# Securing Retinal Template Using Quasigroups

N. Radha
Research Scholar, Department of Computer Science, Karpagam University, Coimbatore-21, India
Lakshmin07@sify.com

T. Rubya
Research Scholar, P S G R Krishnammal College for Women, Coimbatore-4, India

S.Karthikeyan
Director and HOD, Department of Computer Science, Karpagam University, Coimbatore -21, India

***Abstract*—Biometric plays important role in person recognition and identification. It is more secure than the traditional systems like password and token based systems. The traditional systems can be stolen, misplaced or destroyed. But the biometric systems are based on the physiological or behavioral traits of the individual human being. It cannot be altered or misused by the unauthorized persons. It is more reliable than the traditional systems. Although it is powerful, immutable to vulnerable attacks So it is necessary to secure the biometric template using more efficient techniques. Crytography is the most powerful technique to avoid vulnerable attacks. Recently it was found that The non-associative property of quasigroup helps achieving better security by having a randomly generated key for encr[1]yption. The operations involved in Quasigroup are computationally simple and can be efficiently used for protection of voluminous media like images, audio, video and different forms of multimedia In this paper the Quasigroup technique is used to provide better security to Retina Template.**

***Index Terms*—Retina Biometric, Quasigroup, Encryption, Decryption, Isotopes**

## I. INTRODUCTION

Biometrics refers to automatic systems that use measurable, physiological characteristics or behavioural traits to recognize the identity, or verify/authenticate the claimed identity of an individual. The examples of biometric characteristics that have been used for automated recognition. These systems are based on a biometric sample taken from an individual, for instance, retina from iris scan. This physical characteristic may be presented by an image. Often features are extracted from that sample. These extracted data constitute a biometric template.

Cryptography is the science and art to transform message to make them secure and immune to attacks. Encryption is the method of encoding the data by special algorithm that renders the data in an unreadable form to anyone without decrypting it.

Biometric encryption authentication is a strong, certainly far superior to traditional token and password based systems. An efficient method for person authentication based on the retinal blood vessel pattern that extracted features are used for cryptographic process is presented in this paper. Retina and iris can be used in high security applications like access control, military applications, border security control.

The proposed quasi group is constructed with feature points extracted from retina and iris. The concept of biometric encryption has been used which has many advantages over the conventional methods for biometric security [3][4][5]. Biometric Encryption is a process that securely binds a cryptographic key to a biometric, so that neither the key nor the biometric can be retrieved from the stored template. Thus, Biometric Encryption is an effective, secure, and privacy friendly tool for biometric password management.

Quasi group-based permutations have very good encryption properties and, therefore, it has potential uses in symmetric cryptography. If the purpose of the scrambler is to maximize the entropy at the output, then it can be said that the quasi group based system accomplishes this successfully, even for input data that is constant. The immense complexity associated with the task of finding the scrambling transformation ensures the effectiveness of the encryption process.

To extend the security, the biometrics feature of a user is used as a key for encryption [13] process. In this paper, retina features are used for encryption and decryption. This proposed work has been done with MATLAB tool. The paper is organized as follows: In section II Related works are discussed. Section III includes the methodology adopted for the proposed work is given. In section IV the results obtained using quasi group encryption method is discussed. The next section V contains the performance is analysed using covariance and statistical methods which follows Conclusion.

## II. RELATED WORKS

Rajeswari Mukesh *et al*.,[20] proposed an energy efficient security protocol for WBSN (Wireless Biomedical Sensor Network) where security is provided to the physiological data, which is being transmitted from the sensor node to the sink device. This is achieved by

N.Ratha Research Scholar, Karpagam Unversity, Coimbatore.
T.Rubya Research Scholar,PSGR Krishnammal college,Coimbatore.


doi:10.4304/jait.2.2.80-86

authenticating the data using patients biometric , encrypting the data using Quasi Group cryptography after compressing the image data using an energy efficient number theory based technique.

