International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 14
November 2017

A Novel Approach For Biometric Based Encryption By Using Distance Based Encryption

P.Sridharbabu & Ch. Madhava Rao

[1] M-TECH, ECE Department, SIR C R REDDY College of Engineering-eluru, A.P.
[2]Assistant Professor, ECE Department, SIR C R REDDY College of Engineering-eluru, A.P.

ABSTRACT

A new encryption notion called distance-based encryption (DBE) to apply biometrics in identity-based encryption. In this notion, a cipher text encrypted with a vector and a threshold value can be decrypted with a private key of another vector, if and only if the distance between these two vectors is less than or equal to the threshold value. The adopted distance measurement is called Mahalanobis distance, which is a generalization of Euclidean distance. This novel distance is a useful recognition approach in the pattern recognition and image processing community. The primary application of this new encryption notion is to incorporate biometric identities, such as face, as the public identity in an identity-based encryption. In such an application, usually the input biometric identity associated with a private key will not be exactly the same as the input biometric identity in the encryption phase, even though they are from the same user. The introduced DBE addresses this problem well as the decryption condition does not require identities to be identical but having small distance. In this paper, we study this new encryption notion and its constructions. We show how to generically and efficiently construct such a DBE from an inner product encryption (IPE) with reasonable size of private keys and ciphertexts. We also propose a new IPE scheme with the shortest private key to build DBE, namely, the need for a short private key. Finally, we study the encryption efficiency of DBE by splitting our IPE encryption algorithm into offline and online algorithms.

INTRODUCTION

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.

While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck Cryptanalysts are also called attackers.

Cryptology embraces both cryptography and cryptanalysis. ” There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files. Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet.

Within the context of any application-to-application communication, there are some specific security requirements, including:

- Authentication: The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)
- Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver.

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 14
November 2017

- Integrity: Assuring the receiver that the received message has not been altered in any way from the original.
- Non-repudiation: A mechanism to prove that the sender really sent this message.

Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions, each of which is described below. In all cases, the initial unencrypted data is referred to as plaintext. It is encrypted into cipher text, which will in turn (usually) be decrypted into usable plaintext.

In many of the descriptions below, two communicating parties will be referred to as Alice and Bob; this is the common nomenclature in the crypto field and literature to make it easier to identify the communicating parties. If there is a third or fourth party to the communication, they will be referred to as Carol and Dave. Mallory is a malicious party, Eve is an eavesdropper, and Trent is a trusted third party.

Public-Key Cryptography:

Public-key cryptography has been said to be the most significant new development in cryptography in the last 300-400 years. Modern PKC was first described publicly by Stanford University professor Martin Hellman and graduate student Whitfield Diffie in 1976. Their paper described a two-key crypto system in which two parties could engage in a secure communication over a non-secure communications channel without having to share a secret key.

Key exchange, of course, is a key application of public-key cryptography (no pun intended). Asymmetric schemes can also be used for non-repudiation; if the receiver can obtain the session key encrypted with the sender's private key, then only this sender could have sent the message. Public-key cryptography could, theoretically, also be used to encrypt messages although this is rarely done because secret-key cryptography operates about 1000 times faster than public-key cryptography.

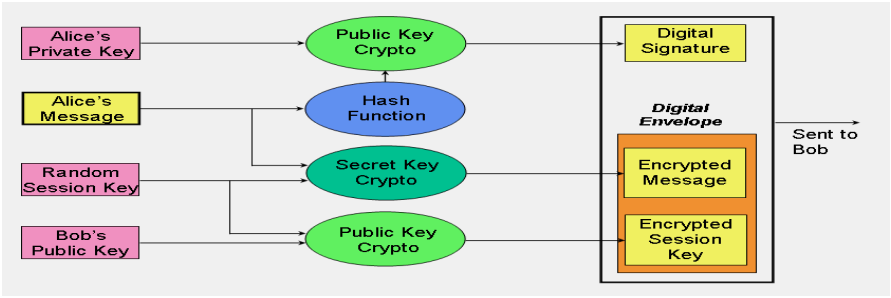


Figure 1: Sample application of the three cryptographic techniques for secure communication.

