International Journal of Computing Algorithm
Volume: 04 Issue: 01 June 2015 Pages:19-21
ISSN: 2278-2397

Multi-Biometric Authentication through Hybrid Cryptographic System

M.Gobi,[1]R.Sridevi[2]
[1]Assistant Professor in Computer Science, Chikkanna Government Arts College, Tiruppur, India
[2]Research Scholar in Computer Science, Government Arts College, Udumalpet, India
Email: mgobimail@yahoo.com, srinashok@gmail.com

Abstract – In most of the real time scenario, authentication is required very much so as to enable the person to access a private database of any type. Researchers have started using biometric traits for the authenticity of a person. The various biometrics traits available are face, iris, palm print, hand geometry, fingerprint, ear etc., But the application that uses a single biometric trait often have to challenge with noisy data, restricted degrees of autonomy, non-universality of the biometric trait and intolerable error rates. Multi biometric systems seem to lighten these drawbacks by providing multiple verification of the same personality. Biometric fusion is the use of multiple biometric inputs or methods of processing to improve performance. In this paper, a novel combination of Multi biometric fusion, Symmetric Cryptography and Asymmetric Cryptography is proposed. A fused biometric image is encrypted using Advanced Encryption Standard whose secret key is in turn encrypted using elliptic curve cryptography which is considered as one of the efficient Asymmetric cryptographic algorithms. As the symmetric cryptographic algorithms involve in key exchange mechanism, the secret key is proposed to be secured by using ECC. Hence, the system proposed is expected to be more secured to store the biometric traits of an individual.

Keywords—Biometric Images; Image Fusion; Elliptic Curve Cryptography; Security; Privacy.

I. INTRODUCTION

Private data in real time applications which involve financial transactions and highly regulated to information zone are portrayed to be very confidential to make it available to the authenticated person. This data tend to be kept very secret so as to measure the identity of an individual. So many methods were proposed to keep this information confidential. Private databases were proposed which can be accessed using ID numbers or password that amounts to knowledge based security. Sometimes the intruders or hackers may well infringe the flap of security. Many cryptographic algorithms are available to protect the private data of an individual. Both symmetric and asymmetric algorithms ensure the confidentiality and privacy of data in different ways. Symmetric algorithms are proved to be better for large data when asymmetric stands for smaller one. Even though one algorithm outperforms the other algorithm, it is always necessary to identify the right algorithm for the right application. Elliptic curve cryptography is one such public key cryptographic algorithm based on the elliptic curves and uses the location of base points on an elliptic curve to secure information. ECC make use of a relatively short encryption key to decode an encrypted message because the short key is comparatively faster and involves less computing power than other asymmetric cryptographic algorithms. Biometric systems were also proposed to provide knowledge based security enhancement over the years of research scenario. Biometric technologies are the automated methods of classifying or authenticating the identity of a person based on a biological or social characteristic. There are various biometric traits like face, fingerprint, iris, palm print, hand geometry and ear etc., in which some of them can be, used for security systems[1-3]. Uni-model biometric systems support one biometric trait taken for recognizing or identifying an individual wherein multimodal biometric systems enable the fusion of two or more biometric images with various levels of integration. In this paper, a multimodal biometric fusion [4] [5] which hides a person's fingerprint under the face image is considered. Though these two biometric traits perform better individually, they fail under certain conditions when used as a uni-modal trait. The problem arises at the time of acquisition of fingerprint images with low quality. Poor quality face image may also create problem of identifying a right person. Therefore these two traits are fused together to make a person's identity better than before. The fused image is encrypted to increase the privacy of the data stored in the private database.

