Open access Journal International journal of Emerging Trends in Science and Technology

Effective Cryptosystem Scheme Using Biometric Template

Authors

Shweta Hariharno[1], Mrs. Shikha Pandey[2]

[1]CSVTU University, Bhilai(Chhattisgarh)
Email-*shwetabandhekar3026@gmail.com*
[2]CSVTU University, Bhilai (Chhattisgarh) Department of Computer Science & Engineering
Email-*shikhamtech2008@gmail.com*

Abstract
Nowadays security is an important issue. Encryption and Decryption is a technique to ensure the security. Having secure and reliable means for communicating with videos and images is becoming a very necessity and its issues must be carefully considered. Hence, network security and data encryption have become important. Nowadays the images and videos are the most usable forms of encryption. There are two types of applications for information transmission over the Internet. The first ones are the online applications and next ones are the web pages, which consider the speed and security respectively as the main issue. In this thesis, encryption algorithms that can fulfil the requirements of these two applications were studied, and were adjusted to meet the requirements of image encryption by using the bio-metric template i.e. palm print. Bio-metric authentication systems are widely used in order to provide authentication without possessing any physical materials. Bio-metric authentication systems are mainly concentrating on security, privacy, and accuracy. In this thesis, propose a provably two way secured biometric authentication system, which concerns of user's privacy, protection, trust issues, network security, and accuracy. The two way secured means, biometric details are going to be encrypted twice i.e. double encryption. In this system two different encryption algorithms have been used. One is private key cryptography another one is public key cryptography. Authentication by using two way encryption will give additional security when comparing with existing system
Index Terms— Biometric, Image encryption and decryption, Image processing, Palm print.

1. Introduction

In our daily lives, there is a frequent need in identifying people correctly and verifying their identicalness. To emphasize, reliable identification mechanisms are required when people across the board, perform financial operations, desire to enter secure places etc. For higher efficiency and increased security, this identification mechanism should be automated. Obviously, high accuracy is required during the identification and this hardens the automation of identification. But once automated, it gives us the opportunity that tasks performed by computers and other devices can be widened and this results in easing our lives. It is here worth noting that, tasks performed by these devices are based on two separate mechanisms, namely authentication and authorization. Authentication is known as identity verification, whereas authorization defines particular rights of authenticated people. Therefore, authorization follows authentication.

There are three basic principles of authentication[1]:

1.What you know,which generally refers to information to be kept secret such as passwords or some non-secret private information such as mother's maiden name.

2.What you have, which generally refers to physical possessions such as keys and smartcards.

3.What you are, which generally refers to biometrics, physical appearances or behavioral characteristics of individuals such as fingerprint, hand geometry and signature.

Here we will discuss about the biometric authentication, biometric system, biometric template protection, security and privacy, palm print and feature extraction.

Features for good biometric authentication system

There are some features of biometric authentication system, these are:

1) Template protection- It is the process of storing biometric information securely, it should be protected from various types of attacks. Critical information could be revealed if the server's biometric template database is compromised.

2) User's privacy- Each and every individual has unique biometrics, so the privacy of the user can be easily maintained.

3) Trust between client and server- Sometimes client and server have disbelief on each other. Denial of service should be overcome by using public key cryptography.

4) Accuracy- False acceptance rate (FAR) and False rejection rate (FRR) should be minimized.

2. Review of Literature

For the last fifteen years Palm print recognition has been done. During this period, the problems related to the field came in to existence. Various verification algorithms were focused upon by research person. They proposed so many feature extraction and matching algorithms. For achieving high verification accuracy, researchers combined different

biometric traits and different features in palm prints. Research persons also told about the problems which were more challenging for real-time palm print identification in large databases. Accuracy and recognition speed are important in this context. Biometric community has also paid attention on the security of biometric systems. To protect palm print systems pioneers have proposed some measures. In addition to summarize the current palm print research, other related issues like privacy are being discussed.

2.1 Overview of Palm print Recognition Systems

The inner surface of palm contains three flexion (i) creases (ii) secondary creases and (iii) ridges. The flexion creases and secondary creases are also known as principal lines and wrinkles respectively. The main creases and flexion creases are formed between the 3rd and 5th months after conception and superficial lines appear after birth. Genetically we cannot find these creases. Even identical twins who have different palm prints but share the same DNA sequences.