Figure: 1 puts all of this together and shows how a hybrid cryptographic scheme combines all of these functions to form a secure transmission comprising digital signature and digital envelope.

A digital envelope comprises an encrypted message and an encrypted session key. Alice uses secret key cryptography to encrypt her message using the session key, which she generates at random with each session. Alice then encrypts the session key using Bob's public key. The encrypted message and encrypted session key together form the digital envelope. Upon receipt, Bob recovers the session secret key using his private key and then decrypts the encrypted message.

PREVIES METHOD

Fingerprint:

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 14
November 2017

Fingerprints are the oldest traits that are mostly represented as friction minutiae- based features while systems are rarely designed to use an entire image of a fingerprint. Thus, a fingerprint of a user consists of a set of unordered features called as fingerprint minutia. Each minutia is assumed to be represented by its 2D spatial location and its local orientation. Discontinuities in the flow of ridges (ridge bifurcations and endings) constitute the minutiae. The following figure2: shows a sample fingerprint image with overlaid minutiae.

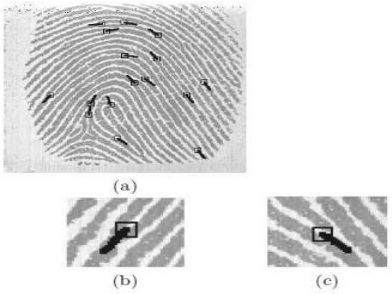


Figure 2: Fingerprint Minutia

The main difficulty within fingerprint biometrics is in finding specific fingerprint orien- tation and its center. Otherwise, all calculations resulting out of minutiae are destined to be orientation/position-dependent. Thus, the matching algorithm has to deal with transformations of fingerprint data by aligning fingerprint images using high curvature points and orientation lines.

In the systems we consider, fingerprints are represented by the cartesian coordinates of the fingerprint minutia features, where the couples of coordinates are concatenated to single numbers that are mapped to the elements of a finite field by some convention

Face :

In a face recognition system, images of the whole face of a person are captured out of which unique key features are extracted to identify persons reliably. The acquired set of key features includes relative distances between characteristics such as eyes, the nose, the mouth, cheekbones and the jaw. Using all of this information, a unique template is created by applying dimension reduction. the ordered set of face features are obtained through the segmentation of regions and lines of interest, feature extraction from the segmented regions and lines, and classification of the feature vectors that model the faces. In figure:3, the segmentation of regions and lines of interest of a face model is shown.

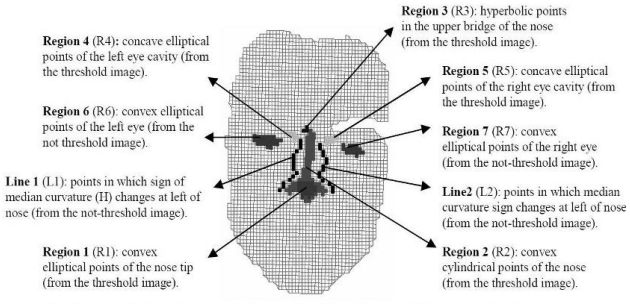


Figure 3: Segmented regions and lines of a face from which facial features are ex-tracted

Biometric Cryptosystems

Combination of biometrics and

cryptography is achieved under different names: Un- traceable Biometrics, Biometric Encryption (BE), Fuzzy Extractor, Secure sketch, Helper Data Systems, Biometric Locking, Biometric Key Generation, etc. Despite the different names, the goal of these systems is the same: Biometric Template Protection., we see an overview of these systems.

One approach focuses on the BE technologies that securely bind a digital key to a bio- metric, or extract a key from the biometric so that neither the key nor the biometric can be retrieved from the stored BE template, also called "helper data" The key is re-created only if a correct biometric sample is presented on verification; and the output of BE verification is either a key (correct or incorrect) or a failure message. There is always a biometric dependent helper data stored in the system, but the cryptographic key is not kept at all. In practice, BE, like any biometric system, has both false rejection and false acceptance rates (FRR and FAR). We note that BE does not use any matching score; instead, the FRR/FAR tradeoff may be achieved in some cases by varying the parameters of the BE scheme.

