ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

A Secure Multimodal Biometric Approach for Face and Iris using Extended Affine Cipher

G.Juchithaa[1], Dr. V. Palanisamy[2]

[1]Research Scholar, [2]Professor
Department of Computer Science and Engineering, Alagappa University,
Karaikudi-600 003, Tamilnadu, India.
[1]juchithaa1225@gmail.com,[2]mvpazhanisamy@yahoo.com

Abstract— **Multimodal are generally much more imperative to fraudulent technologies, because it is harder to fake multiple biometric characteristics than to forge a single biometric characteristic thus provide higher accuracy rate and higher protection from spoofing. The proposed multimodal biometric approach is divided into two parts. In first part, extending a classical affine cipher algorithm and in second part, with help of that algorithm each trait is encrypted separately. In proposed method, read two biometric traits face and iris image from the same person from their database and then convert these images into 8 x 8 blocks of pixels. These blocks are encrypted by proposed extended affine cipher (EAC). In this extended affine cipher method, 0 to 255 ASCII values are generated which is an extension of basic affine cipher method (26 characters). This method is used to enhancing the security of the multimodal biometric system mathematically with key values. The experimental results ensure that it is promising for higher accuracy and also enhancing the security of existing unimodal biometric systems.**

Keywords— **Multimodal, Biometrics, Face, Iris, Extended affine cipher (EAC).**

I. Introduction

With new advances in digital technologies, security and access control are essential requirements. Biometrics is a best way to secure data when compared to traditional methods such as password, PIN, etc. The term biometrics has been originated from the prehistoric Greek terms: bios means life and metros means measure. Biometrics is used to identify individual person uniquely using their physical, chemical or behavioral traits [1]. The use of unimodal biometrics traits susceptible to noise, bad capture, and other inherent problems make unsuited for all applications. Multimodal systems [2], remove some of the drawbacks of the uni-biometric systems by grouping the multiple sources of information. These systems utilize more than one physiological or behavioral characteristic for enrollment and identification/verification.

When choose multi modal biometric system, some factors are need to considered .They are, Application nature, method adopt, number of traits used, cost, etc.[3]. The goal of multimodal biometrics is to reduce False accept rate, False reject rate, Failure to enroll rate, Susceptibility to artifacts or mimics. This system may be classified as four that is architecture, Sources that provide multiple evidence, Level of fusion, Methodology used for integrating the multiple verifiers. Only Biometric system is not sufficient to provide security but also if it is combined with cryptography, provide good security [4]. Cryptography plays a significant role in this digital advancement. To secure data which is transmitting between sender and receiver, so many cryptographic algorithms are available. A simple method is substitution method. In this substitution method, affine cipher is a simple mono alphabetic substitution cipher and idea behind this cipher is to use multiplication combined with addition, modulo m, where m is an integer, to create a more mixed up substitution [5]. The rest of the paper is organized as follows: Some related works are discussed in section 2. Basic affine cipher is defined with examples and proposed algorithm is implemented, illustrating examples in section 3. The strength of the proposed work is evaluated by experiments done on test biometric traits and results obtained in section 4. Conclusion is given in section 5.

II. Related Work

K. Nivethaet *al.* [6] have been proposed method for enhancing security of Multimodal biometric using HIEA which terms Hyper Image Encryption Algorithm. In this method, finger print, and retinaand finger vein is read and extracting that traits feature by using feature level fusion and done encryption on biometric template using HIEA. After that, transformed template only stored in database and also increase level of GAR and reduces FAR which is comparing to unimodel biometric approach using HIEA.

Suzwani Ismail *et al.* [7] have been proposed a new hybrid method which is based on Cancelable and Fuzzy Commitment

Scheme for securing the multi biometric templates. In this method, Right and left irises of a single individual will be used as input templates. The experiment will be carried out using CASIA-v3 iris database to verify the soundness of the proposed system.

SrujanSatyavarapu*et al.* [8] have been introduced novel method for secure the templates. In this method, fingerprint and iris are captured from different sensors and then, from the fingerprint, biometric data is generated and this data is encrypted using the data extract from iris. Here, iris data is used as a key to encrypt data of fingerprint. The experimental results show that is better when compared to individual fingerprint and iris. When separately use fingerprint, iris then recognition rate is92% and 94.4% . When this method used, then recognition rate is 96.42%.

