International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

An Improved Secret Sharing Scheme for Biometric Authentication using Finite Field

N. Rajesh Kumar, R. Bala Krishnan, N.R. Raajan

Abstract— Traditional biometric schemes used master copy minutiaefor authentication. The enrollment and verification process carried out through the same master copy minutiae. However, the protection of biometric template is more crucial as the number of minutiae compromise will be occurred. In this paper, an improved secret sharing scheme for biometric authentication using finite field is proposed. The master copy of biometric template is transformed into finite field for masking minutiae information. The concept of secret sharing is employed to split the template into multiple copies and maintained between smart card and public consortium. This approach allows perfect biometric authentication for operating smart cards with high-level security.

Index Terms — Secret sharing, FiniteField, Stacking, Biometrics, Verification.

I. INTRODUCTION

In the fastest growing ecommerce market, the usage of smartcard technology becomes more popularthat provides cash withdrawals and making point-of-sale (POST) transactions. This technology uses the microcontroller to store human biometrics, carry out various authentication terminologies and interact smartly with the card reader device. Charles Clancy [7] identified and presented a secure smart card processing system based on the finger print authentication in 2003. Shamir proposed a web payment system for making online transactions through one time CCT number through the secure transmission medium. Credit card visual authentication scheme based on finite field [2] application is invented by Feng Wang [1] et al. Combination of mathematical model and image processing techniques have been used to implement their visual authentication scheme. Many investigations are ongoing to authenticate the smart card and identify the forged people while using the smart cards. A secure authentication using watermarking for smart card has proposed by Hafid Mammass [3] in 2013. But high level computation and matching algorithms are needed to implement their system. However, it is difficult to identify the forged people during the transaction time.A novel biometric authentication scheme is needed to solve the smart card issues.

In the past decade, visual cryptography techniques have beeninvestigated rapidly in the field ofimage processing, information hiding and computer security. Digital Image processing is a fully mathematical domain to perform various operations such as image analysis, image protection, object matching, image enhancement and restoration operations. The term “visual” means image and “cryptography” means secret writing which offers high level confidentially over digital images for secret sharing. Conventional visual cryptography architecture had invented by Moni Naor and Adi Shamir [5]in 1994. A secret image is encoded into pair of share images under a built in codebook table. Later, it is reconstructed by stacking the share images. Regrettably, the traditional method failed to reconstruct the high quality of original image. Architecture implementation [6] of Finite field traditionally appeared after the invention of two public-key crypto systems: elliptic curve cryptosystems [4] (ECC) and hyperelliptic cryptosystems (HECC).A foundation of cognitive cryptography with secret sharing techniques has been proposed by Marek R.Ogiela and Lidia Ogiela [8] in 2018. In this method, cognitive cryptography is used to protect the biometric traits of individual features and secret sharing is applied to verify the biometric features. Lidia Ogiela [9] and Urszula Ogiela presented a new method of cognitive computational paradigms that combined three types of cryptographic protocols for data security. The investigators described a new class of threshold scheme for secret sharing and linguistic-biometric schemes. This combined approach improved the security of the share biometric traits.

In this paper, an improved secret sharing scheme for biometric authentication using Galois Field (2^8) with special cryptographic technique is presented.The proposed fingerprint framework uses the combination of finite field and Visual Cryptography techniques to provide the fabulous smart card authentication. The rest of this paperis organized as follows. Section II presents the preliminaries of the famous Galois field theory and Cayley table. The proposed visual secret sharing biometric framework for smart card is depicted in section III.Section IV illustrates the implementation results ofproposed visual authentication scheme. Finally, conclusions are drawn in Section V.

Manuscript published on 30 September 2019
* Correspondence Author
N. Rajesh Kumar*, Assistant Professor, Department of CSE, Srinivasa Ramanujan Centre, SASTRA Deemed to be University, Kumbakonam, Tamilnadu, India.
(Email: rajeshkumar.rb@src.sastra.edu)
R. Bala Krishnan, Assistant Professor, Department of CSE, Srinivasa Ramanujan Centre, SASTRA Deemed to be University, Kumbakonam, Tamilnadu, India.
N.R. Raajan, Senior Assistant Professor, Schoolof Electrical & Electronics Engineering, SASTRA Deemed to be University, Thanjavur, Tamilnadu, India.