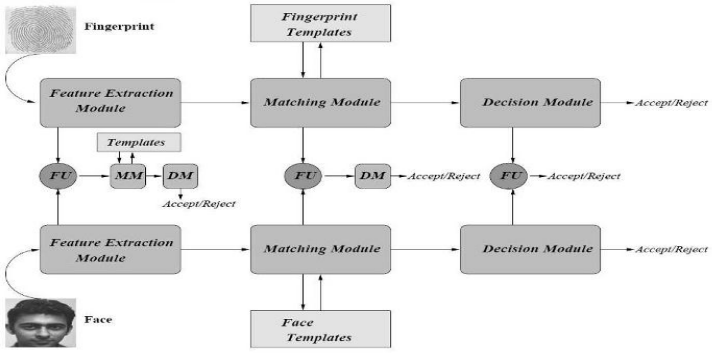


Figure 4: Levels of fusion in a bimodal biometric system

A different line of research is Cancelable Biometrics (CB), which is closer to a conven- tional biometric system. CB technologies apply a secret transform to the biometric. The transform can be invertible or not, and both the transformed template and the secret transform are stored. On verification, the same transform is applied to a fresh biometric sample, and two transformed templates are matched, where the output of CB verification is a Yes/No response.

Recently, biometrics is combined with traditional encryption schemes such as ElGamal- type encryption schemes to obtain secure authentication/fuzzy IBE systems that as- sume biometrics as public data. These systems provide provable security guarantees since they are designed according to a formal security model with a security reduction to a hard problem. Before we describe various biometric cryptosystems, we review the definitions of the primitives required in these systems.

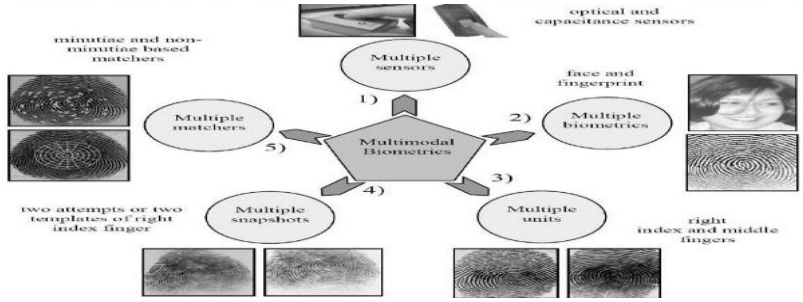


Figure 5: Scenarios in a multimodal biometric system

PROPOSED METHOD

A Stronger Security Model of BIO-IBE

Before presenting the security reduction of BIO-IBE, we describe a stronger model of security for fuzzy IBE (IND-sFSID-CPA) using a game between a challenger and an adversary as follows. The main difference of our new security model is that the adversary is allowed to make private key extraction queries on the challenge identity w^*, where A can obtain $d - 1$ private key components of w^* that A chooses. This new model basically simulates the leakage of partial secret key components of the challenge identity. This property is not considered in the current security model of fuzzy IBE, which return to the adversary only the private key components belonging to any identity other than (i.e. not similar to) the challenge identity.

Phase 1: The adversary declares the challenge identity $w^* = (\mu^*_1, ..., \mu^*_n)$.

Phase 2: The challenger runs the Setup algorithm and returns to the adversary the system parameters.

Phase 3: The adversary issues private key queries for any identity w' such that $|w^* \cap w'| < d$ and the challenger returns the private key components of w'. For the challenge identity w^*, A is given the $d - 1$ private key components of w^* that A selects except for the component $\mu^* \in$

Phase 4: The adversary A sends two equal length messages m_0 and m_1. The challenger picks $\beta \leftarrow \{0, 1\}$ and returns encryption of the message m_β using the challenge identity w^*.

