Indian Journal of Science and Technology, *Vol 7(S4), 8–14, April 2014*

ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Multi Level Encryption and Decryption Tool for Secure Administrator Login over the Network

Delson Therambath Rajanbabu[1*] and Chaithanya Raj[2]

[1]Electronics and Communication Department, Rajagiri School of Engineering & Technology,
Kochi, Kerala, India; delsontr@rajagiritech.ac.in
[2]Electronics and Communication Department, SNM Institute of Management & Technology,
Kochi, Kerala, India; chaithanyasuji@gmail.com

Abstract

Information security and data protection is the key topic of discussion in this research paper. This provides the importance of network security where the network administrator role is to prevent unauthorized or fraudulent activities on the computers connected on this network. For this, the primary task is to construct a double verification check tool for the administrator identity before getting login access to the network. We develop a Matlab based encryption tool which combines visual image encryption using template image fusion and symmetry cipher key cryptographic techniques for this purpose. This provides a reliable and also a simple algorithm tool ensuring data privacy and integrity of the information stored in the computers connected on the network.

Keywords: Data Privacy and Integrity, Information Security, Image Encryption, Symmetry Key Cryptography

1. Introduction

The traditional password or pin protected computer network is replaced by biometric security systems where the Local area network is protected by live fingerprint scanning of the administrator to ensure the prevention of unauthorized access to the computers in the network. However, by using low cost house hold items like gelatin, play-doh and wax, fingerprint images and finger models are constructed and fake the fingerprint system[1]. Therefore, comes more powerful algorithms and fingerprint sensors having additional hardware to check the liveness of the finger placed on the sensor. However, the development of the high level minutia verification algorithm and high cost models are not needed for a simple LAN owned by a network administrator. Another aspect of data protection in the computer network is to use a complex cryptography methods like AES, DES etc to encrypt the administrator password while enrolling into the network and decrypting the password at the verification stage to gain access into the network. But, in this case, if an intruder receives the private key exchanged between the encryption and decryption stage, gaining access into the network is quite simple. We proposed a method by fusing the original fingerprint image of the administrator by any other template image during enrolling stage and get the maximum intensity pixel of this fused image. In addition, a substitution cipher cryptography method is adopted where this fused image is encrypted by a cipher text and a private key is generated. During the verification stage of the administrator, the original fingerprint image is decrypted by providing the maximum pixel value of the center row of the original image stored in the database together with decryption key to get original decrypted