II. DESCRIPTION OF GALOIS FIELD THEORY

In general, digital image is a 2-Dimensional matrix of pixels with various gray level intensity values ranging from 0 to 255. Considering the Galois Field theory, GF (2^8) construction is the best structure to deal the operations of digital images. Finite field is invented by the French mathematician Pierre Galois. GF (q) means, a Galois Field can take q different values for operations. Addition and multiplication are the two major operations of Galois Field.

Rule 1: Galois Field is denoted as GF and p and m refers prime number and modulo-p respectively. In order to satisfy the prime size, a finite field with prime number (p) of elements should fulfill the arithmetic modulo-p computation. Suppose if we take two elements in the field range values (0 to p-1), for performing arithmetic operations, we should apply the modulo-p function on the resultant value.

This proposed scheme employs the Galois field GF(2^8)for encrypting biometric traits. To make the easier computation, Galois Field can be used with Polynomial expressionfor the corresponding Field. For example, the reduced polynomial expression of GF (2^8) is given in equation (1).

$$x^8 + x^4 + x^3 + x^2 + 1 \quad (1)$$

A. Matrix representation of Galois Field (2^8)

In this section, we have discussed how the image matrix has represented under Finite field applications. A matrix with size of m × n has taken for explanation.

$$X = \begin{bmatrix} x_{11} & x_{12} & x_{13} & x_{14} \\ x_{21} & x_{22} & x_{23} & x_{24} \\ x_{31} & x_{32} & x_{33} & x_{34} \\ x_{41} & x_{42} & x_{43} & x_{44} \end{bmatrix}$$

The Original matrix

Creation of Galois Field Array(2^8) is represented in equation (2).

$$A = GF\ (2,8) \quad (2)$$

Galois Field Array (2^8) for given original matrix is represented in equation (3).

$$A = GF\ (X,8) \quad (3)$$

We can perform various operations using Galois field computation such as index into array, transpose array, extracting diagonal, lower, upper elements and concatenate matrices.

B. Galois Field operations

The rules are identical for all general matrix. When we start the matrix operations under the finite field area, the rules for matrix operations are followed based on field type and its corresponding primitive polynomial expression.

The following are major operations of Galois Field (2^8).

1) Logarithm in GF (2^8)
2) Exponentialin GF (2^8)

Definition 1: Let $X_{i,j}$ be a two dimensional M × N matrix, and the logarithm of any k[th]element of X denotes, the element k must be assigned into Galois array $X1_{i,j}$. All index values of matrix $X_{i,j}$ should be non-zero.Then, the Galois Array of the matrix elements can solve the equation for finding logarithmic expression,

$$Y = Log(X1_{i,j}) \quad (4)$$

If we take Galois Field $GF(2\wedge m)$, where m=8, the field has 2^8 = 256, distinct elements and values begin from 0, 1, 2. …. 2^{m-1} .

Definition 2: Let $Y_{i,j}$ be a two dimensional M × N matrix in the form of Galois array, and the exponential of any k[th]element of Y denotes, the element k must be assigned into Galois array $X1_{i,j}$. The exponential value of the k[th] element must be same as the input matrix $X_{i,j}$. Then, the Logarithmic value of Galois matrix elements can solve the equation for finding the exponential term to revert back to the original value.

$$p = gf\,(2,m), where\ m = 8, \quad (5)$$

$$X_{i,j} = p.\hat{}(Y_{i,j}) \quad (6)$$

For example, Let $A = \begin{bmatrix} \mathbf{28} & \mathbf{42} \\ \mathbf{77} & \mathbf{92} \end{bmatrix}$ be an input matrix

Create Galois Field Array,

$X = gf\left([A], m\right)$ Where m=8, the corresponding primitive polynomial equation is $x^8 + x^4 + x^3 + x^2 + 1$

