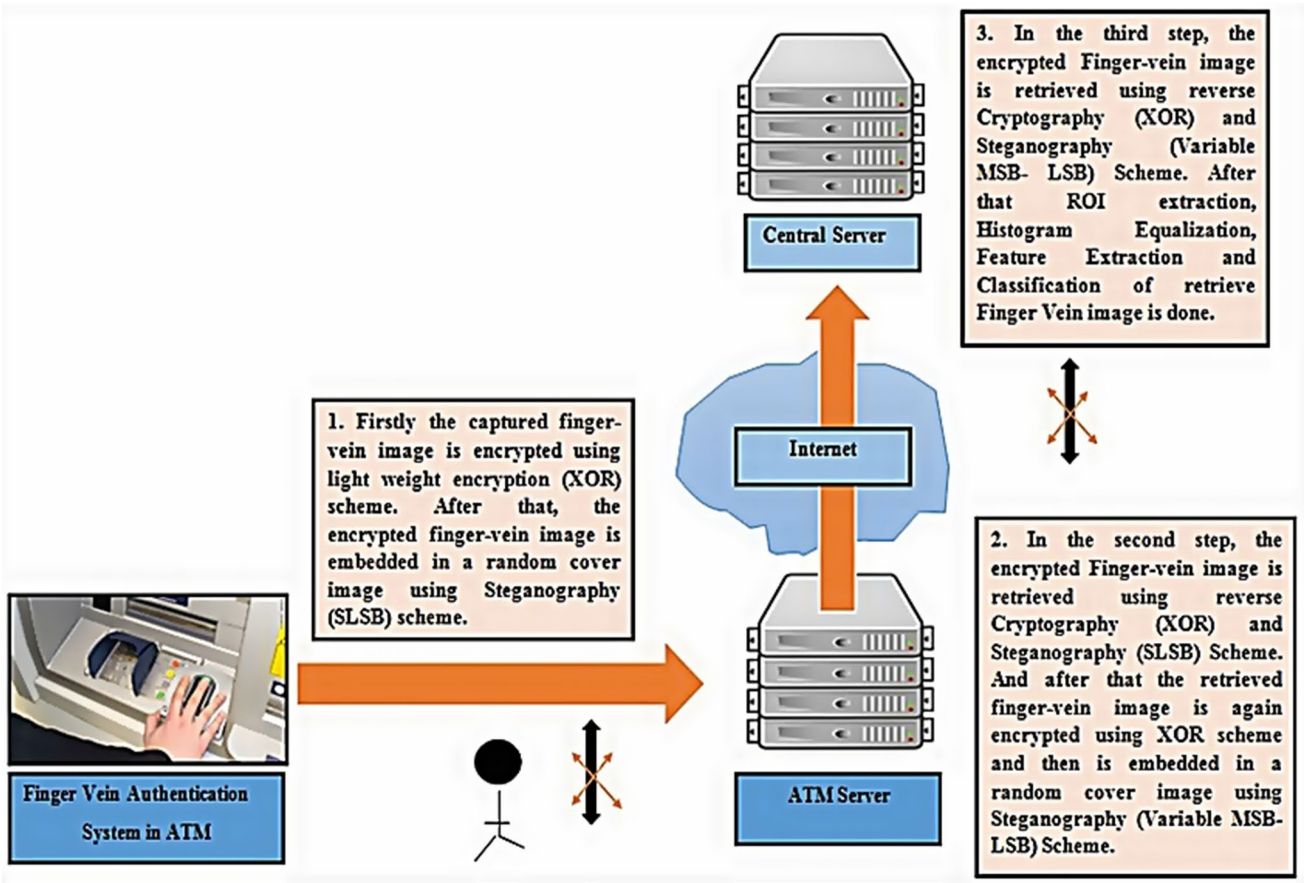


Fig. 6 Proposed finger vein transfer scenario

weight cryptographic method (such as XOR operation) is proposed (shown in Fig. 6).

3.2.1 Variable MSB–LSB substitution algorithm

Single bit LSB substitution is a well-known algorithm and it have the feature of substituting single bit of image pixel in each carrier pixel (in case carrier is image) and within it there is no further scope of adding more pixel bits inside the cover medium. If uses MSB and LSB to substitute, it can embed 2 image pixel bits at maximum. It is favorable in the way that the image quality is not degraded much. The proposed algorithm (variable MSB–LSB) is much identical to simple LSB substitution algorithm (degree of substitution is 1), but it has the ability to embed maximum 2 image pixel bits and it can randomly map the cover image pixel, whereas simple LSB have the ability to embed only 1 image pixel bit and it cannot randomly map the embedding cover pixel. For this randomness and variation, a hashing algorithm is used that randomly maps pixel values of cover image to different targeted hash mapped pixel values each time it embed the image pixel bit. So according to this features,this algorithm can provide better security against confidentiality attacks and replay attacks, if launched by intruders.