There are two types of palm print recognition research these are:

I. high resolution
II. low resolution

High and low resolution approach includes high and low resolution images. High resolution approach is suitable for forensic applications such as criminal detection, while low resolution is more suitable for commercial and civil applications such as access control. High and low resolution stand for 400 dpi or more and 150 dpi or less respectively. Figure 2.1 shows a part of a high and low resolution palm print image. In high resolution images, researchers can use ridges, minutia points, and singular points as features, in contrast low resolution images; they use principal lines, texture and wrinkles. At the launching, the high- resolution approach was the focus but almost all current research is focused on the low resolution approach because of the potential applications.

A palm print recognition system consists of five parts, these are : (i) palm print scanner (ii) preprocessing (iii) feature extraction (iv) matcher and (v) a database. Palm print scanner is to collect palm print images. Preprocessing is to setup a coordinate system to align palm print images and for feature extraction to segment a part of palm print image. Feature extraction is to find effective features from the preprocessed palm prints. Finally, a matcher compares two palm print features. All the images, templates generated are stored in a local or remote database.

2.1.1 Palm print Image Acquisition

It is the first process in palm print recognition systems. Researchers use four different types of sensors to collect palm print images, CCD-based palm print scanners, digital cameras, digital scanners and video cameras. Figure 2.2 shows a CCD-based palm print scanner developed by the Hong Kong Polytechnic University [15]. Generally speaking, CCD-based palm print scanners detention high quality palm print images. Digital scanners are cost-effective to capture the palm print images. In spite of this, they cannot support real-time verification because of the scanning time. Digital and video cameras are two ways to collect palm print images without any connection. Figure 2.3(a) is a palm print image collected by a CCD-based palm print scanner and Figure 2.3(b) shows palm print image captured by a digital scanner.

2.1.2 Palm print Preprocessing

Preprocessing is used to align different palm print images and for feature extraction to segment the central parts. To set up a coordinate system, most of the preprocessing algorithms occupy the key points between fingers. It consists five common steps, (1) binarizing the palm images, (2) extracting the contour of palm and/or fingers, (3) detecting the key points, (4) establishing a coordination system and (5) extracting the central parts. Figure 2.4 (a) illustrates the key points and Figure 2.4 (b) shows a preprocessed image. The first and second steps are same in all the preprocessing algorithms. On the other hand, the third step has several different implementations including tangent-based [15] and wavelet-based [16]. All these approaches uses only the information on the fingers boundaries. After finding the coordinate systems, central parts of palm prints are segmented. For feature extraction several kind of preprocessing algorithms are used.

Figure 2.2: A CCD-based palm print scanner

2.1.3 Palm print Feature Extraction

A lot of work has been done for developing feature extraction algorithms. D. Zhang et al. have used datum point and line features for palm print verification system [17]. Li et al. have used Fourier transform for feature extraction of palm prints [12]. Kong et al. have proposed palm print feature extraction using 2-D Gabor filters [14]. Gan et al. have applied wavelet transform for palm print recognition [18]. Wu et al. have proposed palm print texture analysis using Derivative of Gaussian filters [19].

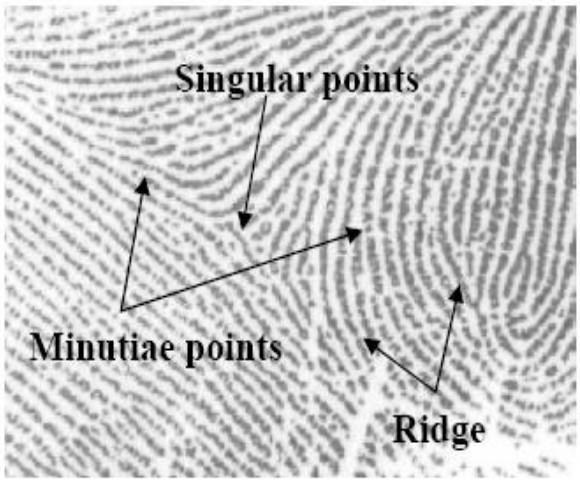
2.1.4 Palm print Matching

There has been lot of works on palm print matching. Many existing classifiers including neural networks [16], various measures are also existing such as cosine measure, weight Euclidean distance, hamming distance, Euclidean distance, and nearest neighborhood distance have been examined [12-19].