*Author for correspondence

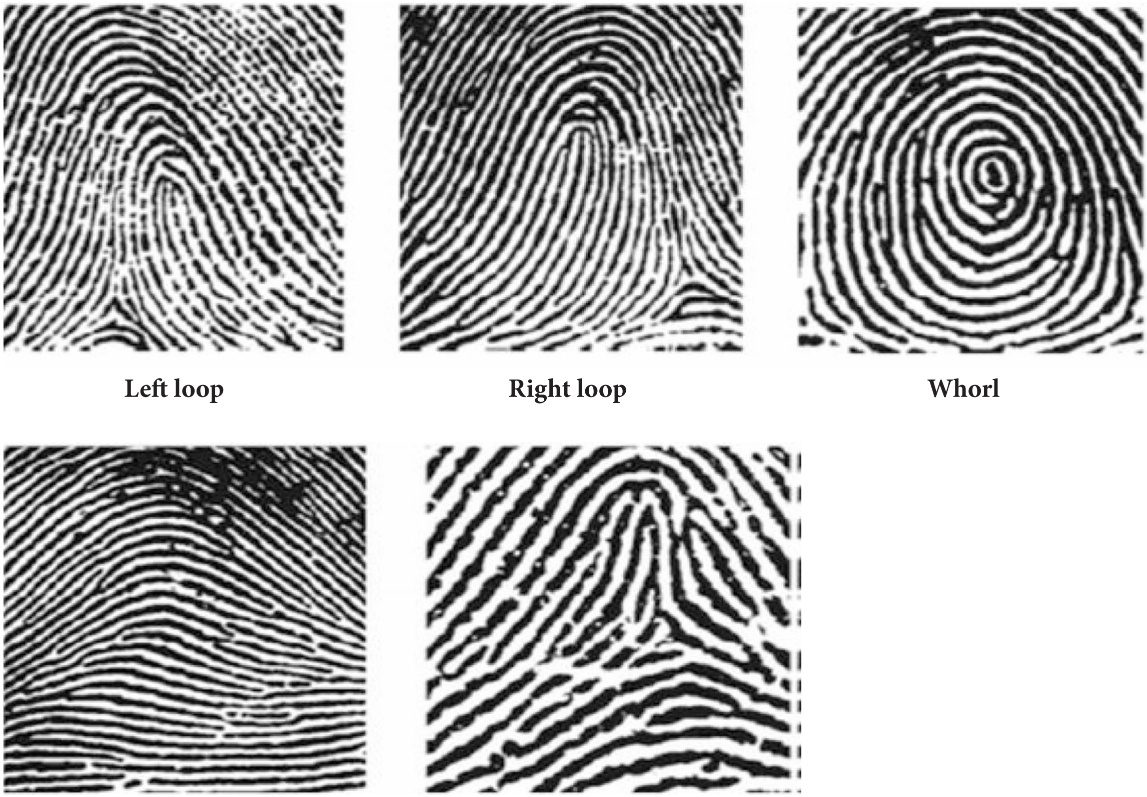
text stored in this fused image. If, all three, original image, maximum pixel value and the key is provided to the system, then the administrator will gain access into the network. Any fraudulent activity by an intruder is not possible to this environment. If the user develops a fake fingerprint model, he/she might not be aware of maximum pixel value of the fused image stored in the network. If the user succeeded in that, still he/she will be prevented from entry as it is needed to provide decryption key to break the data stored in the fused image.

2. Fingerprint based Personal Identification

Fingerprints are the patterns of ridges (black lines) and furrows (white lines) on the surface of the finger. Fingerprint details are permanent and unique as fingerprints are fully formed at about seven months of fetes development and finer ridge configurations do not change throughout the life of an individual except due to accidents such as bruises and cuts on the fingertips[2]. These features make fingerprints an important biometric identifier for personal identification system. Fingerprint classification in global perspective falls under five classes – left loop, right loop, whorl, arch and tented arch[3] as shown in Figure 1. Personal identification by determining the local features, minutia points in the fingerprints such as the ridge endings and bifurcations[4] is predominant than global features as the total number and positions of minutia points differs for each individual whereas global patterns can be alike for different persons. But, fingerprint image verification using minutia extraction requires filterization process, such as gabor filtering and mean, standard deviation estimation, orientation field determination of the image[5].

3. Cryptography Technique

Cryptography is the science of protecting data, which provides means and methods of converting data into unreadable form (encryption technique), so that only valid user can access data (decryption technique)[6].



Left loop

Right loop

Whorl

Arch

Tented arch

Figure 1. Global patterns – five major classifiers[3]

Encryption at the source and decryption at the receiver ensure secure transmission of message through the channel. But, several attacks like interception and modification of information content by an unauthorized person or an intruder can make the channel insecure for confidential data transfer.

Several cryptography algorithms like Caesar cipher (Substitution cipher) method, DES, AES exists. Caesar cryptography algorithm is the conventional cryptography technique where the secret cipher text is replaced or substituted for another character. It involves a secret key or a symmetric key used at encryption and decryption sides as shown in Figure 2. This technique is easy to implement and fast in encryption and decryption process.

However, more complex strong cryptography techniques like DES and AES algorithms required depending on the applications. Symmetry key to be handled at both encryption and decryption side. The use of substitution cipher method is that it is easy and simple to construct. A single bit encryption and decryption technique involved. It has drawbacks as there is a chance for an intruder to guess the key and decrypt the original text message. But, in our security model constructed this encryption decryption technique is added to improve the security level to allow the original administrator to login the network.