A.K.Mohapatra *et al.*,[6] discussed the Security of Biometric Template encryption. This paper presents a modified biometric encryption algorithm which successfully overcomes the limitations of the biometric encryption algorithm for image based templates.

Maruti Venkat Kartik Satti *et al*.,[5] suggested the application of speech scrambling system. In this system he has shown that quasigroup scrambling constitutes an excellent method of encryption and generation of pseudo-random sequences. The randomization obtained is very good and therefore there would be many practical applications of symmetric cryptography where this method found to be useful. In this paper he suggested a Quasi Voice Scrambler which is capable of converting a voice signal to a random noise. The proposed MIQE algorithm could use several group orders (in our examples we use two) and in thier example they use six indices. Thus the proposed example system can compete with DES.Since the complexity involved in breaking DES is simply $2^{64}$ possibilities for a key size of 64 bit. The RSA, on the other hand provides greater security than this for the typical values that are currently used. This process can always use appropriate length keys and index numbers and the value of nonce to obtain security that exceeds that of DES as well as RSA or the ECC cryptosystems.

Bhattacharyya *et al.*,[1] proposed a discrete fourier transformation based image authentication technique. The author proposed that instead of direct embedding a message or image within the source image, choosing a window of size 2 times of the source image in sliding window manner then converts it from spatial domain to frequency domain using discrete Fourier transform (DFT). The bits of the authenticating message or image are then embedded at LSB within the real part of the transformed image. Inverse DFT is performed for the transformation from frequency domain to spatial domain as final step of encoding.

Markovski *et al.,* [2] proposed a Secure two way online communication by using quasigroup enciphering with almost public key. This Quasigroup Enciphering method is based on using quasigroups for defining suitable encryption and decryption functions. Kak [3] presents the concept of secret-hardware public-key (SHPK) cryptography which allows the design of efficient systems, provided there exists a trusted central authority to generate key pairs.

Xuanwu [4] analyzed the security threats and system flaws of present key management schemes. Combining (t,n) threshold cryptography and key management, the author present a threshold key management scheme based on ECC ( Elliptic Curve Cryptosystem ). By utilizing secret key sharing and probabilistic encryption algorithm in key management, the scheme achieves threshold management of symmetric key and public key certificate, avoids the relevance between different certificates generated by the same CA (Certificate Agency) or KDC (Key Distribution Center). The scheme avoids the misuse of certificate generation and anonymity of CA/ KDC members, effectively prevents coalition attack, intruder-in-middle attack and generalized certificate forgery.

## III. METHODOLOGY

### A. *Latin Squares and Isotopes*

A Latin square [5][6] of order 'n' is an 'n' by 'n' array in which each of the '$n^2$' cells contains a symbol from an alphabet of size n, such that each symbol in the alphabet occurs just once in each row and once in each column. Then a matrix such that the row or column consists of elements from 1 through 'n' is built. If permutation is carried in any way the rows, or the columns, or the symbols, of a Latin square, the result is still a Latin square. It can be said that two Latin squares L and $L_0$ are isotopic if $L_0$ can be obtained from L by performing certain row or column permutations or substitution or all three on it. Based upon the order several isotopes of the same fundamental quasi group can be found. The number of isotopes can be give be n! (n-1)! Which is tremendously large for large values of n, for example for n=5, a total of 161280 Latin squares can be formed.

In the proposed implementation the fundamental Latin square [8] based on the priori criteria is generated and then the isotopes are generated based on the same. The number of isotopes that are to be generated should be fixed because there are many isotopes for any Latine square. Since if the number of isotopes generated is a compromise between the security and the space available,it is up to the network provider and the user to come to a common agreement. It is imperative that the length of the index vector is less than the number of isotopes generated.