2.2 Privacy and Security of Biometric Systems

Biometric traits contain information not only for personal identification but also for other applications. For example, deoxyribonucleic acid (DNA) and retina are useful for diagnosing genetic problems and diabetes, respectively. Palm prints are also related to some genetic disorders and are used by fortune-tellers or palmists to predict the characteristics of

the individuals. To protect the private information in palm prints, databases have to store templates and encrypted palm print images, because of the line features.



(a)

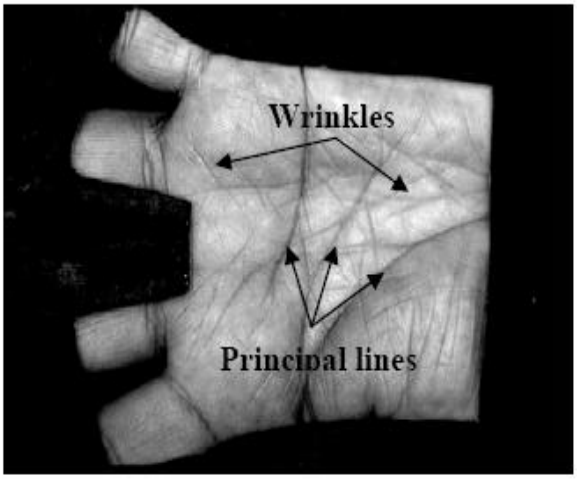


Figure 2.1: Palm print features in (a) a high resolution image and (b) a low resolution image

3. Problem Identification

3.1 Problem Identification

The basic problem in an image encryption is security, when we use private or public attackers, can attack our network and can modify information sent by the client or sender. Symmetric-key cryptography is a technique in which the sender and receiver share a single key that is used to encrypt and decrypt the message . The modern study of symmetric-key ciphers relates mainly to the study of stream cipher and block cipher and to their applications. A stream cipher is a symmetric key cipher where plaintext digits are combined with a pseudorandom (A pseudorandom process is a process that appears to be random but is not) cipher digit stream. In a stream cipher each plaintext digit is encrypted one at a time with the corresponding digit of the key stream. A block cipher is a deterministic algorithm operating on fixed-length groups of bits, called blocks. Block ciphers are commonly used to implement encryption of bulk data; it is important elementary components in the design of many cryptographic protocols. In a sense block ciphers take as input a block of plaintext and a key, and generates same size cipher text output. Since messages are always longer than a single block.

The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are block cipher designs which have been designated cryptography (though DES's designation was finally withdrawn after the AES was adopted)[14]. In contempt of its depreciation as an official standard, DES remains quite popular; it is used across a wide range of applications; many other block ciphers have been designed and released, with considerable variation in quality. Many have been thoroughly broken. Stream ciphers, in contrast to the 'block' type, create long stream of key material, which is combined with the plaintext as bit and character wise. Widely used stream cipher name is RC4. Block ciphers can be used as stream ciphers. Cryptographic hash functions are a third type of cryptographic algorithm. They take a message of any length as an input, and an output short. The quality of hash functions is, attacker cannot find two messages that construct the same hash. A long-used hash function is MD4 but it is broken by MD5. MD5 is an advanced variant of MD4. The Secure Hash Algorithm series of MD5-like hash functions developed by the U.S. National Security Agency, MD5 is much like cryptographic hash functions The MD5 message-digest algorithm is a widely used cryptographic hash function producing a 128-bit hash value, it has been utilized in a cryptographic applications. It is also commonly used to verify data integrity. SHA-0 was a flawed algorithm that the agency withdrew; SHA-1 is widely used and more secure than MD5, but analysts have identified attacks against SHA-1; the improvement on SHA-1 is SHA-2, but it is not commonly used till now. To provide more security we are using Biometric system i.e. palm print with the help of Double encryption scheme. Fingerprint identification has drawn considerable attention over the last 25 year. In spite of this, some people do not have clear fingerprints because of their physical work (hard work) or problematic skin. The accuracy and uniqueness of 3-D hand geometry are still open questions. Iris and retina recognition provide very high accuracy but suffer from high costs of input devices or intervention into users. Now, many researchers have focused on face and voice verification systems; nevertheless, their performance is still not acceptable.

