International Journal of Advanced Science and Technology
Vol. 29, No. 6, (2020), pp. 2406 - 2417

A Technique to Secure Multimodal Biometric Data Using Visual Secret Scheme

[1]Gayathri. M*, [2] Malathy. C

SRM Institute of Science and Technology
gayathrm2@srmist..in, malathyc@srmist.edu.in*

Abstract

With the increase in usage of Biometri sures that edu keep our data safe and secure. Using multimodal biometric systems c parameters to identify individuals, it has become imperative to deploy stringent security mea ensure better protection against identity theft while using advanced cryptography techniques ensure better protection against breach of information to hackers. In this paper, we propose a secured multimodal biometric system with two biometric modalities, Fingerprint, and Iris. our proposed grey scale visual cryptography technique is to used to secure the bio-metric data during the transmission and in storage of biometric data in database . In grey scale visual cryptography, each of the grey scale images is divided into parts called shares. The shares individually, will appear like noise, but when stacked together for decryption, reveals an image that would act like the key. Thus, this proposed system serves two purposes, Data Authentication and Confidentiality.

Keywords: *Authentication, Visual cryptography, biometrics, security, shares.*

1. Introduction

Security is considered to be one of the important aspects of technology. Great priority is given to our privacy and security. The data hacked by others is almost a sensitive threat to our data. This made us propose a system of security. We chose efficient biometric parameters as the core for authentication and have proposed a way of protecting sensitive data. Our system has two phases'. The Authentication and Data confidentiality. The authentication method we adopt here is the biometric mode of authentication. Biometric authentication is a security process that works based on the biological characteristics of a human being in order to verify that they are the person whom they claim to be. Biometric authentication systems use methods, which compares a live template of biometric data captured to a stored template in database. If both the templates of the data match, then the authentication is done. Confidentiality is way of securing data that is being accessed by unauthorized parties. In other words, the people who have proper authorization rights will gain access to the data. Visual cryptography is a frequently used Cryptographic technique in the field of computer vision for keeping

databases with images secured from data thefts. This algorithm permits any information that can be seen such as pictures, to be encrypted such that decryption of the encrypted information can be done by plain sight seeing. Thus, we are going to use this cryptographic technique to secure the biometric data of the users.

The use of hybrid biometric parameters to create a multimodal system and a brand-new cryptographic algorithm form the core of the innovation in this system. The new cryptographic algorithm proposed uses multiple sensitive images to hide each other individual image. In other words, the images themselves hide each other in such a way that no individual image can be extracted without the proper keys. This reduces the trouble of creating multiple shares for each image but rather create shares common to a pair of images. In addition, it reduces the space complexity of existing algorithm to half because of the use of a pair of images instead of one. This algorithm can be a breakthrough in the current domain of visual cryptography as it solves many existing flaws. On a further note, this algorithm can actually be used recursively to reduce the complexity exponentially. The output of one pair of images, after merging can be used as the first image in the next pair of images used and so on. This thus can create a unique image for various dimensions of biometric data instead if storing all of them individually. The final obtained image must be encrypted using the existing encryption algorithms and shared for communication.

1.1 Importance of security:

Security is of great concern in today's world. We have various modes of authentication and we collect a large amount of sensitive biometric data for this purpose. Thus, it is also our responsibility to secure this personal data in an efficient manner. In order to compromise the data privacy of a user, hackers steal the information from digital devices to benefit themselves. This is called data theft and is a very common practice when it comes to illegality acquiring authentication into any system, product or service by stealing and manipulating the user's biometric data. Information can include anything from financial information to personal information like biometric data. Data theft is a growing problem for everyday computer users with respect to large businesses and organization. The more sensitive the data is, it attracts most of the hackers. Thus, protecting such data is step one in the post-process of storing it. Through this work, we aim to fulfil this security drawback in storing sensitive biometric data of people. This proposed work aims at creating a unique image for every individual by combining few traits biometric data into one image. The captured image is divided into shares and transmitted securely in the network and it is stored at various sites on a distributed storage system. Only the right keys can extract the actual data from them, thus making it secure from the outside world.

1.2 Visual Cryptography

Visual cryptography method is considered as secure way of encrypting a material in a method of shares and decrypting is done by visual system. The basic model proposed by Naor and Shamir consists of different shares of cipher text, which is a secret shared key. The original text can be revealed by placing the all the individual shares over the system with the cipher text, even though each one of them is indistinguishable. The model proposed by Naor and Shamir is further extended into a method of the k out of n secret sharing problem. If there are n shares k shares will be utilized to form the original image or the secret. combination of multiple black and white pixels such that each pixel is operated individually. Each of this pixel appears in n modified versions is called shares.