### *B. Quasi Group*

A quasi group [7][10] Q may be defined as a group of elements (1, 2, 3… n) along with a multiplication operator such that for its elements x and y there exists a unique solution z, also belonging to Q, such that the following two conditions are obeyed:

x*a=z
y*b=z

A quasi group may be defined alternatively as a binary system (Q,*) satisfying the two conditions:

1. For any a, b belonging to Q there exists a unique x belonging to Q such that a*x=b
2. For any a, b belonging to Q there exists a unique y belonging to Q such that y*a=b

The multiplication table of a finite quasi group is a Latin square. In effect it means that if a square matrix is made with n symbols such that a symbol does not repeat itself in the row or the column then Latin square can be obtained. Then the Quasi group is obtained by indexing the Latin square. If 'q' is considered as row index and the

column index as ‘p’ then the product of ‘p’ and ‘q’ would give ‘a’ (an entry in the table correspond to row index ‘q’ and column index ‘p’). Thus ‘a’ denotes the product of ‘q’ and ‘p’. It can be called a group because the product of any two symbols within the quasi group results in an element that lies with the symbol set that constitutes the group.

Consider an example of a quasi group Q of order 5 with elements (1, 2, 3, 4, 5) is given by the element multiplications of Table 1.

A multiplication operator in a quasi group behaves as a mapping between the row and the column indices. For example if x = 1 and a = 5, the resulting ‘z’ can be determined by looking up the element having the row index of 1 and the column index of 5 in Table 1. The value of z is obtained as 1.

*C. Encryption*

Since the quasi group, encryptor performs an operation on the input data and produces a randomized output sequence.

However one can also use the cipher for block encryption. The block encryption scheme has the advantage of low error rate while the stream cipher implementation has the advantage of being simple to implement.

The mathematical equation used for encryption is given by:

$$E_a(a_1,a_2,a_3,\ldots,a_n)=b_1,b_2,b_3,\ldots b_n \quad (1)$$

Where E stands for the encryption function and output sequence is defined by:

$$b_1=a*a_1$$
$$b_i=b_{i-1}*a_i$$

Where *i* increments from 2 to the number of elements that have to be encrypted, and *a* is the *leader* or the *hidden key.* Equation (1) describes a typical single level quasi group encryptor.

The following section illustrate the working of equation (1) with the help of the illustration of Figure 2,

TABLE I
MULTIPLICATION TABLE FOR A QUASI GROUP, N = 5 [5].

| * | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 1 | 3 | 4 | 2 | 5 | 1 |
| 2 | 4 | 1 | 5 | 2 | 3 |
| 3 | 2 | 3 | 1 | 4 | 5 |
| 4 | 1 | 5 | 4 | 3 | 2 |
| 5 | 5 | 2 | 3 | 1 | 4 |

for which the value of a=2. This equation maps the initial input data vector $(a_1,a_2,a_3,a_4,a_5,a_6)$ = (2,4,1,2,3,3) into the vector $(b_1,b_2,b_3,b_4,b_5,b_6)$ for the case of the quasi group of Example 1 with the multiplication relationship of Table 1. The following steps are used during the process of encryption:

$b_1=a*a_1=2*2=1$
$b_2=b_1*a_2=1*4=1$
$b_3=b_2*a_3=4*1=4$
$b_4=b_3*a_4=4*2=5$
$b_5=b_4*a_5=5*3=1$
$b_6=b_5*a_6=1*3=2$

Thus the sequence obtained is (1, 1, 4, 5, 1, 2) and then given as an input to another level of the encryptor. This process is repeated for several times. This multiple levels of mapping ensure that the resemblance of the output data to that of the input data is minimized, making it harder for the eavesdropper to decrypt the data until he has sufficient information regarding the number of times the mapping was done by the sender.

In a variation to this approach, the multiplier element is varied, and generated by a special algorithm called MEG1 that generates the multiplier elements based on the index numbers, nonce, and r and s.

This variant implementation may be given by the following equations:

$$E_{h1,h2,h2\ldots hn}(a_1,a_2,a_3,a_4\ldots a_n)=e_1,e_2,e_3,\ldots e_n \quad (2)$$

Where

$e_1=a*a_1$ and $e_i=e_{i-1}*a_i$

In the above equation the incoming stream of data is first mapped using the first multiplier element $h_1$ then the resultant steam is mapped considering the second multiplier element $h_2$ , and this process continues till all the multiplier elements are exhausted.