4. Methodology

Nowadays biometric authentication systems are very useful and widely used because they offer several advantages over classical knowledge-based and token-based personal identification approaches. In spite of this, biometric systems are easy target to various attacks; such attacks must be analyzed before biometric systems are extremely deployed in security systems. Cryptography is one possible solution that would allow us to better protect against replay. Systems are protected by cryptography and also to store and transmit only encrypted templates in databases and through data links. I have proposed a cryptographic approach for encrypting the images to protect the privacy of the users and also to embed the security into the images with the help of palm print images. In this thesis, image has been encrypted with the help of double encryption system. First of all a sample input image has been taken and this image will be encrypted by AES algorithm, AES generates the key and I am using palm

print i.e. biometric template instead of AES as a key. Here palm print is working as a password. These palm prints generate the key for images using MD5 hash function, MD5 generates the 128 bit key called certificate. For generating the key, feature vector (i.e. 5*5 matrix) has been used to reduced the size of palm print. Random number, Maximum number and class (feature extraction technique decides the classes of all palm images) are taken. Range of random number is between 0 to 1, maximum number is 65535 (which we can change, once the maximum number is chosen will be fix for the whole process) and the class decides number of palm per person. This feature vector generates the temporary key, now MD5 hash function uses this temporary key and generates 128 bit hash numbers (key).These 128 bit hash numbers (generated by MD5) will be again encrypted by the RSA algorithm and finally this key will be the AES key and image will be encrypted.

5. Result and Discussions

The implementation of the system consists of double encryption cryptosystem using palm print. The data set consists of 1150 data values for left and right hand, out of which first 920 are used for training and rest of data set are used for testing. The palm print database consisted of the left and right hand images from the 230 users and five images from each of the users were employed. The first enrolled palm print image from each of the users was in use. The successful opening with the rest of the enrolled palm print image of the same user was considered as genuine match while opening with all the other enrolled test images from other enrolled users (*i.e.* 230 users) were considered as pretender matches. Following figure shows the proposed system:

Figure 5.1 shows the layout of the proposed system.

