A Finger Vein Security System Using DNA Encryption, LSB Data Hiding and Image Scrambling

Dnyaneshwari P. Wagh[1], Fadewar H. S[2], Shinde G. N[3]

School of Computational Sciences, SRTMU, Nanded, Maharashtra, India[1,2], Yeshwant Mahavidyalaya, Nanded, Maharashtra, India[3]

Corresponding author: Dnyaneshwari P. Wagh, Email: dnyaneshwari.wagh15@gmail.com

Finger vein technology is a secure biometric solution, reliable and non-invasive that provides authentication from fast and highly accurate identity to access data or secure areas. The personal information security in cyberspace has gradually become an important topic nowadays, and biometric identification technology has emerged as the times require. Finger vein authenticated person information security is another prominent problem in the research area. So, by combining the information security and finger vein image security will improve the security of the whole system. This paper proposes a finger vein image security system using DNA encryption, image scrambling with LSB steganography technique. The secret data of the user is first encrypted using DNA encryption. LSB data hiding is used to hide this encrypted secret data in the finger vein image. This method consists of replacing the least significant bit, the last bit of each byte, of the pixels of an image with the bits of the information to be hidden. The security of the user is given importance by encrypting the details and then hiding the information. The stego image is then encrypted using image scrambling technique. To match a user's vein, the image is descrambled and then compared to the finger vein based on the data extracted from the image. The proposed model provides security to the user information as well as the finger vein image.

Keywords:DNA encryption, Finger vein, Steganography, LSB data hiding.

2023. In Saroj Hiranwal & Garima Mathur (eds.), *Artificial Intelligence and Communication Technologies*, 847–856. Computing & Intelligent Systems, SCRS, India. https://doi.org/10.52458/978-81-955020-5-9-79

1 Introduction

Biometrics is a method of recognizing people based on their physiological characteristics or behavior. It is the application of mathematical and technological methods to identify or verify identity, control access, user authorization, data protection and security management. In contrast with traditional security such as login password systems and PIN, biometric security techniques have shown a higher level of security [1]. This technology is responsible for verifying the identity of the user checking factors that are related to the biology of the some of the most used characteristics are scanning iris, retina scan and fingerprint scan. The identification of user is produced based on their own and unrepeatable features, such as their fingerprints, voice, the geometry of palm, finger veins or the settings of retina [2]. This method does identify the user, since when these devices are working properly, only one individual can be identified with success, by virtue of a correct choice of the physiological parameters to be evaluated.

In order to distinguish a person inherently as authorized against an impostor, biometric based personal identification systems [3] are need of an hour. Since this system identifies an individual based what he or she is rather than what he or she has. This system is much less prone to forgery owing to its high level of distinctiveness, secured and dependable. With all these added advantages this system has gained much popularity as one of most preferred personal identification measures. This technology is defined as to identify an individual based on statistical measurement of human behavioral and unique physiological characteristics.

The various categories of biometric systems as given below figure 2:

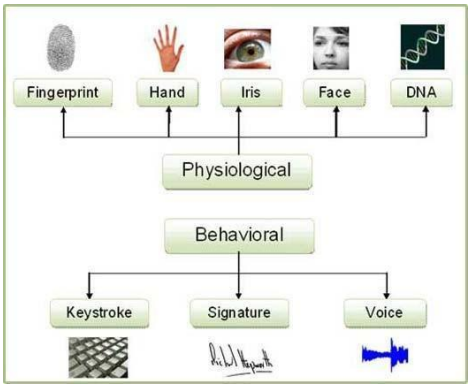


Fig. 1. Categories of Biometrics

Finger vein recognition is a technology [4] that uses near-infrared light to irradiate fingers to obtain vein images and extract vein characteristics for personal identity authentication. It has the following two unique advantages: one is that it can only be recognized in vivo, and the other is that it is located in the body. The inside of the body stands out among the many biometric identification. The two characteristics make finger veins difficult to forge and copy, and are not easily affected by external factors. As a biometric feature [5], the security level is high.

The research on finger vein recognition has developed rapidly. It has achieved remarkable results in region of interest (ROI) positioning and segmentation, image enhancement processing, feature extraction

and feature matching. Finger vein image security related processing technology and algorithm research are still the main content of the moment. Identity authentication security and finger vein fusion are gradually becoming research hotspots. Single template recognition and finger vein security can improve the anti-attack ability of recognition and have higher security. It is particularly important to note that finger vein image-related processing technologies and algorithms have begun to transition from the theoretical research level to the application level, and the development and research of related recognition systems are developing rapidly (research and implementation, system design and application systems), and the specific distribution of the topics.