Abbreviations

Least Significant bit of Image Pixel: LSB
Most Significant bit of Image Pixel: MSB
Image : I
1st bit of Image: I – Bit-1
2nd bit of Image: I – Bit -2
Pixel Number: pixel No

Hash function that incorporates Randomness in Variable MSB - LSB Scheme

Step1: If pixel No > 54
Step 2: Find out the quotient i.e pixel No/54
Step 3: s= quotient -1
Step 4: Hash Value (pixel No, where embedding of message bit occurs) = (pixel No % 54) + pixel No + (53 x s)

Embedding Algorithm

```
Step1:
if (MSB ==0)
   if (LSB==1 && I-Bit-1==0)
   replace LSB by I-Bit-1; // Embed 1 I bit
   else if (LSB==0 && I-Bit-1==1)
   replace LSB by I-Bit-1; // Embed 1 I bit
   else if (LSB==I-Bit-1)
   retain LSB // Embed 1 I bit

Step2:
Else if(MSB ==1 && I-Bit-1==1)
      if (LSB==1 && I-Bit-2==0)
   retain MSB & replace LSB by I-Bit-2    // Embed 2 I bits
   else if(LSB==1 && I-Bit-2==1)
   skip pixel                             // No Embedding
   else if(LSB==0 && I-Bit-2==0)
   retain both the MSB and LSB            // Embed 2 I bits
   else if(LSB==0 && I-Bit-2==1)
   retain MSB and change LSB by I-Bit-2  // No Embedding

Step3:
Else if(MSB ==1 && I-Bit-1==0)
make LSB=1 and retain MSB                  // No Embedding
```

Retrieving Algorithm

```
Step1:
 if (MSB ==0)                    // Retrieve 1 I bit
Step2:
else if (MSB ==1 && LSB==0)   // Retrieve 2 I bits
Step3:
else if (MSB ==1 && LSB==1)     // No Retrieval
```

Fig. 7 Finger vein detector and NIR light

In the following section, experimental outcomes are expressed.

4 Experimental results

Experimental result can be defined into two categories. First is for finger vein authentication system which is done by Python IDLE 3.6.4. Later gives the result of transfer of secure finger-vein images using steganography and cryptography schemes using Matlab R2013a.

4.1 Finger vein authentication system

For performing the experiment Python IDLE 3.6.4 is used on Windows 8.1 OS with specification Intel Core i5 with 2.4 GHZ. Data like name and finger subtleties of people is stored using SQLITE 3 database. In this paper in house developed finger vein acquisition system which consists of an infrared sensitive charge-coupled device (CCD) camera and near infrared radiation (850 nm) light (shown in Fig. 7). To overcome the drawback such as optical blurring, deterioration of image quality, finger position displacement and scattering of light due to bones thickness, the CCD camera and high sensitivity NIR light is used.

The mentioned SQLITE 3 database is used for the purpose of training and testing. The database comprises of 10 sample individuals and each of them have 3 other folders which contains 3 types of finger images i.e. ring, index and middle finger. So there are 6 images in each folder, so for every individual it has 18 images and the resulting total number sample is 180.

When the process of image acquisition is completed, the thresholding is done over finger vein image of 10 individual sample by finger region extraction i.e. region of interest (ROI) which is depicted in Fig. 8. For getting equal contrast in every part of finger vein image, normalization is used by histogram equalization with the help of CLAHE algorithm can be seen in Fig. 9. After that Lacunae and fractal dimension algorithms is used for texture extraction and Gabor filter is used for edge extraction shown in Fig. 10. For classification two processes are used, one is one-versus-one and the other is one-versus-all, both this approaches used training and test set which have 10 classes along with 18 trials which sums up to in total of 180 feature vectors. Venous networks which have 10 classes, each class has contained 4 tests in the test set and are represented by the total of 80 features vectors. Firstly the input images are measured with 180 features by the help of decision functions of $N(N-1)/2$ and in case the match is found it is called match successful. The experiment shows that in proposed procedure (one-versus-one and one-versus-all) the average recognition accuracy is 98.75% and 97.92% and the execution time is 0.168 s and 0.187 s respectively. A comparative study of proposed algorithm with other algorithms is given in Fig. 11.