B.KiranBala*et al.* [9] have been proposed Multi Modal Biometrics using Cryptographic algorithm. In this method, palm vein and iris images are input from user and extract the feature from both traits. Then Cryptographic algorithms are applied to that extracted features to obtained cipher text and it is stored in a database. Here blowfish is used for encrypting both palm vein and iris image. The results ensure that it give higher level security of the Multi model biometrics.

Kande Archana *et al.* [10] have proposed method for Enhance the Security in the ATM System with Multimodal Biometrics and Two-Tier Security. In this method, cryptography technique is used to encrypt the template. Biometric cryptosystem scheme namely fuzzy vault and fuzzy commitment is used to protect the template which is extracted from the biometrics. The results demonstrate that give high security than other methods and it can be deployed in other applications.

III. Proposed Method

A. *Affine cipher*

Affine cipher is a mono alphabetic substitution cipher in which substitute one symbol with another and these symbols may be a number, alphabets. Affine cipher is the combination of additive and multiplicative ciphers with two keys. First key is used for multiplicative cipher and second key for additive cipher. Key for affine cipher is $(k_1, k_2) = (Z_{26}^*, Z_{26})$and '*k1*' should be chosen to be relatively prime to m, where m is *26* characters.

Encrypting plain text is done using *C= (P* x k1+k2) mod 26 and decrypting cipher text is done usingP= *((C-* k2) x $k1^{-1}$) mod 26, where $k1^{-1}$ is the multiplicative inverse of *k1* in the group of integers modulo m. If addition operation is performed at last step in encryption side, then subtraction operation is performed at first step in decryption side [11].

Example

Encryption: - Plain text is "**CARRIER**", k_1= 3, k_2 = 4

Plain text	C	A	R	R	I	E	R
P	2	0	17	17	8	4	17
3 x P+4	10	4	55	55	28	16	55
(3 x P+4) MOD 26	10	4	3	3	2	16	3
Cipher text	K	E	D	D	C	Q	D

Decryption: -Cipher text= "**KEDDCQD**", k_1-1=9, k_2= 4

Cipher text	K	E	D	D	C	Q	D
C	10	4	3	3	2	16	3
(C- 4)x 9	54	0	-9	-9	-18	108	-9
(C- 4) * 9MOD 26	2	0	17	17	8	4	17
Plain text	C	A	R	R	I	E	R

B. *Extended Affine Cipher (EAC)*

In this proposed extended affine cipher method, 0 to 255 numbers are generated to throughout the processing instead of 26 which are in existing scheme. Key for extended affine cipher is (k1, k2) = (Z256*, Z256) and '*k1*' should be chosen to be relatively prime to m, where m is 256 numbers. Here, encryption is performed by using formulae E_i=(K1 × IP + K2) mod 256 and decryption is performed by using formulae Ip = *K1*-1 × (Ei - K2) mod 256. The architecture of proposed work is shown as in Figure1 and flowchart of proposed algorithm is depicted in Figure 2. Algorithm of proposed method is follows.

Method Illustrations

Encryption

Consider Input image blocks matrix

$$I_p = \begin{bmatrix} 150 & 200 \\ 130 & 140 \end{bmatrix}$$

Multiplicative Key (K1),

$$K_1 = \begin{bmatrix} 19 & 21 \\ 23 & 11 \end{bmatrix}$$

Additive Key (K2),

$$K_2 = \begin{bmatrix} 110 & 100 \\ 80 & 60 \end{bmatrix}$$

Encrypt the image traits ($E_{i)}$, use the formulae

$E_{i=}$ (K_1 ×I_P + K_2) mod 256

$$E_i = \begin{bmatrix} 19 & 21 \\ 23 & 11 \end{bmatrix} \times \begin{bmatrix} 150 & 200 \\ 130 & 140 \end{bmatrix} + \begin{bmatrix} 110 & 100 \\ 80 & 60 \end{bmatrix} \text{ mod } 256$$

$$E_i = \begin{bmatrix} 2960 & 4300 \\ 3070 & 1600 \end{bmatrix} \text{ mod } 256$$

Now, original image is encrypted

$$E_i = \begin{bmatrix}144 & 204\\ 254 & 64\end{bmatrix}$$

$E_i$matrix is considered as an encrypted matrix. Then decryption is similar to encryption but reverse operations are used. It is as follows.