Consider Equation 2, the vector $(h_1,h_2,h_3,\ldots h_n)$ consists of all the multiplier elements .In this approach this encryption key is transmitted along with the quasi group (this key is itself encapsulated by another layer of encryption). It is understood that in the above two approaches another reliable encryption algorithm is required to preserve the secrecy of the encryption.

$$b_1=h_1*a_1;\ b_2=b_1*a_2;\ldots\ b_n=b_{n-1}*a_n \quad (3)$$
$$c_1=h_2*b_1;\ c_2=c_1*b_2;\ldots\ c_n=c_{n-1}*b_n$$
$$\vdots$$
$$e_1=h_n*s_1;\ e_2=e_1*s_2;\ldots e_n=e_{n-1}*s_n$$

Thus encryption in MIQE is represented by

$$QE^{I_r,I_s}_{h_1,h_2,\ldots h_n}(a_1,a_2,a_3\ldots a_n)=e_1,e_2,e_3,\ldots e_n \quad (4)$$

where $(a_1,a_2,a_3,\ldots a_n)$ is the input vector and $(e_1,e_2,e_3,\ldots e_n)$ is the output vector, Ir and Is are indices corresponding to the order of the quasi groups. The vector $(h_1,h_2,h_3\ldots h_n)$ is called the hidden key or the secret key.

In hidden key vector the first half entries are generally used as multiplier elements with the first half index

numbers in the Index vector (index in short refers to the isotope of the correspond quasi group ‘r’ or ‘s’) and the second half are used as multiplier elements with the second index numbers in the Index vector.

*D. Decryption*

This process is similar to encryption. First, the generation of the inverse matrix will be described. For this one needs to understand the left inverse ‘\’ I used for the quasi group decryption (Figure 4 illustrates the encryption and decryption of data).

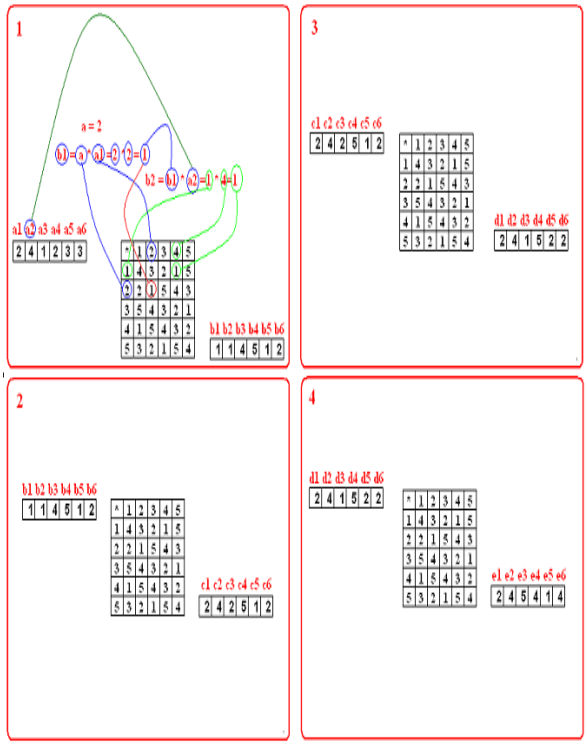


Figure 4. Quasi group mapping using an order 5 quasi group[5].

The basic equation for encryption is as below:

$$D(a_1,a_2,a_3,\ldots a_n)= e_1,e_2,e_3,\ldots e_n \quad (5)$$

Where

$$e_1=a\backslash a_1 \text{ and } e_i=a_i\text{-}1\backslash a_i$$

To perform the process of decryption, first generate the inverse matrix of a given quasi group and execute mapping procedure as described in the previous section (Figure 2). This must be done using (5).

The decryptor for a multilevel indexed based algorithm can be defined as follows:

$$QD^{J_r,\ldots J_s}_{h_n,h_{n-1}\ldots h_1}(e_1,e_2,e_3,\ldots e_n)=a_1,a_2,a_3,\ldots a_n \quad (6)$$

The method of the MIQE decryptor is similar to the MIQE encryptor as shown below.