2 Literature Survey

Madankar et al. [6] has explored the biometric template's privacy based on visual cryptographic schemes. As security is the most essential element, the encryption and decryption techniques are used. The image template, including retina, face, and fingerprints decomposed into two noises like VCS. Based on the observations, the constructed images are similar to the original private image. The higher accuracy is achieved with the reconstructed image and increased the pixel expansion factor.

Dwivedi et al. [7] has introduced a novel crypto-biometric system for generating the symmetric cryptographic keys from the fingerprint biometric modality. For preventing MiM attacks, CA-based authentication is developed and DH algorithm is used for key exchanging. The invariant pair minutiae bit-string is used to derive the private keys and overcome the impact on performance. The cryptographic keys and private keys are analyzed based on key size, randomness, and information entropy. The proposed approach is outperformed the previous crypto-biometric systems.

Shekhawat et al. [8] has investigated efficient sample encryption methods for finger vein data. The author has proposed an approach to disable biometric recognition completely. Based on the results, it indicates that apply the encryption at the start of a bitstream of JPEG2000 in layer progressive ordering.

Evangelin and Fred [9] have proposed a novel methodology to validate the multimodal biometric images based on ECC and VSC cryptographic methods. The ECC-based OCSO system has been used to enhance the key, which chooses the minimum error rate and extreme PSNR. Thus, the model security has been improved.

Ibjaoun et al. [10] has proposed Cancelable Biometrics based on visual cryptography to ensure the security. When implementing the proposed technique, the image quality shouldn't impact by the matching accuracy. The original image's information doesn't leak and good authentication performance is achieved using the proposed technique for finger vein template.

Kakkad et al. [11] has presented a concept of image security for cloud platform based on biometric authentication. The proposed algorithm performs the authentication of images in two basic steps of image compression using image encryption methods like blowfish and SWA and standard discrete wavelet transform method. Different types of biometrics with comprehensive view of encryption techniques have been discussed.

Panchal et al. [12] has discussed how a random and long encryption key can be produced from fingerprint. The key generation will be used using the proposed approach for encryption and decryption to protect the digital content based on DES, AES, etc.

Radhika and Nalini [13] have proposed hyper chaotic system based on DNA sequences and encryption. The hyper chaotic system proves that it is highly resistant to differential attacks, statistical attacks, entropy, sensitivity analysis, etc. by using implementation results.

Yang et al. [14] has proposed a cancellable finger-vein and smart card based bio-crypto system. The proposed system performs data authentication and encryption of sensitive health-care data. During transformation of biometric template or data exchange, the information leak can be avoided by storing the sensitive data and biometric template.

Surse and Jani [15] have proposed a CS-based system of biometric template protection based on Nesterov's algorithm to reconstruct the image of finger-vein template. Based on the measurement matrix, CS data is retrieved and stored the encrypted data in the template database. TV-min norm has been implemented using NESTA for template reconstruction. The results prove that I1-min surpassed by TV-min while reconstructing the template.

3 Proposed Method

The proposed model takes the input vein image as input. The secret data is encrypted using DNA encryption. The encrypted secret information is hidden in the input image using LSB data hiding. The image is then scrambled before storing the image. Figure 2 shows the proposed encryption and steganography model.

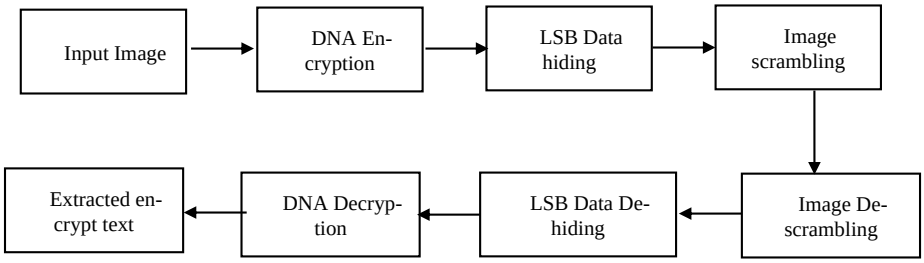


Fig. 2.Proposed encryption and steganography model

3.1 Cryptography based on DNA sequences

After Leonard Adleman published his work entitled "Molecular computation of solutions to combinatorial problems" (Adleman, 1994), where he stated that DNA sequences have the possibility of being used to carry out processes as if they were computers, that is, he proposed the biomolecular computing (BMC, for its acronym in English Biomolecular Computation), the processes of this type of computing are faster than conventional ones, however, a disadvantage of using them is that specialized equipment is needed, which are very expensive therefore many investigations use simulations. Due to the interest that has been aroused in this field, various investigations began to be carried out, including the implementation of cryptography using DNA sequences. One of the advantages of using DNA sequences to encrypt information is its information storage property; a gram of DNA can contain 10 Tera Bytes of information. Another advantage of using DNA is that its sequence is really random, for this reason, they are a good medium that can be used to encrypt information.

