Iris Template Protection based on Enhanced Hill Cipher

1st Author
Emad Taha Khalaf
Faculty of Computer Systems & Software Engineering
University Malaysia Pahang, 26300, Kuantan, Malaysia
emadump@yahoo.com

2nd Author
Muamer N. Mohammad
Faculty of Computer Systems & Software Engineering
University Malaysia Pahang, 26300, Kuantan, Malaysia
muamer.scis@yahoo.com

3rd Author
Norrozila Sulaiman
Faculty of Computer Systems & Software Engineering
University Malaysia Pahang, 26300, Kuantan, Malaysia
norrozila@ump.edu.my

ABSTRACT
Biometrics has become an area of great research interest. The extracted features from the biometric sample is called biometric template. Template protection is a crucial requirement when designing an authentication system, where the template could be modified or stolen by attacker and attack against the stored templates constitutes a major security and privacy threat in a biometric system. Hill Cipher is a block cipher and symmetric key algorithm it has several advantages such as simplicity, high speed and high throughput can be used to protect Biometric Template. Unfortunately, Hill Cipher has some disadvantages such as takes smaller sizes of blocks, very simple and vulnerable for exhaustive key search attack and known plain text attack, also the key matrix which entered should be invertible. This paper proposed an enhancement to overcome these drawbacks of Hill Cipher by using a large and random key with large data block, beside overcome the Invertible-key Matrix problem. The efficiency of encryption has been checked out by Normalized Correlation Coefficient (NCC), histogram and running time.

CCS Concepts

• *Security and privacy~Cryptography* • *Security and privacy~Block and stream ciphers*

Keywords
Biometric, Cryptography, Hill Cipher, Iris Template, Template Protection.

1. INTRODUCTION
Biometric Template protection has been gaining more attention in recent years and attempts in different directions have proven promising [1]. Unlike passwords, stolen biometric templates cannot be revoked, when biometric templates are compromised, it is not possible for a legitimate user to revoke his biometric identifiers and switch to another set of uncompromised identifiers. Due to this irrevocable nature of biometric data, an attack against the stored templates constitutes a major security and privacy threat in a biometric system. In fact, since a biometric trait is a permanent link between a person and his identity, it can be easily prone to abuse in such a way that a person's right to privacy and anonymity is compromised. [2]. Template protection algorithms also depend on the biometric trait and in our research we chose to focus on iris based biometric systems. Iris based-biometric systems have many advantages over other biometric traits: (i) the iris is protected inside the human body and is, hence, less prone to environmental factors like cuts, sweat, dirt, etc, as in the case of fingerprints, (ii) the iris cannot be surgically manipulated without significant risk to the vision, (iii) the iris' reaction to light offers one of many methods of livelihood test against artifice, (iv) iris-based biometric systems [3] [4] [5], have proven to be highly accurate. In this paper we propose a biometric protection approach based on enhanced Hill Cipher, it has been improved to be more secure.

2. HILL CIPHER ALGORITHM
The Hill Cipher is a block cipher and symmetric key algorithm, it was introduced to the journal of mathematics by Lester Hill as a short paper and published in 1929 (Lester, 1929). Hill Cipher has several advantages such as resistant towards frequency analysis, simplicity because of using basic matrix operations, high speed, high throughput [6],[7],[8]. Unfortunately it has some disadvantages such as takes the smaller sizes of blocks so key length is shorter, very simple and vulnerable for exhaustive key search attack and known plain text attack, also the key matrix which entered should be invertible.
The encryption process of classic Hill cipher algorithm is start with encoding each character of the plaintext as a numerical value (a=0, b=1, …, z=25) then breaking encoded plaintext into blocks (vectors) of size n and multiplied by an $n \times n$ key matrix K, which is the encryption key, final process is perform mod 26. Simply the plaintext block P encrypts C by:

$$C = P\,K \pmod{26} \quad (1)$$

Where: C is Cipher text
P is Plain text
K is encryption Key

Decryption requires the inverse of matrix K. The inverse K^{-1} of a matrix K is defined by the equation:

$$K\,K^{-1} = I \quad (2)$$

Where: I is the Identity of matrix
K^{-1} is the invers of the encryption key

[6],[9],[10] The proposed enhancement is inspired from a number of researches which are related to cryptography biometric techniques.

Not all the matrices have an inverse, only those that have a determinant is not zero and does not have any common factors with the modular base. In decryption the reverse process, deciphering, is computed by:

$$P = K^{-1}C \pmod{26} \quad (3)$$