Phase 5: Phase 3 is repeated. A is not allowed to issue private key queries for the remaining $n - d + 1$ attributes of w^*.

Phase 6: A outputs a guess β' for β.

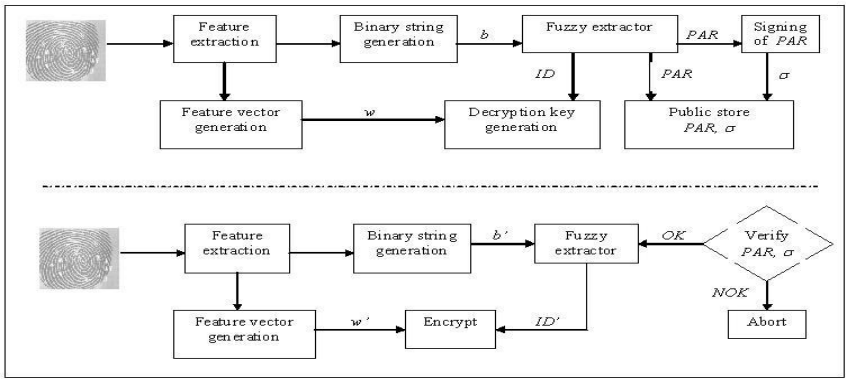


Figure 6: Modified BIO-IBE Flow diagram for single-biometric trait

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 14
November 2017

Here, we summarize the algorithms of our new scheme, which is obtained by modifying the Key Generation and Encrypt algorithms of BIO-IBE. To avoid the key escrow problem, the technique explained above can also be applied.

Setup: The parameters of the scheme are generated as in BIO-IBE. Two additional hash functions $H_3 : \{0, 1\}^* \rightarrow Z^*_p$, $H_4 : \{0, 1\}^* \times F \rightarrow Z^*_p$ are required for the signature scheme as described before.

Extract: First, a user's biometric attributes w are obtained from the raw biometric information using a reader and the feature extractor and each attribute $\mu_i \in w$ is associated to a unique integer in Z^*_p as before. Besides, the identity string ID= H(b) is calculated from the biometric template b using a fuzzy extractor, which also outputs the public value PAR that is used in the reconstruction of the ID by the sender (or encryptor). Next, PAR is signed by the PKG or the receiver of the ciphertext.

Given a user's biometric attributes w and ID, the PKG returns $D_{\mu}^{ID}{}_i = g^{y/(x+H1(\mu_i,ID))} = g^{y/(x+h_i)}$ for each $\mu_i \in w$. Finally, the PAR and the signature σ are stored in a public file.

Encrypt: The sender obtains a biometric reading of the receiver together with the signed public parameter PAR, verifies the signature on the PAR, extracts the feature vector w' and computes $ID' = Rep(b', PAR)$. Here, if $dis((b, b') < t$, then $ID = ID'$. The encryption of $m \in M$ using ID' and w' is identical to BIO-IBE.

Decrypt: The same algorithm as in BIO-IBE.