1. The elements of the quasi group (marked as 1 in Figure 4) are labeled as w, the indices along the horizontal are labeled v and the indices along the vertical are labeled u.

2. The elements of the inverse (left-inverse) of quasi group (labeled as 2 in Figure 4) are labeled as v, the indices along the horizontal are labeled w and the indices along the vertical are labeled u-1.

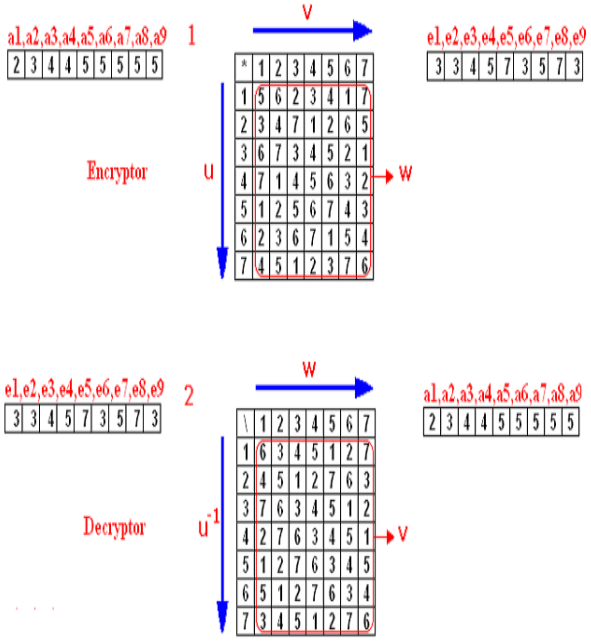


Figure 3. Determination of left division and the compete process of encryption and decryption [5].

## IV. Experimental Result

The theory of quasigroups applications in cryptology goes through the period of rapid enough growth. Quasi groups (or Latin squares) provide a powerful method for generating a large set of permutation transformations by permuting across their range. Retinal image has been selected for the encryption using quasi group method. The first step is the features of retinal image are extracted. Then the quasi group and Leader have been generated and passed as key while encrypting the retinal features. Different quasi groups can be generated at different times. So that different leaders can be used at different situations. So it is not so easy for the hacker to guess the key and trace the original templates. After the encryption the original image has been transferred into unpredictable format.

The Figure 3 is the original retina image taken for the encryption. From that image retinal feature are extracted. The fig 4. Contains the feature extracted image. This undergo the process called Thinning.

Figure 3. Original retina image

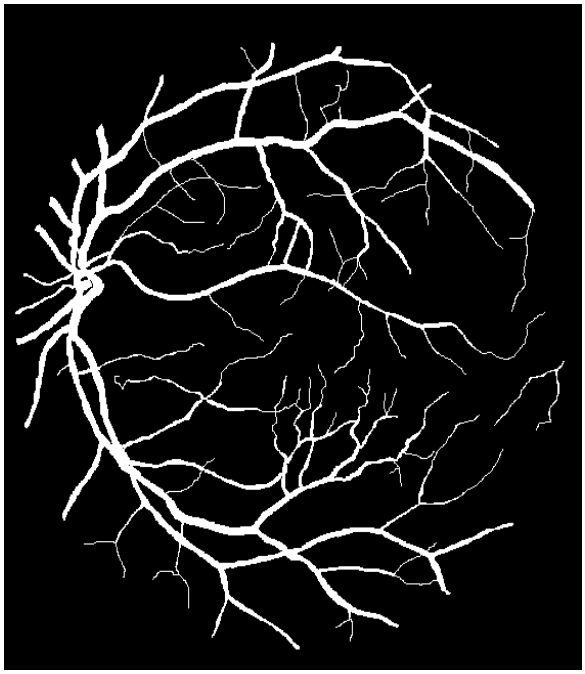

Figure 4. Feature extracted image

From which the quasi group is been generated. This image has been encrypted by using randomly generated encryption key. This process used seems to be a symmetric key encryption. Because the same set of keys are used for both encryption and decryption process.