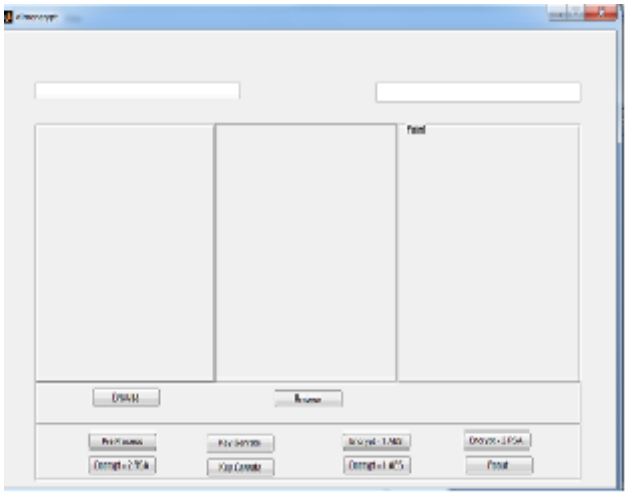


Figure 5.1: Layout of the proposed system

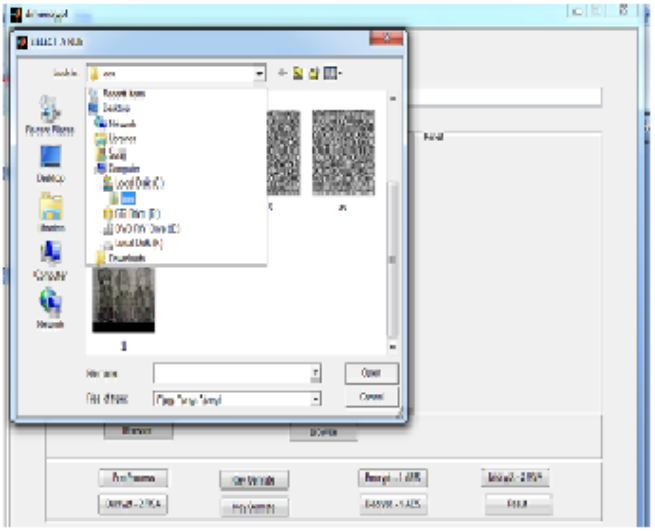


Figure 5.2: Taking an input image

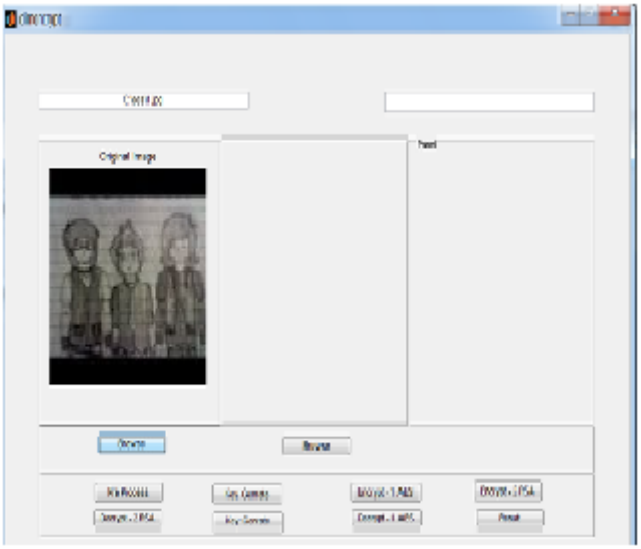


Figure 5.3: The input image for encryption

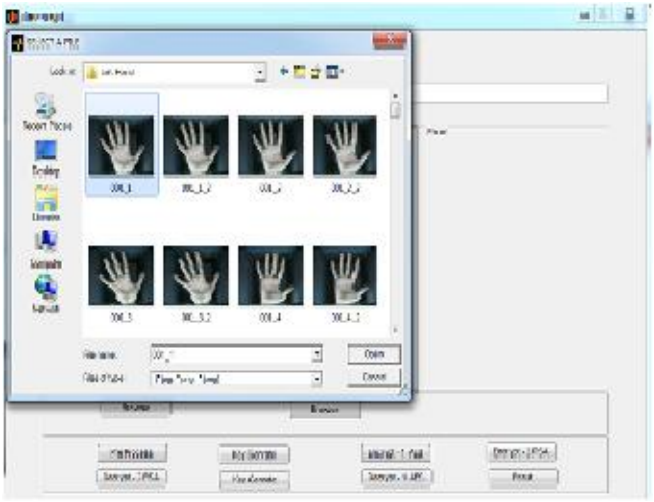


Figure 5.4: Generating Key Using Palm Print for Encryption

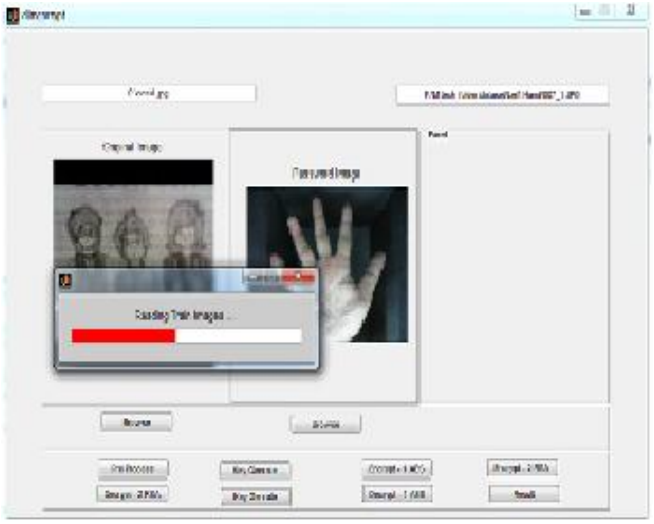


Figure 5.5:Reading train images(PreProcess)