Logarithmic Process – Step 1

$$Y = \log\begin{bmatrix} 28 & 42 \\ 77 & 92 \end{bmatrix}$$

$$Y = \begin{bmatrix} 200 & 142 \\ 145 & 131 \end{bmatrix}$$

Exponential Process – Step 2

$$p = gf\,(2\wedge 8);$$

$$X = p.\wedge Y$$

$$X = p.\wedge\begin{bmatrix} 200 & 142 \\ 145 & 131 \end{bmatrix}$$

$$X = \begin{bmatrix} 28 & 42 \\ 77 & 92 \end{bmatrix}$$

$$= A \quad (Input\ matrix)$$

C. Cayley Table

Cayley's theorem states that every group G is isomorphic to a subgroup of the symmetric group acting on G. The Cayley table of G= {0,1,2,3} under addition mod 4 is represented in Table 1. This table describes the structure of finite group as well as code table for proposed visual secret sharing scheme.

Table 1. Cayley Table Z_4

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

III.GALOIS FIELD BASED VISUALAUTHENTICATION SCHEME

This section presentsan improved secret sharing scheme using Cayley table in the elements of Galois Field (2^8) for biometric authentication at point of sale terminals. Fingerprint is a main biometric component to perform the authentication. The proposed framework converts themaster fingerprint copy into the elements of Galois field (GF) (2^8) to perform various arithmetic operations. This scheme mainly focused on element-wise exponentiation and element-wise logarithm for masking biometric information in the form of Finite field elements. The values of masked image are further encoded using a special type of Visual Secret sharing scheme based on Cayley table (Z_4).The design of proposed visual authentication framework is shown in Figure. 1.

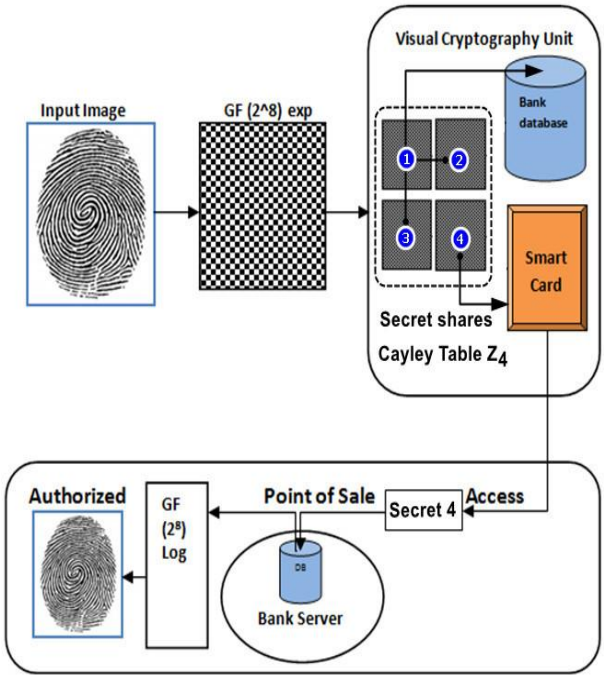

Fig. 1 The proposed Visual Authentication Framework

The proposed biometric authentication scheme has three levels. Two levelshave been implemented from banking sector and one level has completed at the time of point of sale transaction. The banking sector must enroll the biometric information from their customers for initial level computation. The fingerprint is a unique component of biometric system, so that can be used as an input image for smart card authentication system. The bank selects the card holder's fingerprint information to apply the Galois Field exponential function for initial level encryption.

Then Cayley table addition mod 4 based visual cryptography technique has been used for constructing fingerprint visual secret shares for next level encryption. After the successful computation of secret shares, the fingerprint has divided into four parts. Share 1, Share 2 and Share 3 is stored into bank database and share 4 is stored into the customer's smart card chip. This type of encryption technique is called visual cryptography unit.

Now, the smart card has been distributed to the customers for initiating transactions at any point. The smart card contains the copy of fingerprint in the form of secret shares. Whenever they use the smart card for transactions, the card has been verified through the bank database by overlapping all qualified shares which is retrieved from smart card and bank database. After overlapping process, the Galois Field logarithmic function has taken for finding correlation between two images and generates hash code. If the hash code has matched with bank database, the smart card is authenticated perfectly at the place of POS and ensures the identity of the card. The proposed Visual authentication scheme is described in Algorithm 1 and Algorithm 2.