II. METHODOLOGIES

A. Biometric Image Fusion

Biometrics is programmed methods of identifying a person based on a physiological or behavioral characteristic. Biometric features normally stated are face, fingerprints, hand geometry, iris, retina, vein, and voice. Since Biometric data are distinct from personal information, these cannot be reverse-engineered to refabricate personal information. They cannot be whipped and used to access the personal information. Although biometric technology has been popular for many years, modern developments in this incipient technology, attached with other security algorithms, now make biometrics efficiently used for security reasons [6]. Image fusion is a technique that can be done in many ways. A simple method of image fusion is followed in this work, where the two images are taken as such they both have same pixel dimensions. Then the fusion of these images is done as follows:

Step 1: Read two input images, fingerprint and face images in a buffered image array.
Step 2: Load the images onto the input array.
Step 3: Measure the width and height of each image to check for the same dimensions.
Step 4: Draw each of the input images onto the output image.
Step 5: Create the output image file and write the output image to it.
Step 6: Display the output image.

B. Advanced Encryption Standard Algorithm

AES is a block cipher with a block length of 128 bits. AES allows for three different key lengths: 128, 192, or 256 bits.

Encryption consists of 10 rounds of processing for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. Except for the last round in each case, all other rounds are identical. Each round of processing includes one single-byte based substitution step, a row-wise permutation step, a column-wise mixing step, and the addition of the round key. The order in which these four steps are executed is different for encryption and decryption. Although, overall, the same steps are used in encryption and decryption, the order in which the steps are carried out is different, as mentioned previously[7]. The overall structure of AES encryption/decryption is shown in Fig 1.

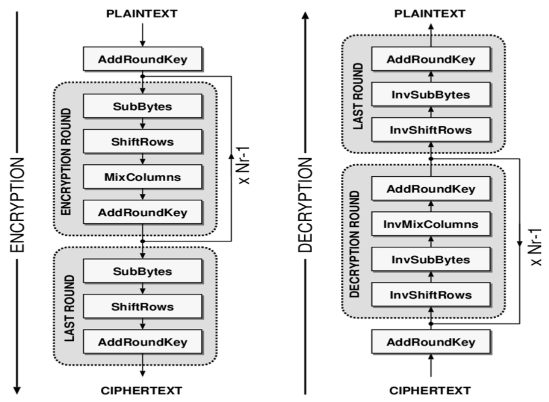

Fig 1. AES Encryption and Decryption

C. Elliptic Curve Cryptography Algorithm

1) Key Generation:

Key generation is an important part where we have to generate both public key and private key. Here, Elliptic curve cryptography algorithm is used to generate both of these keys. The encryption of the fused image is done using a public key and the same will be decrypted using the corresponding private key. For this key pair generation, select a number d, within the range of 'n', which is the random number representing the maximum limit. Using the following equation, the public key, Q can be generated.

$$Q = d * P \quad (1)$$

d = the random number that we have selected within the range of (1 to n-1).

P is the point on the curve.

Q is the public key

D is the private key.

2) Encryption & Decryption:

The Elliptic Curve Integrated Encryption Scheme is as follows [12].To encrypt the AES Secret Key,

Step 1: Select a random integer r in [1, n– 1]

Step 2: Compute R = rG

Step 3: Compute $K = hrQ_B = (K_x, K_y)$, checks that $K \neq 0$

Step 4: Compute keys $k1||k2 = KDF(K_x)$

Where KDF is a key derivation function.

Step 5: Compute $c = ENC_{k1}(m)$

Where m is the text file of fused image

Step 6: Compute $t = MAC_{k2}(c)$

Where MAC is message authentication code

Step 7: Store (R, c, t) in the database for decryption.

To decrypt AES Secret Key,

Step 1: Perform a partial key validation on R

(Check if $R \neq 0$, check if the coordinates of R are properly represented elements in F_q and Check if R lies on the elliptic curve defined by a and b)

Step 2: Compute $K_B = h.d_B.R = (K_x, K_y)$,

Check $K \neq 0$

Step 3: Compute $k_1, k_2 = KDF (K_x)$

Step 4: Verify that $t = MAC_{k2}(c)$

Step 5: Compute $m = ENC_{K1}$-1(c)

K = KB, since K = h.r.QB = h.r.dB.G
= h.dB.r.G = h.dB.R = KB

III. Proposed System

A system is proposed to enhance the privacy, confidentiality and integrity of an individual with the biometric traits to access the private data stored in the database. It also verifies the authentication by checking biometric traits with the previously stored biometrics in the database. The system of Image Processing and Cryptography join hands together to intensify the secrecy of private data which is to be kept confidential [8]. This includes

A. Multi biometric Image Fusion
B. Fused Image Encryption using AES
C. Encryption of AES Key using ECC
D. Decryption of AES Key
E. Decryption of Fused Image.