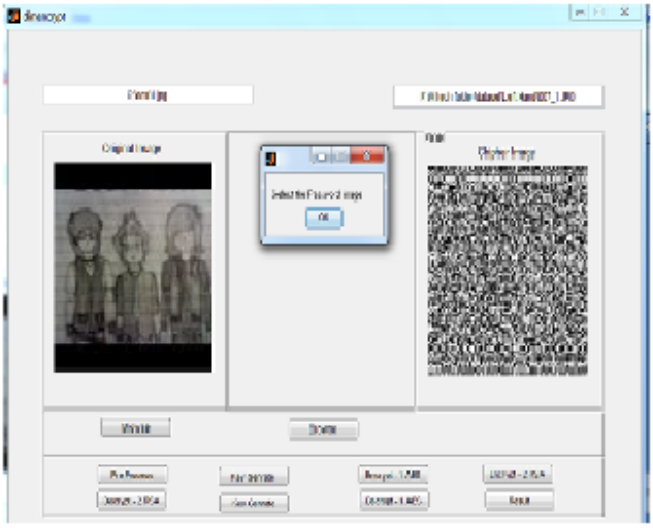


Figure 5.8: Select password image

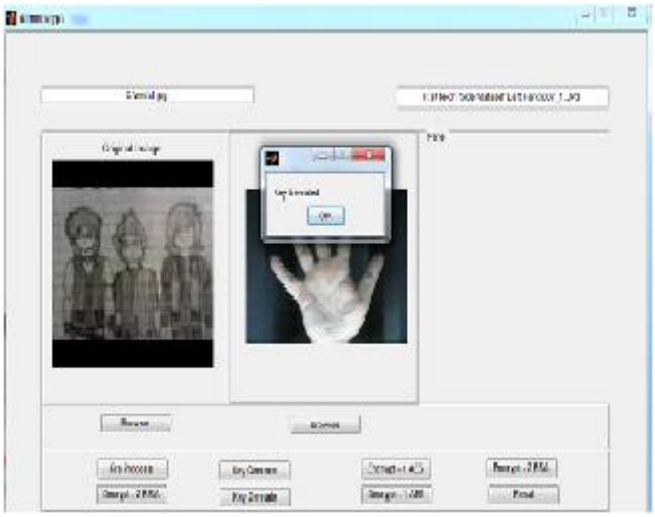


Figure 5.6: Generated key

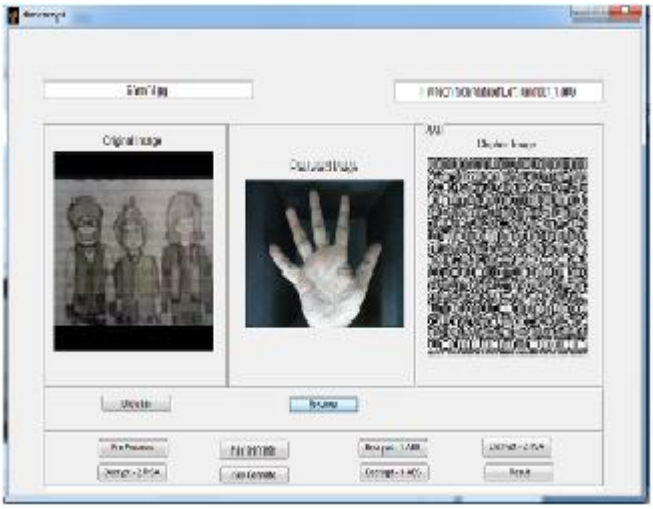


Figure 5.9: Password image for decryption

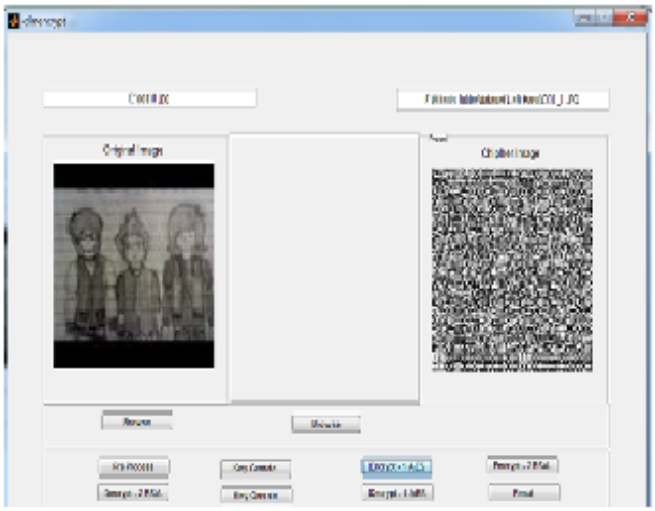


Figure 5.7: Encrypted image

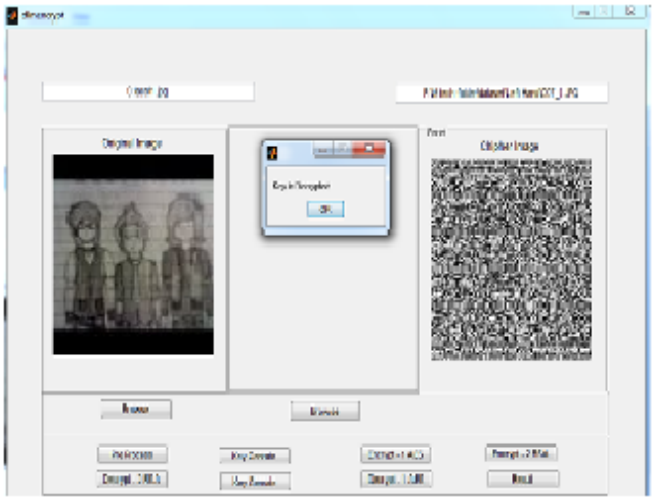


Figure 5.10: Decrypted key generated

Figure 5.11: Image Decrypted

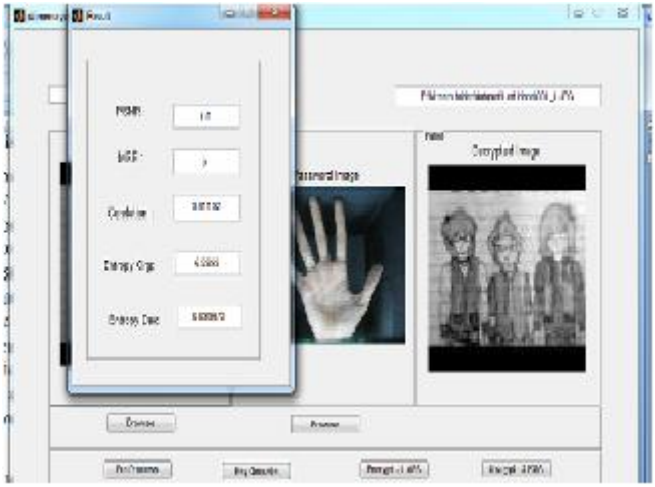


Figure 5.12: Final result(output)

Final result are discussed below:

- **PSNR and MSE**

The PSNR block computes the peak signal-to-noise ratio, in intensity, between two images. This ratio is often used as a quality measurement between the original and a compacted image. Higher PSNR provides better quality of the compressed or reconstructed image.

The *Mean Square Error (MSE)* and the *Peak Signal to Noise Ratio (PSNR)* are the two error metrics used to compare image compression quality. The MSE represents the cumulative squared error between the compressed and the original image, while PSNR represents a measure of the peak error. Error depends on the lower MSE value .

To calculate the PSNR, the block first calculates the mean-squared error using the following equation:

$$MSE = \frac{\sum_{M,N}[I_1(m,n)-(I_2(m,n)}{M*N}$$

Where *M* and *N* are the number of rows and columns in the input images, respectively. Then the block computes the PSNR using the following equation:

$$PSNR = 10 \log_{10} \frac{R^2}{MSE}$$

Where *R* is the maximum fluctuation in the input image data type. For example, if the input image has a double-precision floating-point data type, then *R* is 1. If it has an 8-bit unsigned integer data type, *R* is 255, etc.