Decryption

Encrypted Matrix $E_i = \begin{bmatrix}144 & 204\\ 254 & 64\end{bmatrix}$

Modulo inverse of K_1 is $K_1^{-1}\begin{bmatrix}19 & 21\\ 23 & 11\end{bmatrix}$is $\begin{bmatrix}27 & 61\\ 167 & 163\end{bmatrix}$,

$$K_2 = \begin{bmatrix}110 & 100\\ 80 & 60\end{bmatrix}$$

Decrypt ($D_{i)}$ the encrypted image traits, use the formulae

$$I_{p=}\ K_1^{-1} \times (E_i - K_2) \bmod 256$$

$$D_i = \begin{bmatrix}27 & 61\\ 167 & 163\end{bmatrix} \times \begin{bmatrix}144 & 204\\ 254 & 64\end{bmatrix} - \begin{bmatrix}110 & 100\\ 80 & 60\end{bmatrix} \bmod 256$$

$$D_i = \begin{bmatrix}918 & 6344\\ 29058 & 652\end{bmatrix} \bmod 256$$

Now, original image is recovered.

$$D_i = \begin{bmatrix}150 & 200\\ 130 & 140\end{bmatrix}$$

Therefore, $E_i = D_i$

C. *Overview of Proposed work*

The goal of this research work is to develop a novel security framework for multimodal biometrics. Here two biometric traits (Face, Iris) are used to develop the multimodal biometrics system. In proposed method, firstly Face and Iris images are taken as input from database and then secondly, both images are converting into 8*8 blocks. Third, apply extended version of affine cipher on this blocks to get resultant image which is encrypted. To decrypt the image, reverse operation of encryption is applied on encrypted image.

Encryption Algorithm

Step1: Two Biometric traits are Face and Iris image taken from their respectivedatabases as an input image.
Step2: Convert input image traits into 8x8 pixel blocks.
Step3: On this blocks, apply proposed extended affine cipher method.
Step 4: Then, image is encrypted which is stored in database.

Decryption Algorithm

Step 1: Apply Inverse operation of extended affine cipher method.
Step 2: Then decrypted the encrypted image.
Step 3: Original biometric traits are recovered.

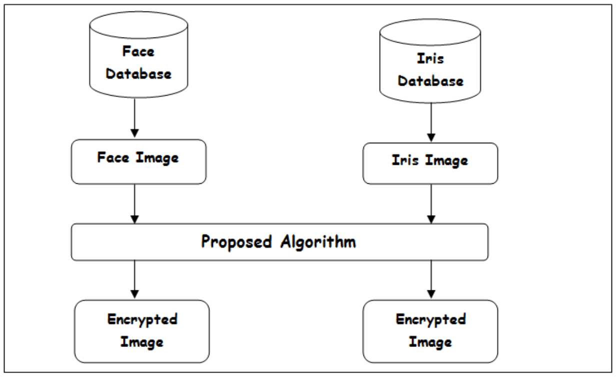

Fig.1Proposed System Architecture

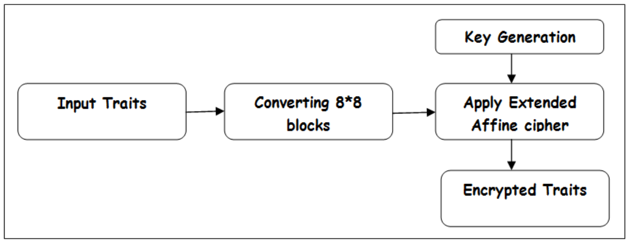

Fig.2 Flow chart of proposed algorithm

IV. Result and Discussions

A. *Experimental Results*

A Multimodal biometric traits are encrypted based on proposed extended affine cipher is carried out with different samples. The original traits and encrypted traits are shown in Fig. 3. It has 256×256 pixels with 256 gray levels.

Fig.3Experimental results of the proposed image Encryption algorithm (a) Original Traits (b) Encrypted Traits (c) Decrypted Traits

B. *Performance Analysis*

1) Information Entropy Analysis:Entropy is the most outstanding feature to measure the randomness. In order to design a good image encryption scheme, the entropy of the encrypted image has to be close to the ideal case.

For gray-scale images of 256 levels, if each level of gray is assumed to be equiprobable, then the entropy of this image will be theoretically equal to 8 Sh (or bits). Ideally, an algorithm for encryption of images should give an encrypted image having equiprobable gray levels.