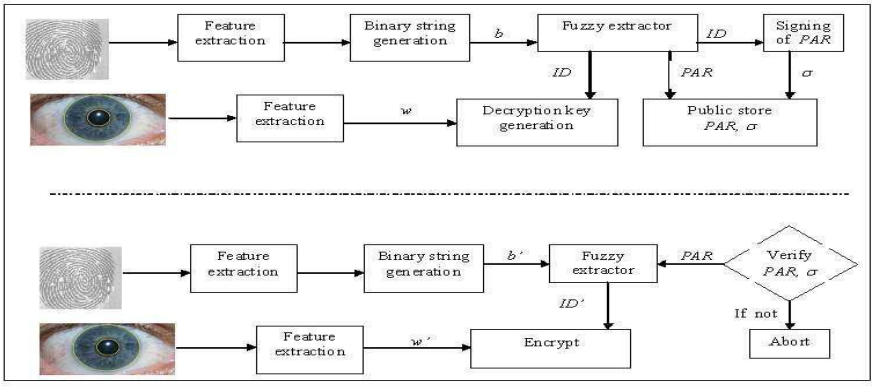
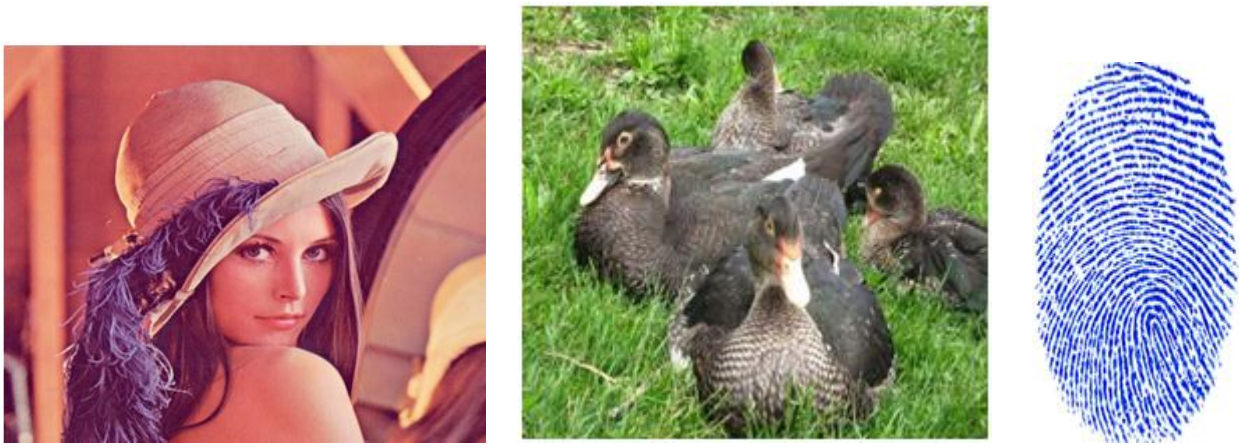