4. Proposed Algorithm Design

4.1 Block Diagram

We propose a combined approach of image fusion and cryptography techniques on the network administrator fingerprint image when placed on the fingerprint scanner for verification to gain access into the computer network. The algorithm takes two major directions, that of image differencing of the original fingerprint image (image encryption) and then encrypting this combined image with a cipher text and an associated key by symmetric substitution method. At the decryption stage, first the maximum pixel value of the combined image is verified and then the decryption key is entered. The block diagram of the proposed work described in Figure 3. If both these values are correct, the cipher text decryption is succeeded and also the image decryption of the original image from the template image is also succeeded. Finally, the access will be granted to the administrator.

4.2 Algorithm Steps

The algorithm design steps are provided below:

1. Original fingerprint image of the administrator is taken from a sensor with the resolution of 256×256 pixels size (image1).
2. Maximum pixel value at the center row of this image is computed by taking the row i = 256/2, which computes the maximum pixel at the row 128 (maxValue).
3. This maximum value pixel is taken as the threshold, because the image will be focused more on the center row and the maximum value pixel in that row. This value is subtracted with all other pixel values of the image and will get a darker image. But still the image is easily reconstructed by an intruder as the ridges and a furrow of the image is still clear (H=maxValue-image1).
4. Hence, another template image of size 256×256 (image2) is fused with this image by taking the

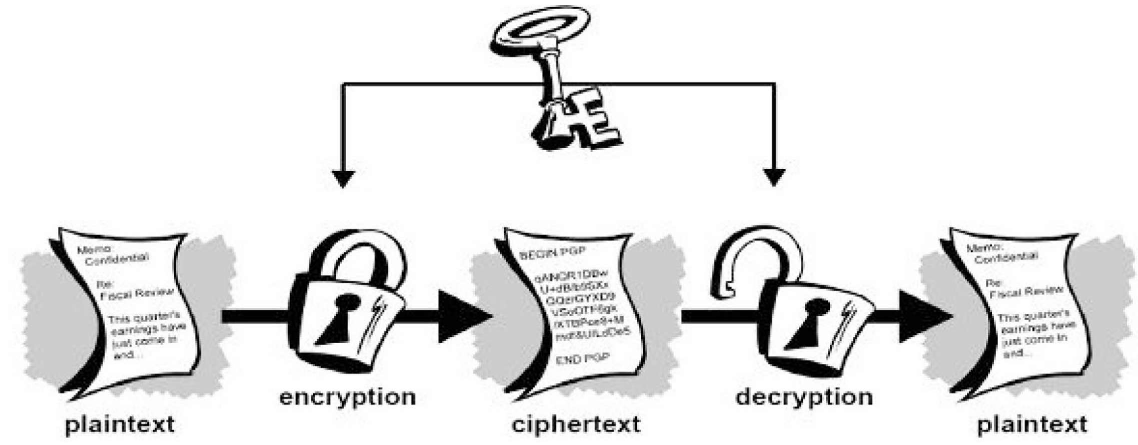
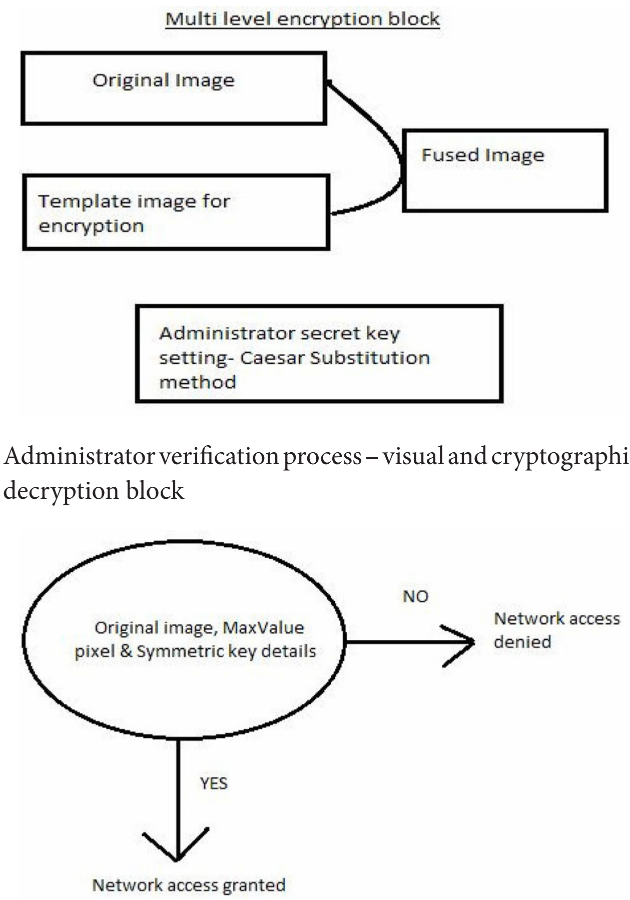