Algorithm 1. Cayley Table based Secret Share Construction on Finite Field

Input: Fingerprint $F = \left(F[x,y]\right)_{x,y=0}^{N-1}$ with Size of $m \times n$

Output : Meaningful shares : S-hare 1 and Share 2

1. Read the size of fingerprint and assign a new matrix A.
2. Define the Cayley table for addition mod 4 (Z_4)
3. Change the ordinary matrix (A) into elements of Galois Field 2^8 (X).
4. P =gf(2^q), where q=8;
5. Perform matrix exponentiation on Galois array of biometric trait.
6. Store the exponential result
7. Apply the structure of Cayley table addition modulo 4 on all the elements of exponential values and construct the shadow images.

Finally, Store three shadow images in bank database and one shadow in smart card separately.

Algorithm 2.Point of Sale Transaction Authentication Scheme

Input: Smart card chip

Output: Smart card authentication

1. Read the smart card at point of sale terminal
2. Extract the fingerprint sharefrom smart card
3. Extract all qualified shares from bank databaseand perform stackingprocess for smart card authentication
4. Compute logarithm on stacked fingerprint

5. Generate Has code
6. If (hashcode = = bank_dbcode)
7. disp “Smart card is original”
8. else
9. disp “Duplicate card is detected”
10. End

IV. EXPERIMENTAL RESULTS

The proposed fingerprint visual authentication scheme using Galois Field theory and Cayley table based Visual cryptography technique has implemented on Intel core i3-3110M CPU @ 2.40GHZ with 4 GB of internal memory space. The following experiments are carried out to compute the efficiency of visual authentication scheme. The implementation results are shown in Figure 2. The execution time for various fingerprint images have been recorded and are represented in Table 2.

Table 2. Processing Time for Smart Card Authentication

Size	GF Exp (s)	Share Generation (s)	Log (s)
30 kb	0.04	28	28
16 kb	0.95	18	18
4 kb	0.31	10	11
62 kb	0.03	58	58