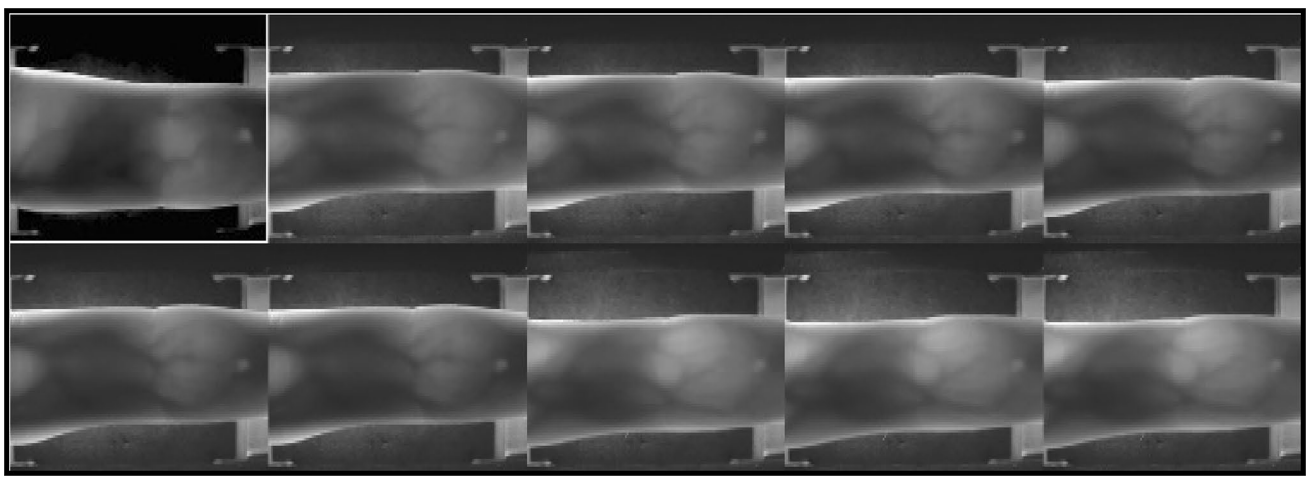


Fig. 8 Region of interest extraction

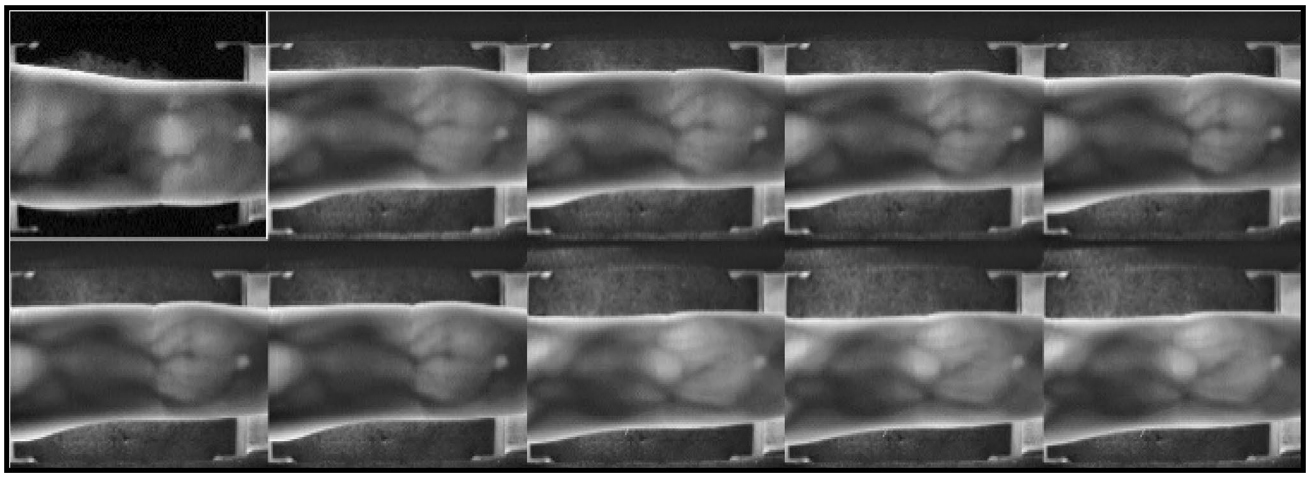


Fig. 9 Histogram equalization

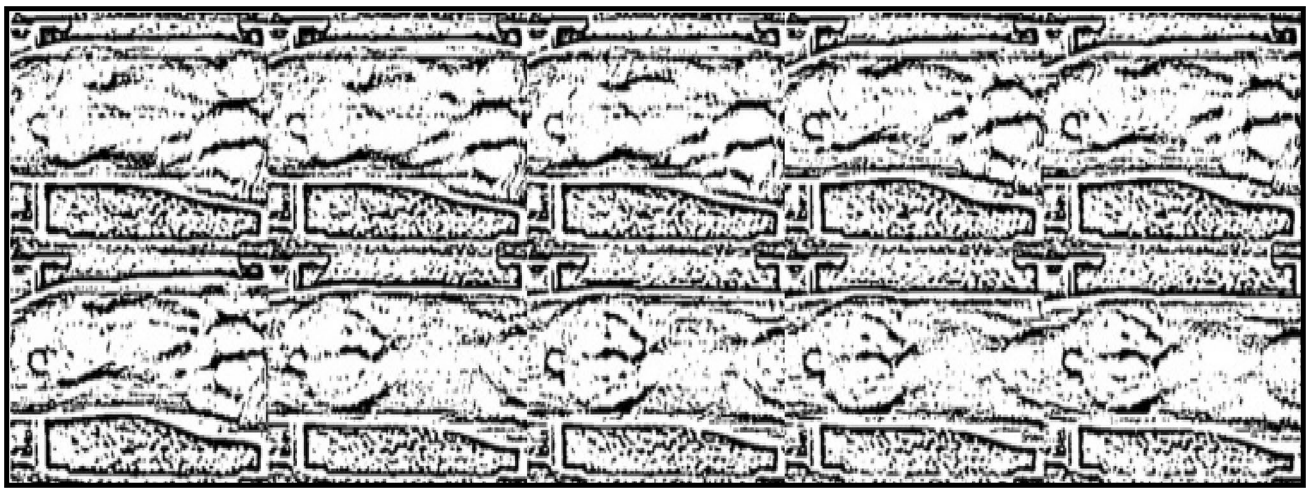


Fig. 10 Feature extraction

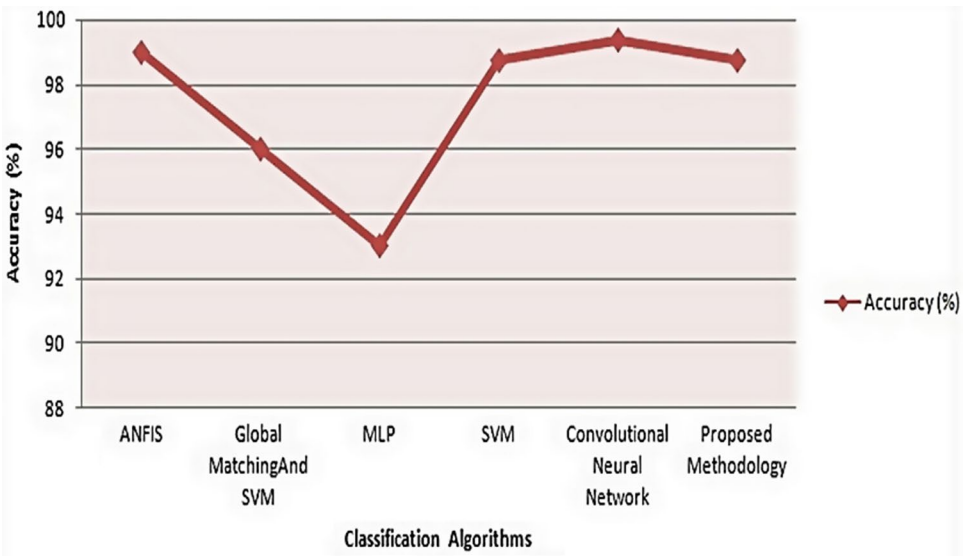


Fig. 11 Comparative analysis of classification accuracy

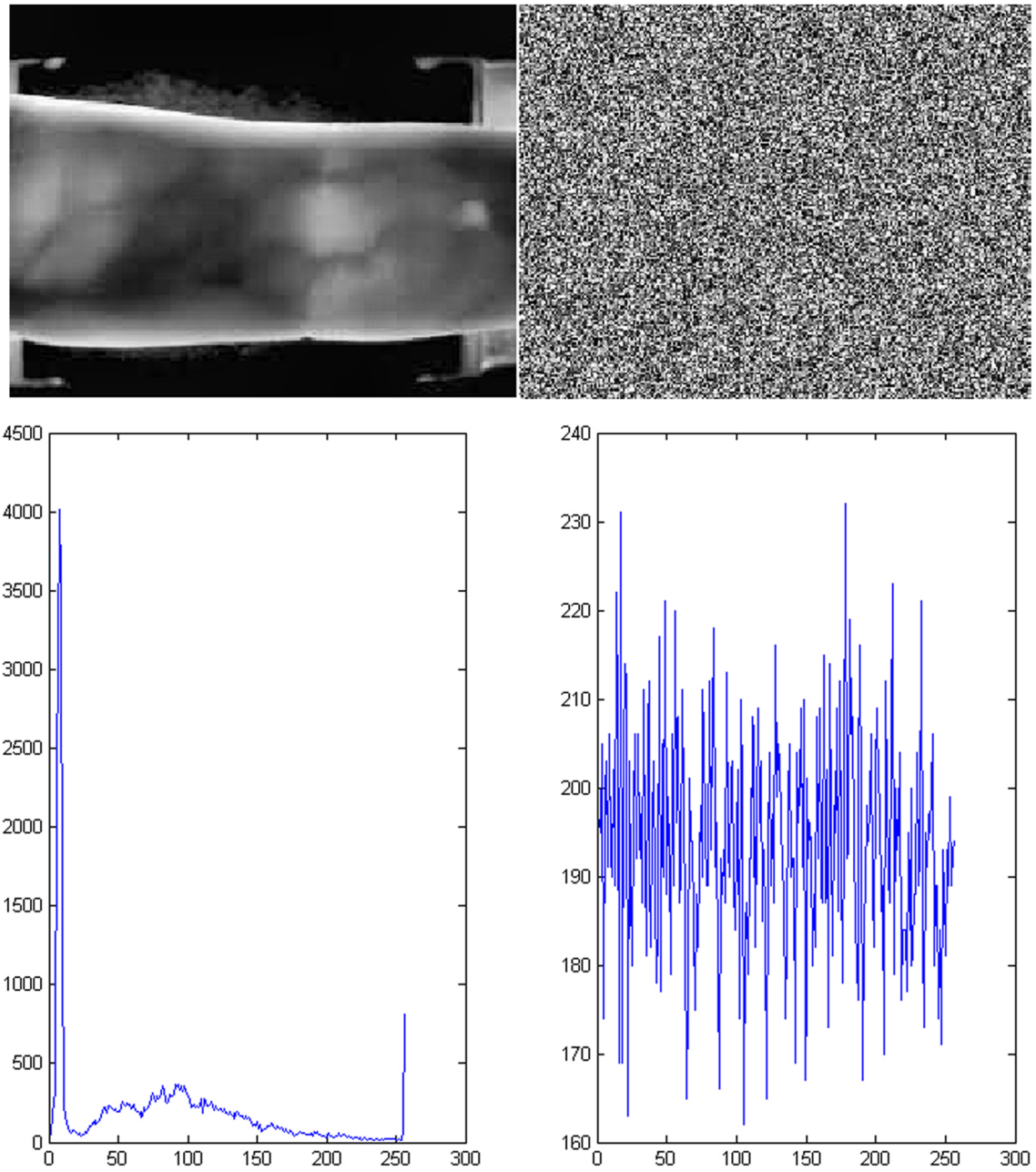


Fig. 12 Finger vein encryption (XOR) and histogram

Figure 11 depicts that the two algorithms have better classification accuracy than proposed methodology i.e. adaptive neuro-fuzzy inference system (ANFIS) and convolutional neural network (CNN) with 99% and 99.38% accuracy respectively. However, the execution time of 4.5 s is required for ANFIS which is comparatively greater than proposed procedure and CNN does not give efficient result for low quality finger vein images, whereas the proposed procedure has no such issue.

So as a result it can be said that the proposed methodology is better in terms of classification accuracy when compared with the algorithms except ANFIS and CNN and has advantage of lesser execution time required and give efficient result for low quality finger vein images.

4.2 Secure finger vein information transfer

This experiment is done using Matlab R2013a. As per proposed design, first the finger vein information is encrypted using lightweight encryption algorithm (XOR operation), then embedded it in a randomly selected cover image employing using our newly proposed (variable MSB–LSB