The steps to perform encryption and decryption are described below.

3.1.1 Encryption

Step 1: Read the image, represented by I_o(m, n, c), where m are the columns, n the rows and c the matrix of the corresponding primary color.

Step 2: Generate DNA sequence of Length≥mxnx4, using the rand seq(N) instruction, which belong to the bioinformatics toolbox. The first instruction generates a sequence of N nucleotides of DNA and the second requests them from the database of the National Center for Biotechnology Information (NCBI) under the accession name "Accession".

Step 3: Regroup the DNA sequence into a set of 4 nucleotides, then convert them into an 8-bit binary value number, for example, consider the following nucleotide sequence "A GT C, which will become the following binary values"00 10 11 01"later these bits will be regrouped to obtain the following binary number"00101101". The conversion of nucleotides to binary numbers is reported in the reference.

Step 4: Convert the 8-bit binary numbers into decimal numbers, then regroup them $M_d(m, n)$. in the matrix.

Step 5: Blur the colors of the original image I_o. This is achieved by adding the matrix $M_d(m, n)$ under modulus 256 with each of the matrices of the primary colors belonging to the image, that is,

$$I_d = (I_o(m, n, c) + M_d (m, n)) \bmod 256.$$

where I_d, is the blurred image.

Step 6: Generate two pseudo-random sequences of the positions of the rows and columns using the two chaotic states of the Hénon map, that is, of x and y of (1), these sequences of positions are represented by m_p and respectively.

Step 7: Permute the positions of the pixels in the image, which is achieved by performing the following operation

$$I_c(m, n, c) = I_d (m_p,n_p ,c)$$

where I_c is the permuted image.

Step 8: Save the encrypted image, that is I_c, as well as the DNA sequence obtained in step 2.

3.1.2 Decryption

In the decryption process, the reverse process is carried out, that is, first step 7 is carried out with the difference that now an inverse permutation will be carried out, that is $I_d (m, n, c) = I_c(m_p, n_p, c)$ and then step 5 with the difference that now a subtraction will be performed modulo 256, that is,

$$I_r= (I_d (m, n, c) + M_d (m, n)) \bmod 256.$$

where I_r, is the recovered image.

3.2 LSB data hiding

The most efficient method for steganography in images is the LSB method (Least Significant Bit or Less Significant Bit), in which, for each of the pixels that make up the image, its least significant bit is used to store information, and thus obtain an image practically the same as the original but with a hidden message in it. This method is one of the so-called substitution methods and consists of substituting the least significant bit, the last bit of each byte, of the pixels of an image for the bits of the information to be hidden. This process can be repeated with each byte of the image, spreading the message throughout the image without any difference being seen with the naked eye.

Table 1. Least significant bit "UC3M" characters least significant bit

ASCII	Decimal	Binary	Least Significant Bit
U	85	01010101	01010101
C	67	01000011	01000011
3	51	00110011	00110011
M	77	01001101	01001101

In the above table, which is the least significant bit of the "UC3M" characters? Now, hide a message in the least significant bit of each pixel of an image. The following steps illustrate how this method is used to hide the secret data "A" in cover image "Mansoura.bmp".

Step 1: Convert the secret data into binary form

$$[Message] \rightarrow Dec\ 2\ Bin \rightarrow [100001]$$

Step 2: From the cover image, read each pixel value

Step 3: Convert the pixel into binary form.

$$[10000001] \rightarrow is\ divided\ in\ to\ 8\ bits\ \rightarrow [1\ 0\ 0\ 0\ 0\ 0\ 0\ 1]$$

Step 4: Replace the LSB bit with secret bit.

Step 5: Repeat the step for all the pixels till the secret data is hidden completely.