The biometric images after encryption along with the encrypted AES key are sent to the receiver. At the receiver end, the encrypted key is first decrypted to get the secret key. Then this secret key is used to decrypt the biometric images. To access the confidential information like bank account details, patient history or health insurance details, biometric images are to be scanned for authentication. They are compared with the images already stored. This allows no other than the authenticated person to access the private and confidential details [9] [10]. The system is explained in Fig 2.

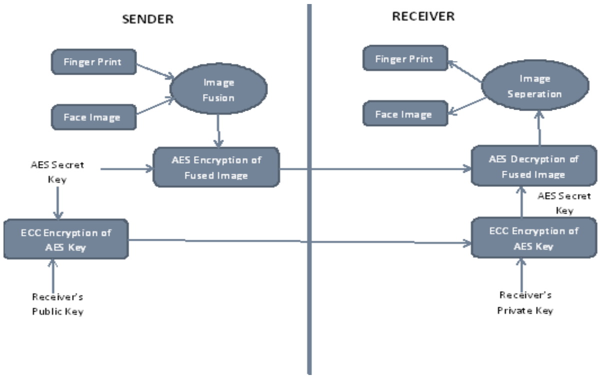

Fig 2.Proposed System of Hybrid Cryptography

A. Multi Biometric Image Fusion

Biometrics proposes the ability to rapidly capture real-time data and provide authentication. The significant purposes for biometric fusion are to improve system precision, competency, applicability, and robustness. Some types of fusion have been used successfully for years in large scale applications. Any two biometric images like fingerprint image, iris, face or palm print images can be taken for consideration [11] [12]. Both of the images are taken in .png format and preferably in equal size. An image fusion program is implemented to create a new layered image out of these two biometric images. The output image will have two layers one lying on the background and the other as foreground.

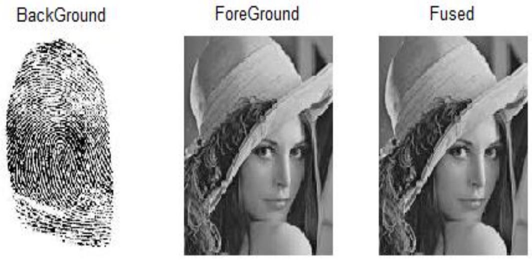

Figure 3. Image Fusion of Fingerprint under Face Image

B. Fused Image Encryption using AES

The biometric images after fusion undergo encryption phase in which Advanced Encryption Standard is used. AES is considered to be one of the efficient and secure secret key cryptographic algorithms for encrypting larger data comparatively with other cryptographic algorithms. It is widely used for encryption and authentic applications. In a scenario of encryption, the following steps are carried out to encrypt a 128-bit block:

1. Derive the set of round keys from the cipher key.
2. Initialize the state array with the block data (plaintext).
3. Add the initial round key to the starting state array.
4. Perform nine rounds of state manipulation.
5. Perform the tenth and final round of state manipulation.
6. Copy the final state array out as the encrypted data (cipher text).

This ensures the confidentiality of private data over the network transmission of data. In authentication applications, the sender encrypts the data using the secret key, which is to be decrypted at the receiver end.

C. Encryption of AES Key using ECC

Since the AES Key is required to be sent to the receiver to decrypt the fused image, and this key exchange mechanism should ensure at most security. To attain this security, Elliptic Curve Cryptography is used to encrypt the AES secret key. Public key cryptographic techniques are proved for high security environment using smaller key sizes[13]. Though, various public key algorithms are outperforming each other, Elliptic Curve Cryptography is even more better than other public key cryptographic system. Hence, the proposed system eventually uses ECC for encrypting AES Secret Key. ECC uses the receiver's public key for encryption, which is made available in the public key ring. The encrypted AES Key along with the encrypted image is sent to the receiver through unprotected public media.