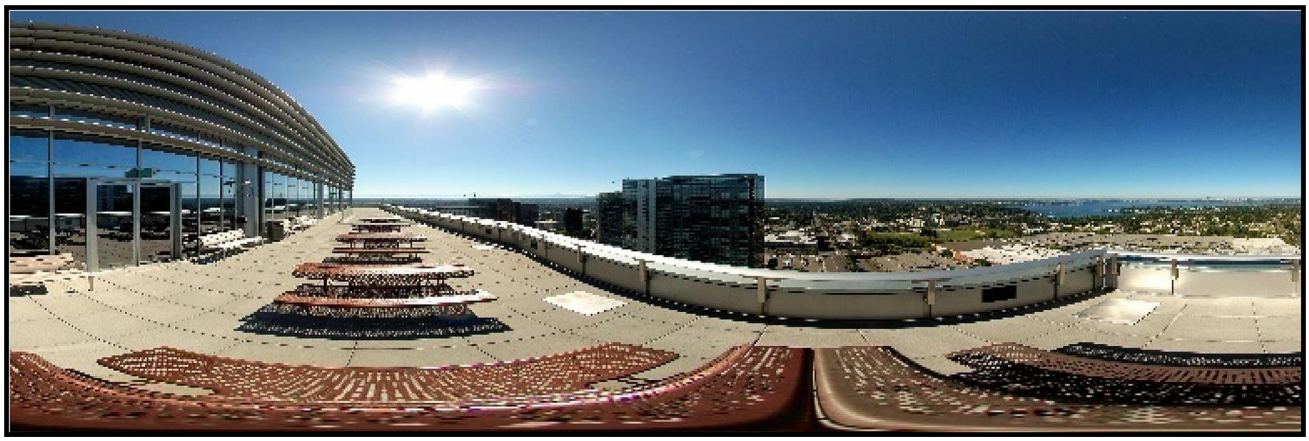


Fig. 13 Random cover image

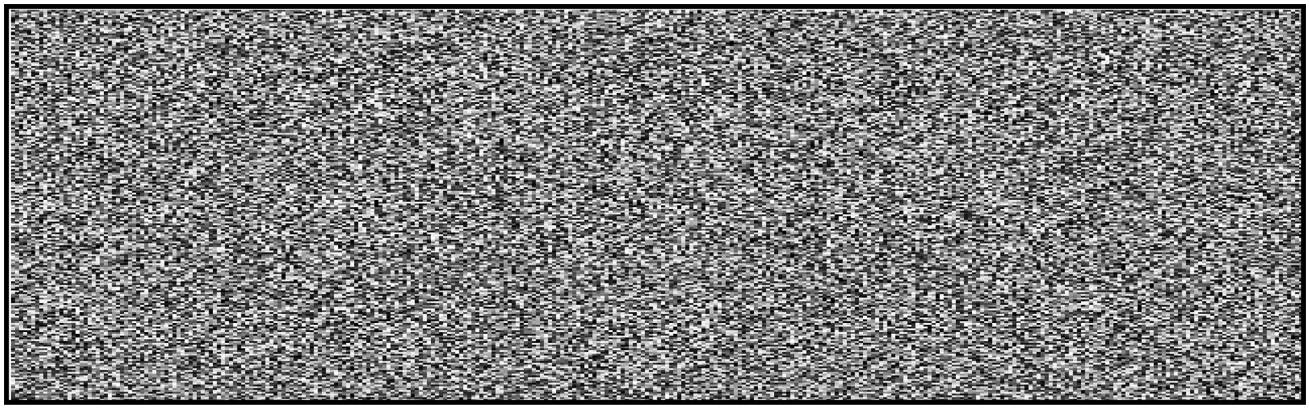


Fig. 14 Encrypted (XOR) finger vein image

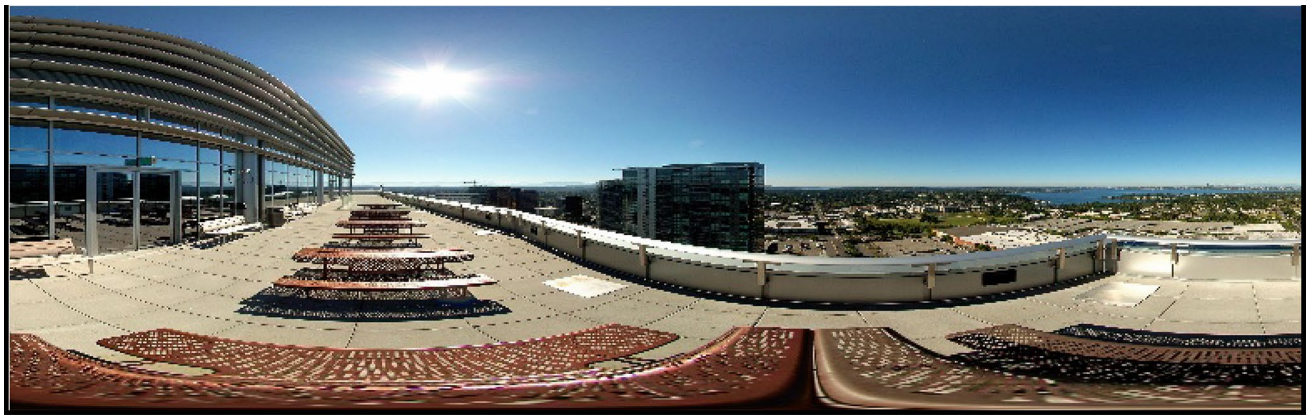


Fig. 15 Embedded image (cover image + encrypted finger vein image)

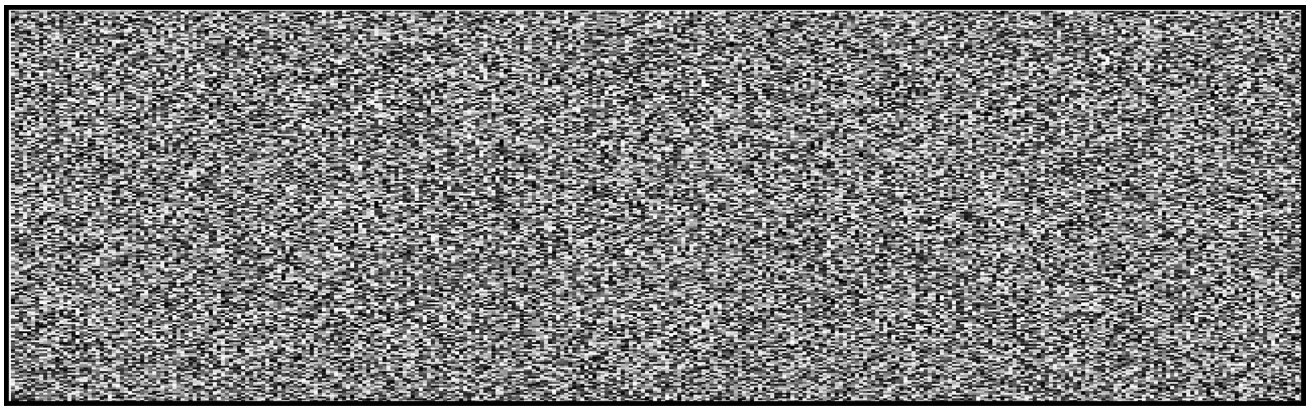


Fig. 16 Retrieve encrypted finger vein image

substitution scheme) steganography technique. The given procedure is shown in the consecutive image (Figs. 12, 13, 14, 15, 16, 17). The Fig. 18 shows that variable MSB-LSB technique is better than Simple LSB because it requires less number of pixels for embedding.

The accompanying section concludes the paper.