Figure 7: Modified BIO-IBE Flow diagram for two biometric traits

SIMULATION RESULTS

INPUT IMAGES



Input image **hiding image** **key**

Fig 8: Encryption Images

ENCRYPTION RESULTS

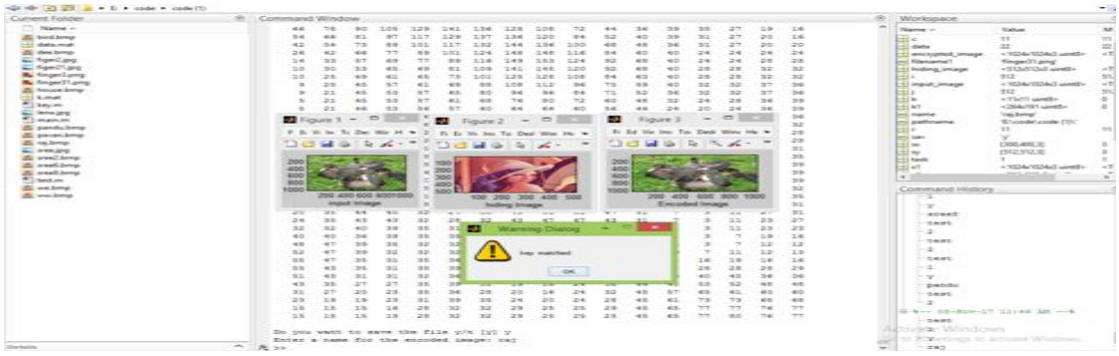


Fig 9.Encryption image when key matched

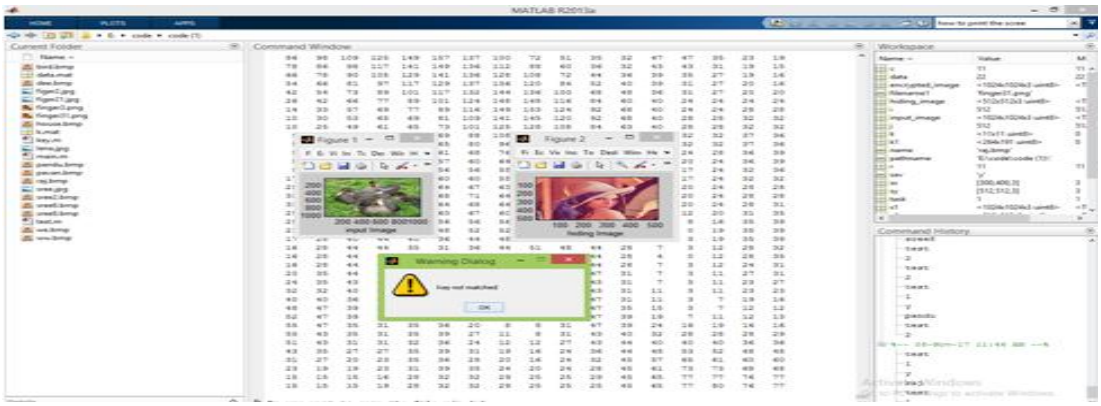


Fig 10: Encryption when key not matched

DECRYPTION RESULTS

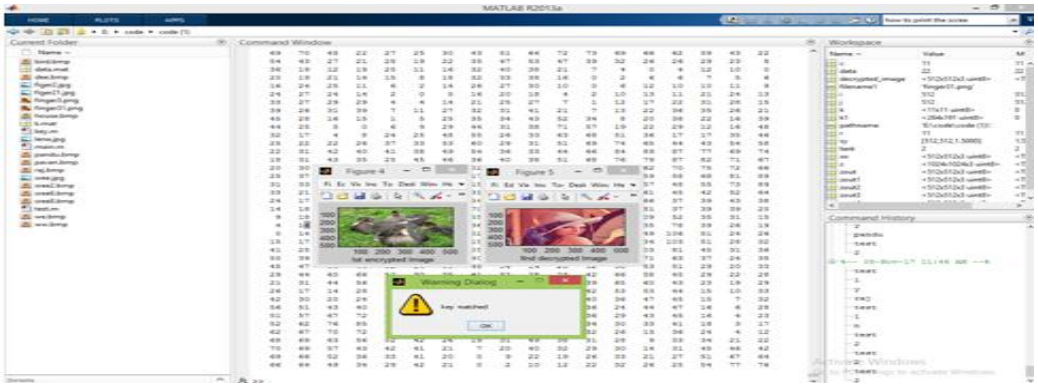


Fig 11;Decryption when key matched

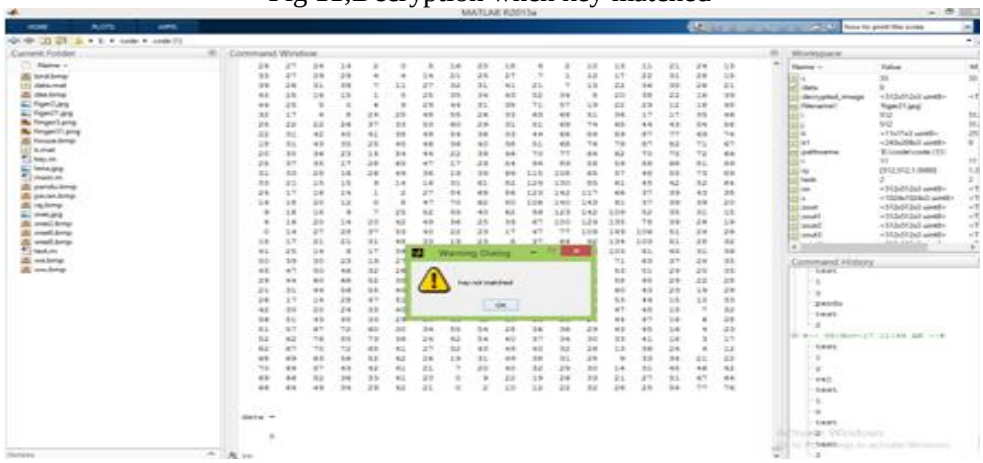


Fig 12 Decryption when key not matched

CONCLUSION

In this chapter, we propose efficient biometric IBE schemes that are provably secure in the ROM and standard model depending on the size of the universe of attributes and the representation of the attributes of the user. We start with an efficient fuzzy IBE scheme denoted as OrdFIBE that is restricted to ordered biometrics or attributes that can be grouped/ordered. Thus, OrdFIBE can be generalized to attribute-based encryption. Next, we describe BIO-IBE that is applicable to any type of biometric modality if combined with a fuzzy extractor to avoid collision attacks. For the two universe sizes, BIO-IBE is currently the most efficient biometric IBE scheme with a tight reduction cost among the other pairing based fuzzy IBE schemes applied for biometric identities. Besides, BIO-IBE is the first biometric IBE scheme that is applicable for multi-modal biometrics as opposed to the claim in [Zhang et al., 2011], which combines fuzzy extractors with multi-biometric encryption. Key escrow problem inherent in all IBE (and thus fuzzy IBE) systems can also be solved with a simple modification on BIO-IBE.

Author's Profiles

P.SridharBabu Pursing M.tech degree in the stream of communication systems from Sir C. R. Reddy college of Engineering, Eluru, Andhra Pradesh,, and B.Tech in Electronics & communication engineering from SRI VASAVI ENGINEERING, Tadepalligudem,Andhra Pradesh.