3.3 Image Scrambling using Random Shuffling

Scrambling is a reversible digital stream conversion without changing the transmission rate in order to obtain properties close to those of a random sequence. The original message can be restored, scrambling to applying the reverse algorithm. Image scrambling (one of the kinds of encryption) is a good method for providing security to image data by making image visually unreadable and also difficult to decrypt it for unauthorized users.

3.3.1 Block-Wise Image Scrambling

This processing pipeline of block-wise image scrambling. Figure 3 illustrates the pipeline. In the developed system, an input image is first divided into blocks with B×B pixels, where the number of yielded blocks is N. For example, the segmentation of a 32×32 pixel image into blocks with 4×4 pixels yields 64 blocks. The positions of the segmented blocks are then shuffled (i.e., block shuffling). In addition, pixels in each block are shuffled with security keys, where different keys are applied to every blocks (i.e., block wise pixel shuffling). Finally, the blocks with the shuffled pixels are concatenated to obtain the resulting scrambled image.

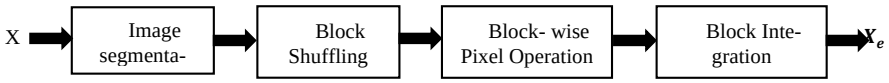


Fig.3. Processing pipeline of block-wise image scrambling. Image is segmented into bocks with B × B pixels. Block locations are shuffled, pixels in block are shuffled independently in every block, and shuffled blocks are concatenated.

3.3.2 Unscrambling

To restore the image to its pre-scrambled form, one must simply exchange roles of prepared data (our image) and repeat the scrambling steps with the same iteration numbers. This will successfully restore the image as long as the correct sets of puzzles and iteration numbers are used.

A block-wise pixel shuffling algorithm is proposed for the learnable image encryption. The procedure of the proposed block-wise pixel shuffling algorithm for 8-bit RGB image can be summarized as follow:

(i) The 8-bit RGB image is divided MxM-sized blocks.
(ii) Each block is split to the upper 4-bit and the lower 4-bitimages. Then, we have 6-channel image blocks.
(iii) Intensities of randomly selected pixel position are reversed.
(iv) Random pixel shuffle is applied.
(v) Encrypted image is restored.

4 Results and Discussion

This section presents the experimental results carried out to evaluate the proposed method. First the input patient details are selected. Figure 4 shows the process of selecting an input image. The user can select the patient details or exit the application.

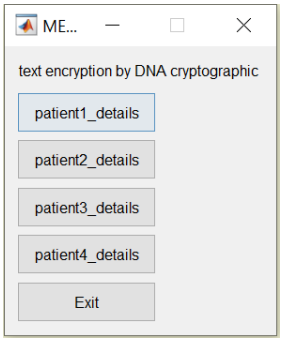


Fig. 4. Input patient details selection

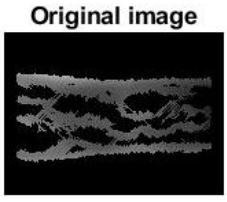


Fig. 5. Input image

Figure 5 shows the input image that is used for image stegongraphy and image encryption.

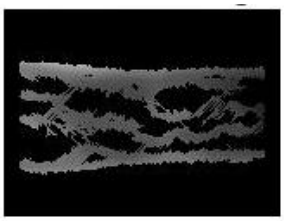


Fig 6. Data hidden image

Figure 6 shows the image which is embedded with secret information. The secrete information selected in figure 4 is encrypted using DNA encryption. This data is hidden using LSB data hiding.

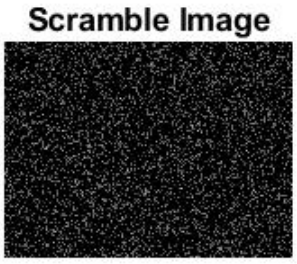


Fig. 7. Scrambled image

Figure 7 shows the scrambled output of the image shown in figure 6. This secret image is stored to improve the security.

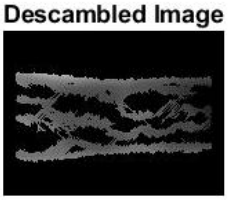
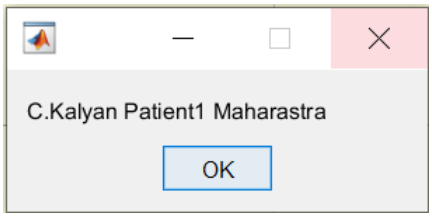
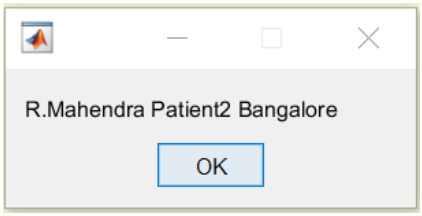


Fig. 8. Descrambled image

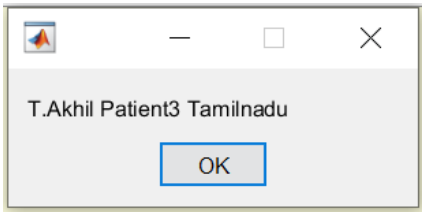
The descrambled image is shown in image 8. This image is used recognize the person.