5 Conclusion

Due to an expansion in globalization, the normal individual's life has being compromised by the expanding grievous events of attacks of individual data and in the case of financial transaction and banking-related tasks in automated teller machines (ATMs). PIN and Password are most common way of accessing ATMs for financial transaction but they can be forged and thus are subjected to attack such as phishing, spoofing etc. In order to overcome such attacks higher security is required. Subsequently the human physiological and behavioral characteristics, for example iris, voice, finger print, face palm and so on are being utilized to give better security arrangements. In any case, they all can be effectively deceived and replicated at one level and a superior arrangement is required for the security necessities which are cost productive and reliable too. Hence, the combined approach (machine learning and image processing) of finger vein authentication method is used and for finger vein image transfer variable MSB–LSB steganography and light weight cryptography is proposed in this paper. The vein authentication method is relatively complicated, so it could be better to use it for some special applications. For finger-vein authentication system, the experiment shows that in proposed classification procedure (one-versus-one and one-versus-all) the average recognition accuracy are 98.75% and 97.92% and the execution time is 0.168 s and 0.187 s respectively. One comparative study is done among 5 algorithms which includes ANFIS, Global Matching and SVM, MLP, SVM and CNN. Adaptive neuro-fuzzy inference system (ANFIS) and convolutional neural network (CNN), the two algorithms have better classification accuracy than proposed methodology i.e. with 99% and 99.38% accuracy respectively. However, the execution time of 4.5 s is required for ANFIS which is comparatively greater than proposed procedure

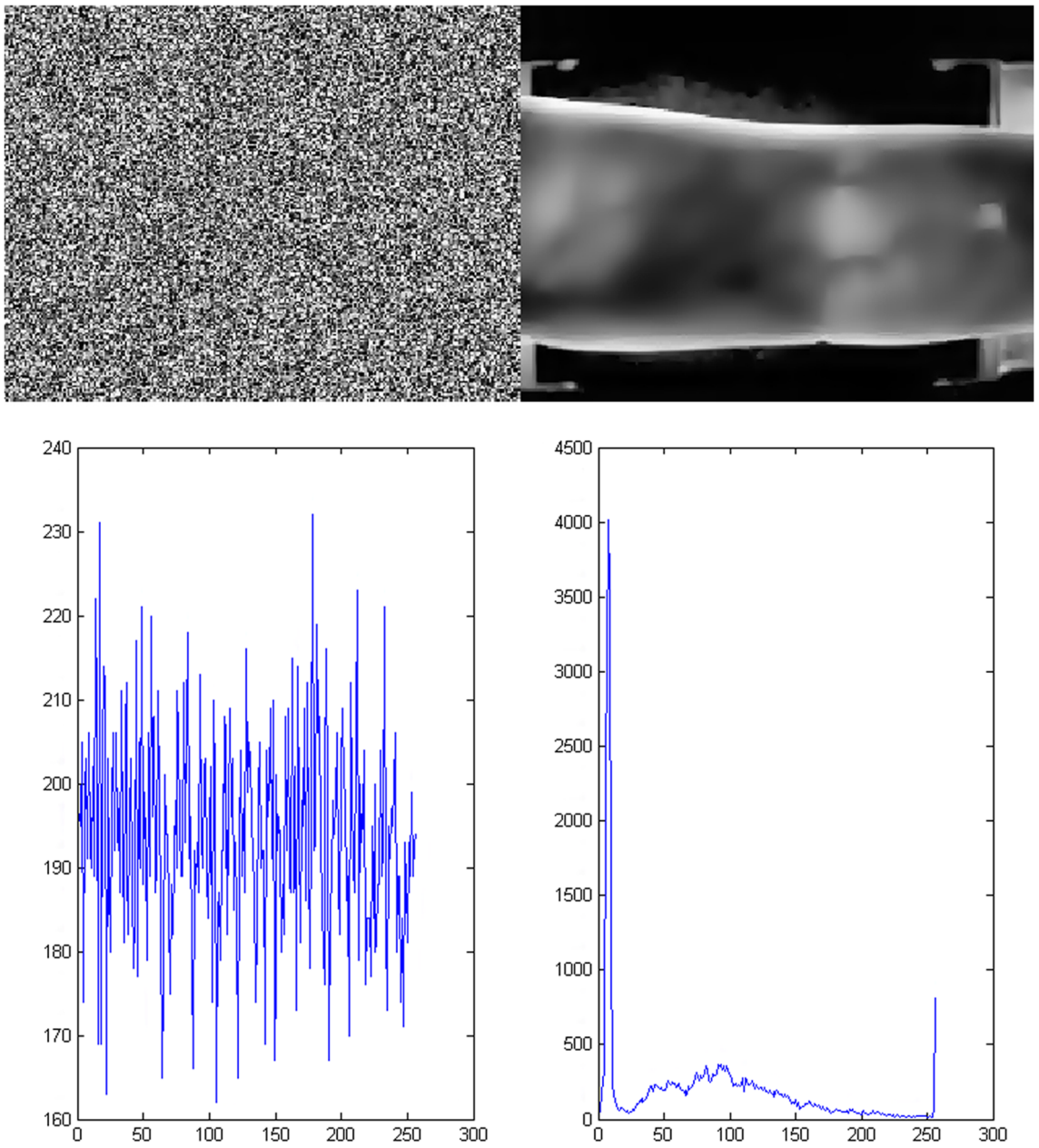


Fig. 17 Decrypted original finger vein image and histogram

and CNN are not giving efficient result for low quality finger vein images, whereas the proposed procedure has no such issue. Thus, the proposed approach is better in regards to classification accuracy when appeared differently in relation to ANFIS and CNN and furthermore have advantageous if there should be an occurrence of time of execution, noise sensitivity and better for non perfect finger vein cases. Another issue which is to be considered is the means by which this biometric image (finger vein) can be transferred safely. And the variable MSB–LSB algorithm