Figure 2. Symmetry key cryptography technique[4]


Multi level encryption block
Original Image
Template image for encryption
Fused Image
Administrator secret key setting- Caesar Substitution method
Original image, MaxValue pixel & Symmetric key details
NO
Network access denied
YES
Network access granted

Administrator verification process – visual and cryptographic decryption block

Figure 3. Proposed work block diagram

difference of the image with the template image. Now, this image is an encrypted image (B=H-image2). The template image is the image used for encryption.

5. Decryption of the original fingerprint image is possible by taking r as the maxValue and the computation, Q=r-H, where, Q is the decrypted original image.
6. This image encryption and decryption technique is simple to implement because of less algorithm design. So, we thought of adding one more encryption – decryption level security check through substitution cryptography (Caesar cipher encryption and decryption) technique. This is a fast and simple to implement, because it uses a symmetry key for encryption and decryption.
7. Here, a secret key is selected which is of single bit and this key is added to every bit of data for example if our Data is 'HELLO'. The secret key if selected is 2, H will be now J, E to G, L to N, O to Q.
8. First, Input is taken and the length of the string is calculated. Two dummy arrays say, array and input are declared. The x contains the ASCII values of characters (for example: - A =65, B=66 so on). Now the single alphabet from the variable x is calculated and the result is stored in the array input.
9. Now, the cipher key is entered by the user and then adds the key value one by one in input variable and save the result in array variable.
10. Now, in the Network access granted or denied to the administrator, granted only if the original fingerprint image is sensed by the sensor, maxValue and the decryption key of the cipher text also entered correctly.
11. The algorithm uses both visual encryption and also cryptographic cipher text hiding in the image. Visual encryption by template image fusion with original fingerprint image of the administrator and symmetry key cryptography by using single bit substitution cipher key cryptography technique.

5. Results and Discussions

We have used Matlab simulation environment (Version – 7.10.0) construct a GUI for the Multi-level encryption tool algorithm design. The menu of GUI consists of the provision to enter, the administrator original fingerprint image (for illustration, we say, a 256×256 pixel size or crop the image for this required size), template image (another fingerprint image, ideally a 256×256 pixel size), encrypted image (fusion of original and template image, differencing pixel values of template image with original image), decrypted original image(only if providing correct maxValue, say 244 be our administrator fingerprint image maxValue of the center row), Substitution or Caesar cryptography encryption and decryption facility (single bit symmetry key), network access granted or denied menu to the administrator by providing maxValue and cipher key entered in the command prompt of Matlab interface. The Matlab GUI and corresponding simulation results are given in Figure 4.

The simulation results are given in Figure 5.

In the simulation, we have used administrator original fingerprint image with the maxValue of the center row computed as 244 and the substation Caesar key as 3.