CH. Madhava Rao completed M.Tech(Opto Electronics) from **Shri Govindram Seksaria Institute of Technology and Science- Indore M.P.**in the year 2001. He is working as Assistant Professor, ECE Dept., SIR C R REDDY COLLEGE OF ENGINEERING-ELURU, A.P. He published papers in national and international journals. Research area of interestis image processing , optical fiber networking.

REFERENCE

[1] F. Guo, W. Susilo, and Y. Mu, "POSTER: Euclidean distance based encryption: How to embed fuzziness in biometric based encryption," in *Proc. ACM Conf. Comput. Commun. Secur.*, 2014, pp. 1430–1432.

[2] T. Kanade, "Picture processing system by computer complex and recognition of human faces," Ph.D. dissertation, Dept. Inf. Sci., Kyoto Univ., Kyoto, Japan, 1973.

[3] R. Brunelli and T. Poggio, "Face recognition: Features versus templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 15, no. 10, pp. 1042–1052, Oct. 1993.

[4] A. K. Jain, S. Prabhakar, L. Hong, and S. Pankanti, "Filterbankbased fingerprint matching," *IEEE Trans. Image Process.*, vol. 9, no. 5, pp. 846–859, May 2000.

[5] H. Moon and P. J. Phillips, "Computational and performance aspects of PCA-based face-recognition algorithms," *Perception*, vol. 30, no. 3, pp. 303–322, 2001.

[6] B. A. Draper, K. Baek, M. S. Bartlett, and J. R. Beveridge, "Recognizing faces with PCA and ICA," *Comput. Vis. Image Understand.*, vol. 91, nos. 1–2, pp. 115–137, Jul./Aug. 2003.

[7] V. Perlibakas, "Distance measures for PCA-based face recognition," *Pattern Recognit. Lett.*, vol. 25, no. 6, pp. 711–724, Apr. 2004.

[8] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology—EUROCRYPT* (Lecture Notes in Computer Science), vol. 3494, R. Cramer, Ed. Heidelberg, Germany: Springer-Verlag, 2005, pp. 457–473.

[9] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology—CRYPTO* (Lecture Notes in Computer Science), vol. 196, G. R. Blakley and D. Chaum, Eds. Heidelberg,
Germany: Springer-Verlag, 1984, pp. 47–53.

[10] D. Boneh and M. K. Franklin, "Identity-based encryption from the Weil pairing," in *Advances in Cryptology—CRYPTO* (Lecture Notes in Computer Science), vol. 2139, J. Kilian, Ed. Heidelberg, Germany: Springer-Verlag, 2001, pp. 213–229.