D. Decryption of AES Key

The receiver after receiving the encrypted key and the encrypted image initially decrypts the secret key using ECC private key. The AES Key is obtained through this and this key is in return used to decrypt the fused image.

E. Decryption of Fused Image

Decryption of the fused image is decrypted using AES decryption for which Secret key derived from the previous step is used. The output is the fused image in which the fingerprint is hidden behind the face image. This makes the system more reliable, robust and authentic.

IV. CONCLUSION

In this paper, a system proposing a new hybrid cryptographic system is proposed. Since, both symmetric and asymmetric have their own advantages and drawbacks, this system proposed made use of both the type of cryptographic algorithms taking the advantages of each type. As implied AES algorithm ensures the secrecy of the delicate images. And ECC is used to securely exchange the AES key to the receiver. As combined together, hybrid cryptography is expected to achieve more security, robust and confidentiality. The system proposed is limited to the following constraints. These limitations can be overcome in future by identifying new technologies and innovative modifications. Biometric images should be scanned and stored as .png images so as to support the image fusion code which is written; the two biometric images, fingerprint and face images should be taken in equal dimensions, in pixels for the images to be fused. The unequal dimension images cannot be fused.

REFERENCES

[1] KarthikNandakumar,Yi Chen, SaratC.Dass, and Anil K.Jain, "Likelihood ratio- based biometric score fusion", IEEE T PATTERN ANAL, vol.30, pp.342-347, February 2008.

[2] Unsang Park, Raghavender Reddy Jillele, Arun Ross, and Anil K .Jain,"Periocular biometrics in the visible spectrum", IEEE T INF FOREN SEC, vol 6,no.1, pp 96-106, March 2011.

[3] [3] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems", IBM SYST J, vol 40, pp 614-634, 2001.

[4] Dong Han, ZhenhuaGuo, and David Zhang, "Multispectral palmprint recognition using wavelet-based image fusion,In International Conference on Software Process, 10-11 May 2008, Leipzig, Germany,pp 2074 – 2077.

[5] KarthikNandakumar, "Multibiometric systems: fusion strategies and template security," Ph.D.dissertation, Michigan State University, Dept.of Computer Science and Engineering, 2008.

[6] Kamlesh Gupta and Sanjay Silakari, "Performance analysis for image encryption using ECC", in International Conference on Computational Intelligence and Communication Networks, pp. 79-82, 2010.

[7] Zeghid, Medien, et al. "A modified AES based algorithm for image encryption", International Journal of Computer Science and Engineering, vol 1, 2007, pp 70-75.

[8] ShahriarMohammadi and SanazAbedi, "ECC based biometric signature: a new approach in electronic banking security", in International Symposium on Electronic Commerce and Security, 2008.

[9] Shanthini. B and S. Swamynathan, "Multimodal biometric-based secured authentication system using steganography", Journal of Computer Science, pp. 1012-1021, 2012.

[10] Mahalakshmi. U and Shankar Sriram V.S, "An ECC based multibiometric system for enhancing security", Indian Journal of Science and Technology, vol 6, April 2013.

[11] Norman and Josef Kittler, "A unified framework for biometric expert fusion incorporating quality measures", IEEE T PATTERN ANAL, pp 3-18, January 2012.

[12] Ajay Kumar and SumitShekhar, "Personal identification using multibiometrics rank-level fusion", IEEE T SYST MAN CY C, vol 41, pp.743-752, 2010.

[13] K.Brindha, G.Ramya and RajpalAmitJayantila, " Secured data transfer in wireless networks using hybrid cryptography", International Journal of Advanced Research in Computer Science and Software Engineering, Vol 3, October 2013.