6. Conclusion and Future Scope

Multi level encryption and decryption tool developed in this paper provides a high degree of secure login into the computer network. An intruder or an unauthorized entry

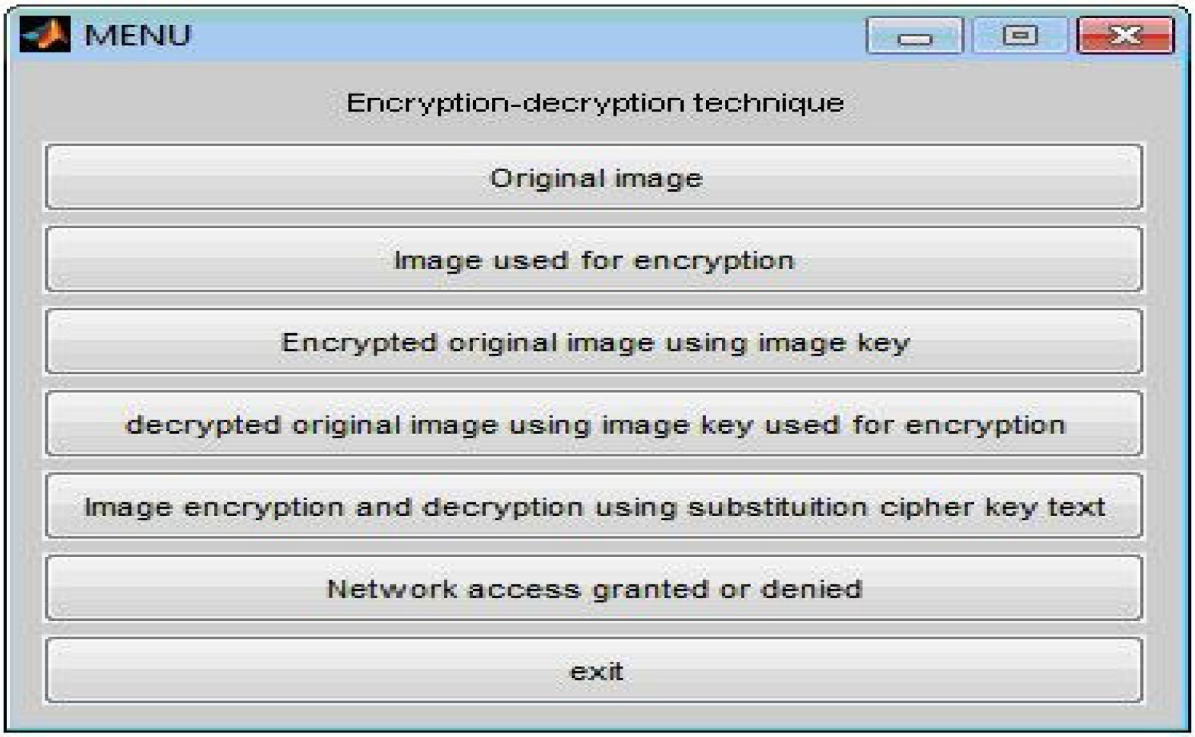
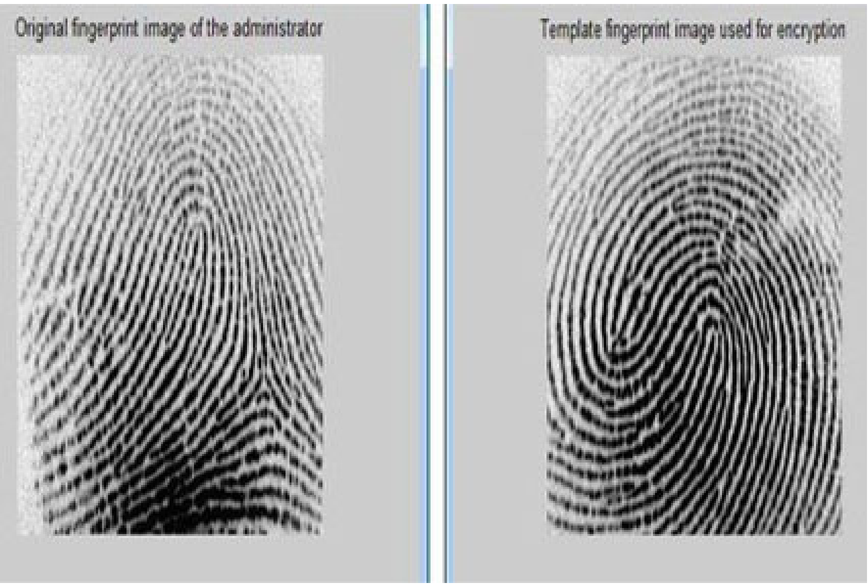
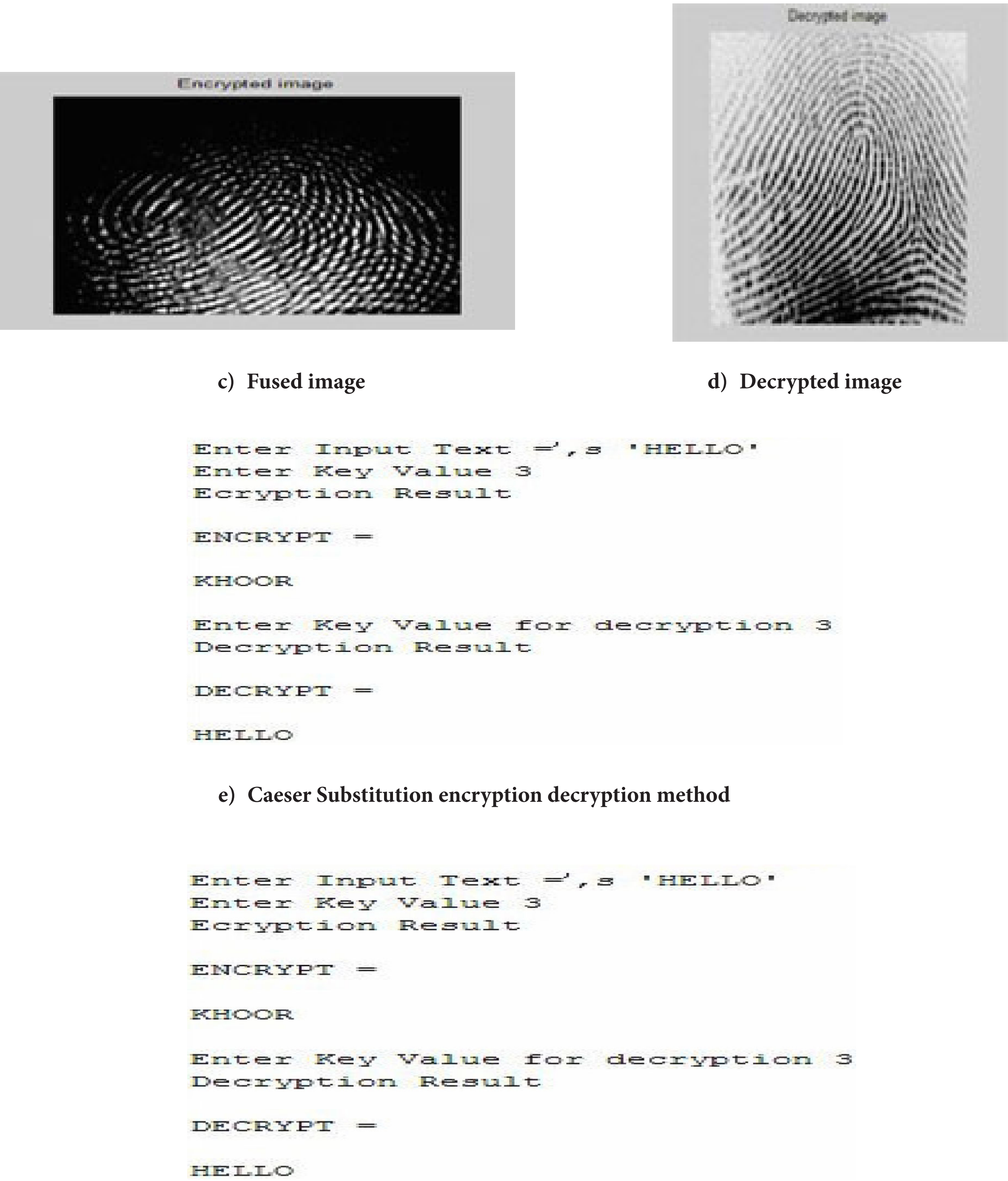