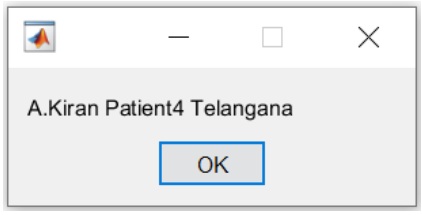
(a)



(b)



(c)



(d)

Fig. 9. Image matching output

5 Conclusion

Different from the traditional knowledge-based key technology to protect personal privacy, biometric identification uses the characteristics of the human body to perform identity authentication to achieve the purpose of ensuring the security of personal information. LSB method consists of hiding information in the least significant data bits of the object based on the mathematical functions used in the data compression and transformation algorithms. DNA encryption is used to encrypt the secret information. The stego image is ten encrypted using image scrambling. The result of the proposed model proves that the secret information and finger vein image both are secured.

References

[1] Liu, C. et al. (2019). Finger-Vein as a Biometric-Based Authentication. *IEEE Consumer Electronics Magazine*, 8(6): 29-34.

[2] Zhang, J., Lu, Z. and Li, M. (2020). Active contour-based method for finger-vein image segmentation. *IEEE Transactions on Instrumentation and Measurement*, 69(11): 8656-8665.

[3] Vásqucz-Villar, Z. J. et al. (2020). Finger Vein Segmentation from Infrared Images Using Spectral Clustering: An Approach for User Indentification. In *IEEE 10th International Conference on System Engineering and Technology (ICSET)*, 245-249.

[4] Kirchgasser, S. et al. (2020). Finger vein template protection based on alignment-robust feature description and index-of-maximum hashing. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 2(4): 337-349.

[5] Maser, B. and Uhl, A. (2021). Identifying the Origin of Finger Vein Samples Using Texture Descriptors. *arXiv preprint arXiv:2102.03992*.

[6] Madankar, M., Sawarkar, S. D. and Pete, D. J. (2018). Biometric Privacy Using Various Cryptographic Scheme. In *IEEE Global Conference on Wireless Computing and Networking (GCWCN)*, 159-162.

[7] Dwivedi, R. et al. (2020). A fingerprint based crypto-biometric system for secure communication. *Journal of Ambient Intelligence and Humanized Computing*, 11(4): 1495-1509.

[8] Shekhawat, S. et al. (2020). Efficient fingervein sample image encryption. In *8th International Workshop on Biometrics and Forensics (IWBF)*, 1-6.

[9] Evangelin, L. N. and Fred, A. L. (2021). Securing recognized multimodal biometric images using cryptographic model. *Multimedia Tools and Applications*, 80(12): 18735-18752.

[10] SanaIbjaoun, et al. (2017). Biometric template privacy using visual cryptography. In *International Conference on Innovations in Bio-Inspired Computing and Applications*, 309-317.

[11] Kakkad, V., Patel, M. and Shah, M. (2019). Biometric authentication and image encryption for image security in cloud framework. *Multiscale and Multidisciplinary Modeling, Experiments and Design*, 2(4): 233-248.

[12] Panchal, G., Samanta, D. and Barman, S. (2019). Biometric-based cryptography for digital content protection without any key storage. *Multimedia Tools and Applications*, 78(19): 26979-27000.

[13] Radhika, K. R. and Nalini, M. K. (2017). Biometric image encryption using DNA sequences and chaotic systems. In *International Conference on Recent Advances in Electronics and Communication Technology (ICRAECT)*, 164-168.

[14] Yang, W. et al. (2018). Securing mobile healthcare data: a smart card based cancelable finger-vein bio-cryptosystem. *IEEE Access*, 6: 36939-36947.

[15] Surse, N. M. and Jani, P. V. (2019). Finger-vein template protection using compressed sensing. *Innovations in Computer Science and Engineering*, 299-307. Springer, Singapore.