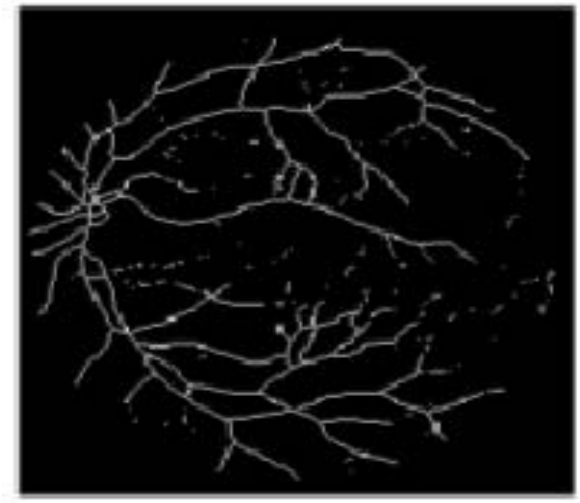

Figure 5. Feature extracted image (Thinned image)

Figure 6. Encrypted image (Thinned image)

Figure 7. Decrypted image (Thinned image)

The above Figures 5,6 and 7 show the result of feature extracted ,encrypted using quasi groups and decrypted image. The Purpose of selecting retina is it has certain advantages over other biometric traits. Retinal scans are used in high-end security applications like access control to areas or rooms in military installations, power plants,

and other high risk security areas. There is no known way to replicate a retina and the eye from a dead person would deteriorate too fast to be useful, so no extra precautions have to been taken with retinal scans to be sure the user is a living human being. In this paper, the security is increased by using different types of leaders which includes so many permutations. So that it is difficult for the hackers to reveal the secret information.

## V. PERFORMANCE ANALYSIS

The performance has been measured by generating histogram with specified parameters. Image histograms can be useful tools for thresholding. Because the information contained in the graph is a representation of pixel distribution as a function of tonal variation, image histograms can be analyzed for peaks and/or valleys which can then be used to determine a threshold value. This threshold value can then be used for co-occurrence matrices.

When the histogram of the encrypted image is considered, it appears very uniform and does not resemble with the original image's histogram. The histogram of the Retina feature extracted and encrypted image is shown in figure 9 and 10. Due to vast difference in both the images the attackers cannot easily trace the original features.

Let X be the linear form of an image. Let E(y) be the expected value for variable y. Then, the covariance matrix for an image is calculated using the following equation:

$$C[i, j] = E((X[i] - E(X[i])(X[j] - E(X[j]))$$

The covariance matrices of the given original image and its encoded image are plotted in figure 11 and 12 respectively. The comparison of these two matrices shows that it is very difficult for the statistical attackers to find the similar image.