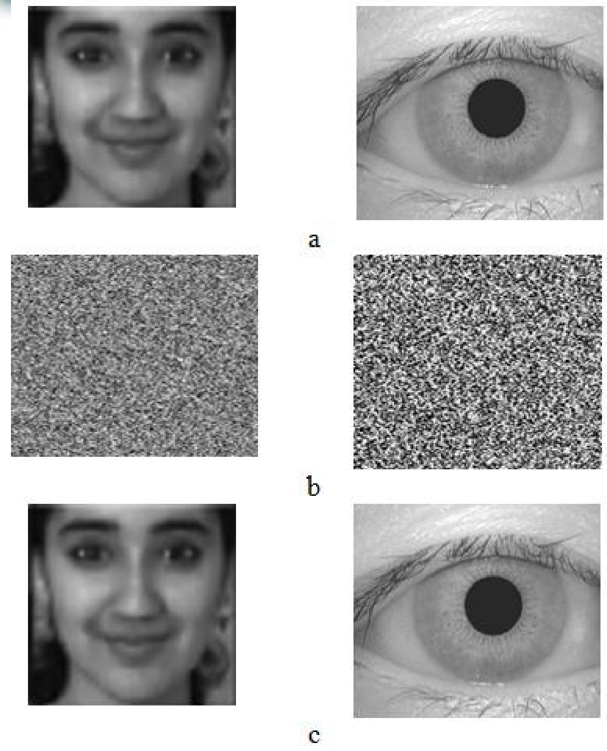

Table 1 gives the entropy values of the several encrypted for both traits. On the other hand, the entropy values of the encrypted traits are very close to the ideal value of 8 Sh, which means that the proposed encryption algorithm is highly robust against entropy attacks.

The values obtained are very close to the theoretical value of 8. The scheme is robust, and its performance against an entropy attack is good.

TABLE I
ENTROPY VALUES OF THE ENCRYPTED TRAITS

Samples	Encrypted Face Trait	Encrypted Iris Trait
1	7.9968	7.9880
2	7.9960	7.9962
3	7.9890	7.9920
4	7.9950	7.9935
5	7.9928	7.9890
6	7.9889	7.9968
7	7.9880	7.9960
8	7.9948	7.9890
9	7.9978	7.9950
10	7.9945	7.9890
11	7.9898	7.9889
12	7.9984	7.9954

V. CONCLUSION

In this Secure Multimodal Biometric Approach for Face and Irises using Extended Affine Cipher is elegantly proposed. Multimodal security system for recognition and authentication purpose using iris and faces biometric traits are encrypted by proposed extended affine cipher with better data protection and less complexity. This method gives more security compared to unimodal encryption because of two biometric features are encrypted to enhances more security. Also the proposed method is very difficult to forge and can be made for secure by combining more than one biometric traits. The performance analysis gives that the proposed image encryption algorithm is highly secure.

REFERENCES

[1] Pocovnicu, Adrian. “Biometric security for cell phones.” InformaticaEconomica 13.1 (2009): 57.

[2] Jain, Anil K., and Arun Ross. “Multibiometric systems.” Communications of the ACM 47.1 (2004): 34-40.

[3] Anwar, Farhat, MdArafatur Rahman, and MdSaiful Azad. “Multibiometric systems based verification technique.” European Journal of Scientific Research 34.2 (2009): 260-270.

[4] Gaikawad, Vaibhavkumar S., and S. N. Kini. “A Survey of Multi-Biometric Cryptographic Security System.”

[5] Thomas, B. H. “An invitation to cryptology.” ISBN-13 (2001): 978-0130889768.

[6] Nivetha, K., and D. Saraswady. “Enhancing security for multimodal biometric using Hyper Image Encryption Algorithm.” Electronics and Communication Systems (ICECS), 2015 2nd International Conference on. IEEE, 2015.

[7] Suzwani Ismail, Fakariah Hani HjMohd Ali, Syed Ahmad Aljunid., A New Hybrid Approach for Securing Multibiometric Templates Based on Cancelable and Fuzzy Commitment Scheme. Aust. J. Basic & Appl. Sci., 9(26): 72-76, 2015.

[8] SrujanSatyavarapu, Farida Khurshid and Shoaib Amin Banday, “Multimodal Biometric Template Access Control Using Fingerprint Data Encrypted By Iris Data”, International Journal of Electrical, Electronics and Data Communication, ISSN: 2320-2084, Volume-2, Issue-10, Oct.-2014.

[9] Bala, B. Kiran, and J. Lourdu Joanna. “Multi Modal Biometrics using Cryptographic Algorithm.” European Journal of Academic Essays 1.1 (2014): 6-10.

[10] Kande Archana, Dr.A .Govardhan, “Enhance the Security in the ATM System with Multimodal Biometrics and Two-Tier Security”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol.3, Issue.10, 2013.

[11] Forouzan, A. Behrouz. Data Communications & Networking (sie). Tata McGraw-Hill Education, 2006.