MENU
Encryption-decryption technique
Original image
Image used for encryption
Encrypted original image using image key
decrypted original image using image key used for encryption
Image encryption and decryption using substituition cipher key text
Network access granted or denied
exit

Figure 4. Matlab GUI for the algorithm design of multi level encryption and decryption tool for administrator login


Original fingerprint image of the administrator
Template fingerprint image used for encryption

a) Original fingerprint **b) Template image**



c) Fused image

d) Decrypted image

```
Enter Input Text =',s 'HELLO'
Enter Key Value 3
Ecryption Result

ENCRYPT =

KHOOR

Enter Key Value for decryption 3
Decryption Result

DECRYPT =

HELLO
```

e) Caeser Substitution encryption decryption method

```
Enter Input Text =',s 'HELLO'
Enter Key Value 3
Ecryption Result

ENCRYPT =

KHOOR

Enter Key Value for decryption 3
Decryption Result

DECRYPT =

HELLO
```

f) Network access granted by providing maxValue of the image and key value of substitution cipher

Figure 5. Simulation results of the proposed algorithm design

into the computer network can hijack privacy enabled data for example banking transaction passwords; medical records or even high values science and research materials. The possibility to restrict unauthorized entry into this network can be done by a simple password login for the administrator. But, as we know, a low level password if set by the administrator can be guessed and could attack the system. Better, to verify the administrator login the network using a biometric security system which prompts for the live biological samples of the individual to grant access into the secured area. Cryptography is another mathematical algorithm where an original text is enciphered or altered by a key at the source and the decryption of the original text is done at the receiver side. In this proposed model developed, a secret text of administrator choice is embedded into the fused image of the fingerprint and the template image. A symmetric key is chosen and the key is known for the administrator to gain access into the computer network where the network is monitored, controlled and maintain by this authorized administrator. The model is simple, easy to implement and fast in running the code execution as it involves the fingerprint global pattern verification, image encryption by template image fusion determining the maxValue of the center row of the original image and later the secret text and key embedding using single bit substitution cryptography method. Of course, some weakness such as the single bit encryption – decryption symmetry key and intruder possibility of guessing the key. The future scope of this work can be in the direction of fingerprint minutia extraction and strong cryptography method like DES OR AES cryptography standards.

7. References

1. Rajanbabu DT. Development of a simple fingerprint pattern verification method and construction of fake fingerprint image models. National conference Proceedings, ACC; 2012; Santhigiri College. p. 1–3.
2. Maltoni D, Maio D, Jain AK, Prabhakar S. Introduction - handbook of fingerprint recognition. Chapter 1. New York, USA: Springer Verlag; 2003 Jun.
3. Kulkarni JV, Jayadevan R, Mali SN, Abhyankar HK, Holambe RS. A new approach for fingerprint classification based on minutiae distribution. World Academy of Science, Engineering and Technology. 2008; 2(3):843–849.
4. Vatsa M, Singh R, Noore A, Houck MM. Quality-augmented fusion of level-2 and level-3 fingerprint information using DsM theory. International Journal for Approximate Reasoning. Jan 2008.
5. Jain AK, Prabhakar S, Hong L, Pankanti S.Filter-bank based fingerprint matching. IEEE Trans Image Process. 2000 May; 9(5):846–49.
6. Buba ZP, Wajiga GM. Cryptographic algorithms for secure data communication. Int J Comput Sci Secur. 2011; 5(2):227–243.