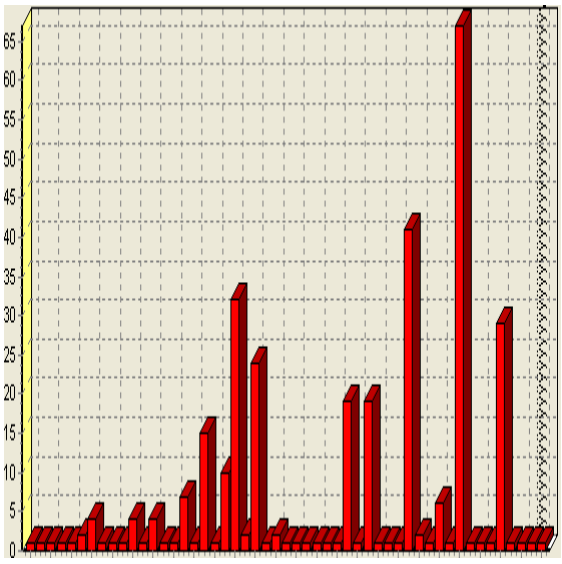


Figure 8. Histogram of the original Retina image

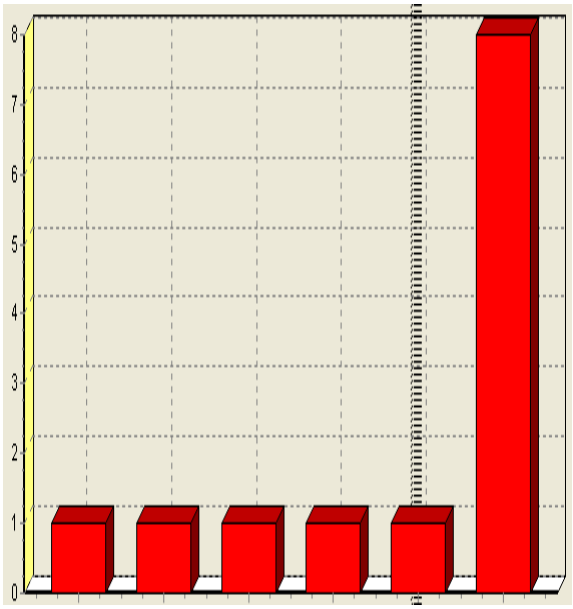


Figure 9. Histogram of the encoded image

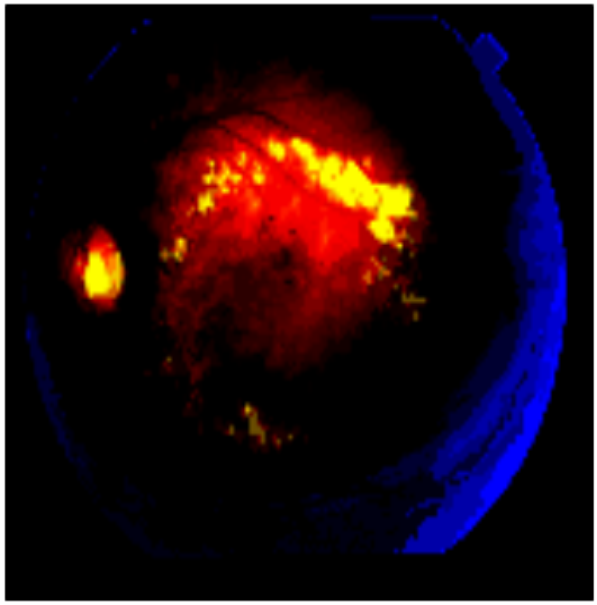

Figure 10. Covariance for the original image

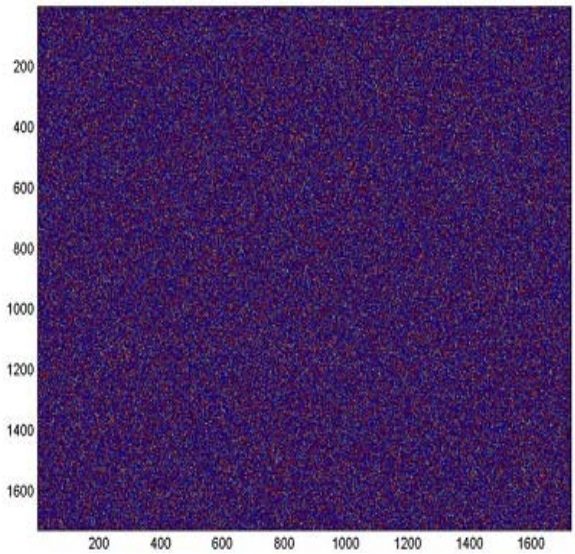


Figure 11. Covariance for the encoded image

## VI. Conclusion

In this paper, Security provide to Retina Template has been discussed. This paper presents a quasi-group based retinal encryption which successfully overcomes the limitations of the biometric encryption algorithms for image based templates. The usage of Quasi group in key generation makes the digital data transmission more secure when compared to the existing algorithms. Construction of large and unstructured quasi-group is useful for design of encryption schemes with a different selection of leaders at different situation. The proposed methodology which uses quasigroup to boosts up the security of retina templates. Statistical analysis using histograms and correlation showed that the proposed method is not vulnerable to statistical attacks. In addition, the huge number of possible keys makes a brute-force attack on the proposed method impossible. Hence the proposed retina template encryption using quasi-group is robust against stored biometric template attacks and it is used to protect biometric templates and secret data. Future work will be carried out in different biometric models to improve the security.