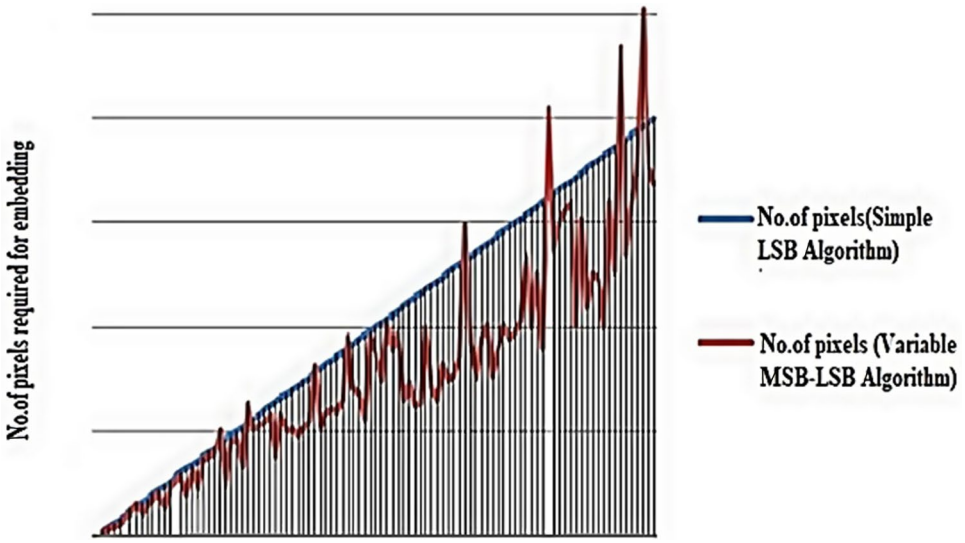


Fig. 18 No. of image pixel needed to embed

is better than simple LSB algorithm because it requires less number of pixels for embedding and have better randomness, security etc.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interests.

References

1. Wu J-D, Ye S-H (2009) Driver identification using finger-vein patterns with Radon transform and neural network. Expert Syst Appl 36(3, Part 2):5793–5799
2. Yanagawa T, Aoki S, Ohyama T (2007) "Human finger vein images are diverse and its patterns are useful for personal identification" 21st Century COE Program, Development of Dynamic Mathematics with High Functionality, April, pp 1–8
3. Lee EC, Park KR (2011) Image restoration of skin scattering and optical blurring for finger vein recognition. Opt Lasers Eng 49:816–828
4. Podgantwar UD, Raut UK (2013) Extraction of finger-vein patterns using Gabor filter in finger vein image profiles. Int J Eng Res Technol 2(6):3294–3298
5. Yang J, Shi Y (2012) Finger-vein ROI localization and vein ridge enhancement. Pattern Recognit Lett 33(12):1569–1579
6. Miura N, Nagasaka A, Miyatake T (2004) Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification. Mach Vis Appl 15:194–203
7. Liu Z, Yin Y, Wang H, Song S, Li Q (2010) Finger vein recognition with manifold learning. J Netw Comput Appl 33:275–282
8. Wu J-D, Liu C-T (2011) Finger-vein pattern identification using principal component analysis and the neural network technique. Expert Syst Appl 38(5):5423–5427
9. Zhang J, Lu Z, Li M (2018) A finger-vein extraction algorithm based on local Radon transform. In: 13th World Congress on intelligent control and automation (WCICA), July, 2018
10. Khanam R, Khan R, Ranjan R (2019) Analysis of finger vein feature extraction and recognition using DA and KNN methods. In: Amity international conference on artificial intelligence (AICAI), 4–6 Feb 2019, pp 477–483
11. Fairuz S, Habaebi MH, Elsheikh EMA (2018) Finger vein identification based on transfer learning of AlexNet. In: 7th International conference on computer and communication engineering (ICCCE), 19–20 Sept 2018, pp 465–469
12. Buchmann J, Gopfert F, Guneysu T, Oder T, Poppelmann T (2016) High-performance and lightweight lattice-based public-key encryption. In: Proceedings of 2nd ACM international workshop on IoT privacy, trust and security (IoTPTS), pp 2–9
13. Boughaci D, Kemouche A, Lachibi H (2016) Stochastic local search combined with LSB technique for image steganography. In: 2016 13th Learning and technology conference (L&T), 10–11 April 2016, pp 36–44
14. Hitachi (2006) "Finger vein authentication—white paper", Copyright
15. Gupta P, Gupta P (2015) An accurate finger vein based verification system. Digit Signal Process 38(C):43–52
16. Liu Z, Song S (2012) An embedded real time finger vein recognition system for mobile devices. IEEE Trans Consum Electron 58(2):522–527
17. Kumar A, Zhou Y (2012) Human identification using finger images. IEEE Trans Image Process 21(4):2228–2244
18. Park KR (2011) Finger vein recognition by combining global and local features based on SVM. Comput Inform 30:295–309

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.