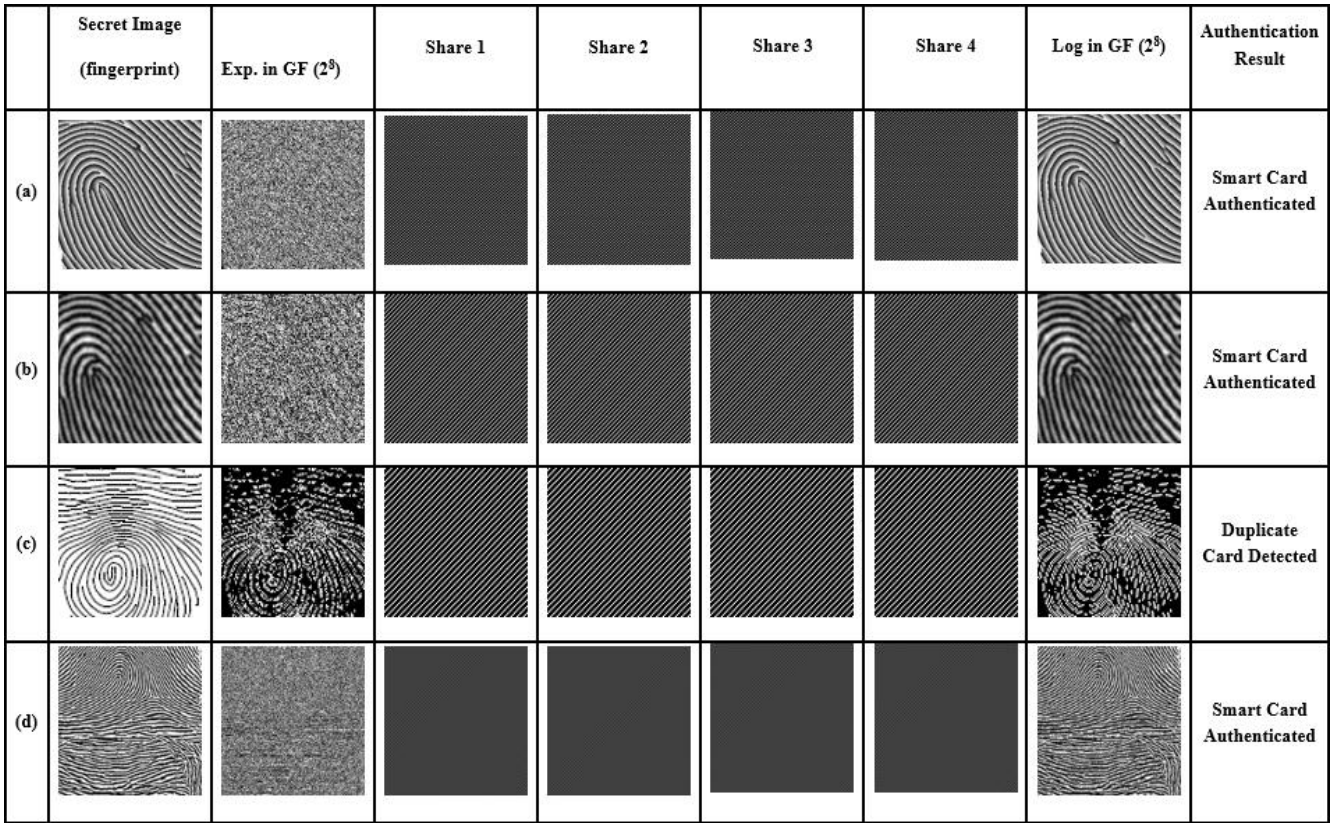

Fig. 2 Implementation visual authentication of result

V. CONCLUSION

In this work, we presented an improved secret sharing scheme using Cayley table in the elements of Galois Field (2^8) for biometric authentication at point of sale terminals. The experimental results show that the proposed visual authentication scheme detected the duplicate smart card effectively in a fast manner. Three level encryption standards ensure the protection of master fingerprint copy and secure online transaction processing at POS terminal.

REFERENCES

1. Feng Wang, Chin-Chen Chang, Wan-Li Lyu, “The credit card visual authentication scheme based on GF (2^8) field,” *Multimedia Tools and Applications*, Vol. 74, No. 24, pp. 11451-11465, Dec.,2015.
2. Irving S. Reed, T. K. Truong, Yik S. Kwoh, Ernest L. Hall, “Image Processing by Transforms Over a Finite Field,” *IEEE Transactions on Computers*, Vol. c-26, No. 9, pp. 874-881, Sep., 1977.
3. Hafid Mammass, Fattehallah Ghadi, Mohammed Elhajji, “Secure Watermarking Method with Smart Card,”*International Journal of Computer and Information Technology*,Vol. 02, No. 05, pp. 874-881, Sep.,2013.
4. Jorge Guajardo, Tim Guneysu, Sandeep S. Kumar, Christof Paar, Jan Pelzl, “Efficient Hardware Implementation of Finite Fields with Applications to Cryptography,”*Acta Applicandae Mathematica*,Vol. 93, No. 1, pp. 75-118, Sep., 2006.
5. Naor M, Shamir A., “Visual Cryptography Advances in Cryptology”, *Eurpocrypt'94, Springer-Verlag, Berlin*, pp.1-12. 1994.
6. Joon-Ho Hwang, “Efficient Hardware Architecture of SEED S-box for Smart Cards,”*Journal of Semiconductor Technology and Science*, Vol. 4, No. 4, Dec., 2004.
7. Charles Clancy T, “Secure Smartcard-Based Fingerprint Authentication,” *WBMA '03*,Berkeley, California, USA. Copyright 2003 ACM 1-58113-779-6/03/00011, Nov., 2003.
8. Marek R. Ogiela, Lidia Ogiela, “Cognitive cryptography techniques for intelligent information management “, International Journal of Information Management, Vol. 40, pp. 21-27, Jan 2018.
9. Lidia Ogiela, Urszula Ogiela, “Cognitive and biologically cryptographic protocols for data security”, Cognitive Systems Research, Vol. 56, pp. 1-6, Feb 2019.