## REFERENCES

[1] Bhattacharyya, D. Dutta, J. Das, P. Bandyopadhyay, R. Bandyopadhyay and S.K. Tai-hoon Kim," Discrete fourier transformation based image authentication technique", Cognitive Informatics, 2009. ICCI '09. 8th IEEE International Conference on June 2009.

[2] S.Markovski, D. Gligoroski and B. Stojcevska,"Secure two way online communications by using quasigroup enciphering with almost public key".

[3] Kak. S, "On secret hardware, public-key cryptography," Computers and Digital Technique (Proc. IEEE - Part E), vol. 133, pp. 94-96, 1986.

[4] Xuanwu Zhou Ping Wei," Key Management Scheme Based on (T, N) Threshold Cryptosystem", Intelligent System and Knowledge Engineering, 2008. ISKE 2008. 3rd International Conference on Nov. 2008.

[5] Maruti Venkat Kartik Satti B.Tech, "QUASI GROUP BASED CRYPTO-SYSTEM" Gokaraju Rangaraju Institute of Engineering and Technology, 2005 Hyderabad, India December 2007.

[6] Mohapatra1. A.K, Madhvi Sandhu2," Biometric Template Encryption", IGIT, GGSIP University,Kashmere Gate,Delhi, International Journal of Advanced Engineering & Application, Jan. 2010.

[7] S. Kak and N.S. Jayant, Speech encryption using waveform scrambling. Bell System Technical Journal, vol. 56, pp. 781-808, 1977.

[8] Vaudenay. S: On the need for multipermutations: Cryptanalysis of MD4 and SAFER, Proc. Fast Software Encryption, pp 286–297,1994.

[9] Denes.J. Keedwell., A.D.: Latin Squares and their Applications, English Univer Press Ltd 1974.

[10] Bakhtiari, S., Safavi-Naini, R., Pieprzyk, J. 1997. A Message Authentication Code Based on Latin Squares, Proc. Australasian Conference on Information Security and Privacy, pp. 194–203, 1997.

[11] Gligoroski, D. 2005. Candidate One-Way Functions and One-Way Permutations Based on Quasi group String Transformations. arXiv:cs. CR/0510018.

[12] S. Singh, "The Code Book: The science of Secrecy from Ancient Egypt to Quantum Cryptography" Anchor Books, New York, 1999.

[13] Merkle R. C, Secrecy, authentication, and public key systems. Stanford Ph.D. thesis 1979, pages 13-15.

[14] Smith J. D. H. , An introduction to quasigroups and their representations, Chapman & Hall/CRC,2007.

[15] Pal S. K., Bhardwaj D., Kumar R., Bhatia V., "A New Cryptographic Hash Function based on Latin Squares and Non-Linear Transformation", Proceedings of the 2009 IEEE International Advance Computing Conference, pp. 2529-2534, 2009.

[16] Schneier B., Applied Cryptography (Second Edition), John Wiley & Sons, 1996.

[17] Hussain S.M., Ajlouni N.M., "Key Based Random Permutation", Journal of Computer Science, Vol. 2, No. 5, pp. 419-421, 2006. Koscielny C.Z. , "Generating Quasigroups for Cryptographic Applications", International Journal of Applied Mathematics & Computer Science, Vol. 12, No. 4, pp. 559-569,2002.

[18] Meyer K.A., "A New Message Authentication Code Based on the Non-associativity of Quasigroups", Doctoral Dissertation, Iowa State University Ames, Iowa, 2006.

[19] Rajeswari Mukesh, Damodaram. A, V.Subbiah Bharathi, "Energy Efficient Security Architecture For Wireless Bio-Medical Sensor Networks", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 6, No.1, 2009