- **The Correlation Coefficient:**

A functional measure to evaluate the encryption quality of any image cryptosystem is the correlation coefficient between pixels at the same indices in the plain and the cipher images. This metric can be calculated as follows:

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(X)\sqrt{D(Y)}}}$$

where x and y are the gray-scale values of two pixels at the same indices in the plain and cipher images. In numerical computations, the following discrete formulas can be used:

$$E(x) = \frac{1}{L}\sum_{i=1}^{L} X_l$$

$$D(x) = \frac{1}{L}\sum_{i=1}^{L}(X_l - E(x))^2$$

$$Cov(x,y) = \frac{1}{L}\sum_{i=1}^{L} X_l - E(x)(Y_1 - E(y))$$

Where L is the number of pixels implicated in the calculations. The closer value of r_{xy} to zero is the better the quality of the encryption algorithm.

Entropy

Entropy is a measure of the loss of information in a transmitted signal or message, Shannon demonstrated mathematical methods of treating communication channels, bandwidth, and the effects of random noise on signals

$$H(X) = -\sum_{i=1}^{n} p(x_i) log_b\, p(x_i)$$

Where $\mathbf{p_i}$ is the probability of a given message (or piece of information) and **n** is the number of possible messages (or pieces of information).

6. Conclusion

6.1 Conclusion

A new image encryption and decryption scheme based on palm print has been proposed in this project. Using palm print features this project has investigated a new approach to construct the cryptographic system. The implementation of double encryption has been suggested in order to combine cryptography with palm prints. This can efficiently reduce the possibility of hacking within a cryptosystem. This scheme allows, sender sends a secret image to the receiver over the open network, yet lots of intruders listen. For that reason, this scheme may be useful in many applications. This scheme gives reliable security. The salient features of the proposed asymmetric image encryption proposal can be summarized as: (a) Lossless encryption of image. (b) Less computational complexity. (c) Convenient realization (d) Choosing a suitable size of matrix according to the size of image. It requires minimized computational resources [23]. We can execute this system in various fields like Military, protection, and other places where the confidentially of data should be must

References

1. Aloha Sinha, Kehar Singh, "A technique for image encryption using digital signature", Optics Communications, 2003, 1-6.

2. Biometric Security Concerns CESG UK Biometric Working Group, Tech. Rep., 2003 [Online]Available:http://www.cesg.gov.uk/policy_technologies/biometrics/media/biometricsecurityconcerns.pdf, Retrieved Oct., 2008
3. S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," *IEEE Security Privacy Mag.*, vol. 1, no. 2, pp. 33–42, Mar./Apr. 2003.
4. E. Mordini, "Biometrics, human body and medicine: A controversial history," in *Ethical, Legal and Social Issues in Medical Informatics*, P. Duquenoy, C.George, andK.Kimppa, Eds. Hershey, PA: Idea Group Inc., 2008, pp. 249–272.
5. R. Cappelli, A. Lumini, D. Maio, and D. Maltoni, "Fingerprint image reconstruction from standard templates," *IEEE Trans. PAMI*, vol. 29, no. 9, pp. 1489–1503, Sep. 2007.
6. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *Special Issue on Biometrics, EURASIP J. Adv. Signal Process.*, pp. 1–17, Jan. 2008.
7. C.S. Laih, and K. Y. Chen, "Generating visible RSA public keys for PKI",InternationalJournal of Information Security, Vol. 2, No. 2, Springer-Verlag, Berlin, (2004), pp. 103-109.
8. S.S.Maniccam, N.G. Bourbakis, "Losslessimage compression and encryption using SCAN",Pattern Recognition 34 (2001), 1229-1245
9. X.Y. Jing and D. Zhang, "A face and palmprint recognition approach based on discriminant DCT feature extraction", IEEE Transactions on Systems, Man, and Cybernetics Part B: Cybernetics, vol. 34, no. 6, pp. 2405-2415, 2004.
10. L.S. Penrose, "Fingerprints and palmistry", The Lancet, vol. 301, no 7814, pp. 1239- 1242, 1973.
11. I.Ozturk, and I. Sogukpinar, "Analysis and Comparison of Image EncryptioAlgorithms", International Journal of Information Technology, Vol. 1, No. 2, (2005), pp. 64-67.
12. D. Zhang and W. Shu. Two novel characteristics in palm print verification: Datum point invariance and line feature matching. *Pattern Recognition*, 32(4):691{702, 1999}.