The original problem of visual cryptography is a special case of the 2 out of 2 visual secret sharing problem. It can be solved by dividing each pixel into to sub pixels, which in general practice can distort the aspect ratio of the original image. Thus, to solve this drawback, it is recommended to use 4 sub pixels arranged in a 2 X 2 array and each share can take one of the following forms in Figure 1

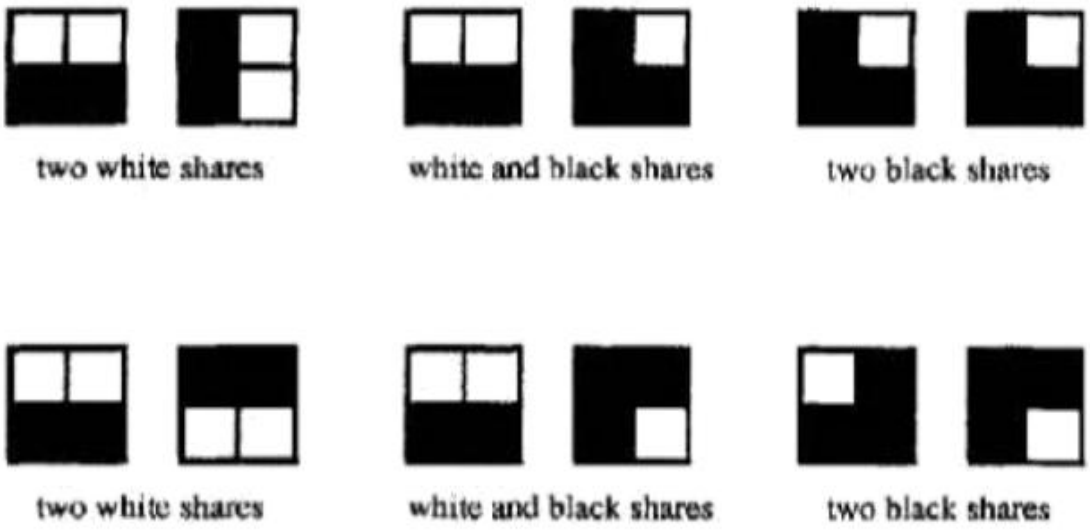

Figure 1. The representation of a 2x2 pixel shares for an image

2. Literature survey

In paper [17], the author proposes to use Stream Ciphers for the generations of a onetime password from the fingerprint biometric data. Standard stream cipher Rivest Cipher 4 is used for the Fingerprint code extraction. The code then goes through the Bio Hashing function that features standards methods- Secure Hashed Algorithm or Message Digest 5. The bank and the receiver share the 128 bits or 256 bits key.[18] Proposes the possibility of using visual cryptography paired with chaotic encryption, suitable for securing static biometric data. A private biometric image will be broken into two host images.

Chaotic systems are then used to encrypt them independently. Two different database servers are used. They are used to transmit the results and to store them in different servers for ensuring the security of the overall data. The private data identity is of utmost importance and it is seen that it must not be revealed to the other server. While the process of authentication process is going on, the enrolled and authenticated entity is required to send a request to all the servers involved. Thus, the corresponding shares are decrypted and transmitted to it. Shares are also super imposed in order to reconstruct the private image. In paper [19], the author proposes a new watermarking approach, which reduces the storage space and produces a quality-reconstructed image. It is also reinforcement in nature. The suggested approach is validated on two biometric modalities, fingerprint and face, and it is applied two times to improve the security level. Face image is watermarked and it is inserted into the enrolled image of fingerprint. This method helps in finding an individual accurately. [19]. Paper [20] proposes a spatial steganography algorithm to secure lips biometric data. Scale Invariant Feature Transform (SIFT) detect Local interest points. Using these points lip features are extracted and they employ minimum distortion when being utilized. In spatial domain the modulation technique is used for the lip images with some identifiers so that this takes care of that the image and the difference is less compared with the original lip images, and it guides proper recognition rate. The iris and dual fingerprint modalities are combined together with the

fuzzy technique to generate the key and to provide proper recognition accuracy. The hash function plays a major role in securing the traits and they work on structured dataset. The unstructured points of minutiae are converted into structured pints in order to cooperate with the key generation procedure. [21]

3. Design of the proposed methodology

Our work is largely about focusing on how to accurately authenticate a user based on multi modalities of biometrics while keeping his/ her data secure in the database. Thefts of Biometric data cannot only help in overriding the system but also the malpractice of the data in other places outside the scope of the biometric system under discussion. Hence, there are essentially two parts of the problem that we are addressing:

1. Biometric System Data Security
2. Biometric Authentication

3.1 The Biometric Data Security System:

Security system addresses the vital need of the data protection against data theft within the biometric system. A Visual Cryptography technique is implemented to carry out this task. In reality, this can be seen a simulation in which, the data storage is done in the form of the single image involving visual cryptography. Essentially, even if the data is lost, it cannot be deciphered and does not possess the threat of wrong usage. The shares developed will not reveal any meaningful information. The shares are transmitted in the network securely.

3.2 The Biometric Authentication System

Authentication part is for the computation of all the direct biometric system work, collecting enrolment data, and training on existing datasets to determine important features to be extracted. Feature extraction from the images of the biometric traits, features matching for the purpose of authentication, computing fusion algorithms for the biometric data, decision making about whether to accept or reject a user for authentication

3.3 Biometric Traits Used

The biometric traits, which we used, are Fingerprint impression and Iris . The sensors for these biometric traits have the advantages but not limited to, benefits over other sensors for other biometrics traits, they are Easy to use, Cheap with small sizes, portable, need low power to operate, on intrusive, huge databases

3.4 Dataset Used

CASIA datasets for all the two modalities are taken for experimentation. CASIA-IRISV3 dataset is used. It consists of total 22,034 images from over 700 individuals. Every image is 8-bit grey level JPEG image. Experiment was carried on 40 images from them. Images are gathered under infrared illumination. It includes three subsets of datasets labelled as:CASIA-Iris-Interval, CASIA-Iris-Lamp CASIA-Iris-TwinsCASIA-ATVS FFp Dataset is used. 40 images from the given dataset are utilized for experimentation.

3.5 Proposed Frame Work

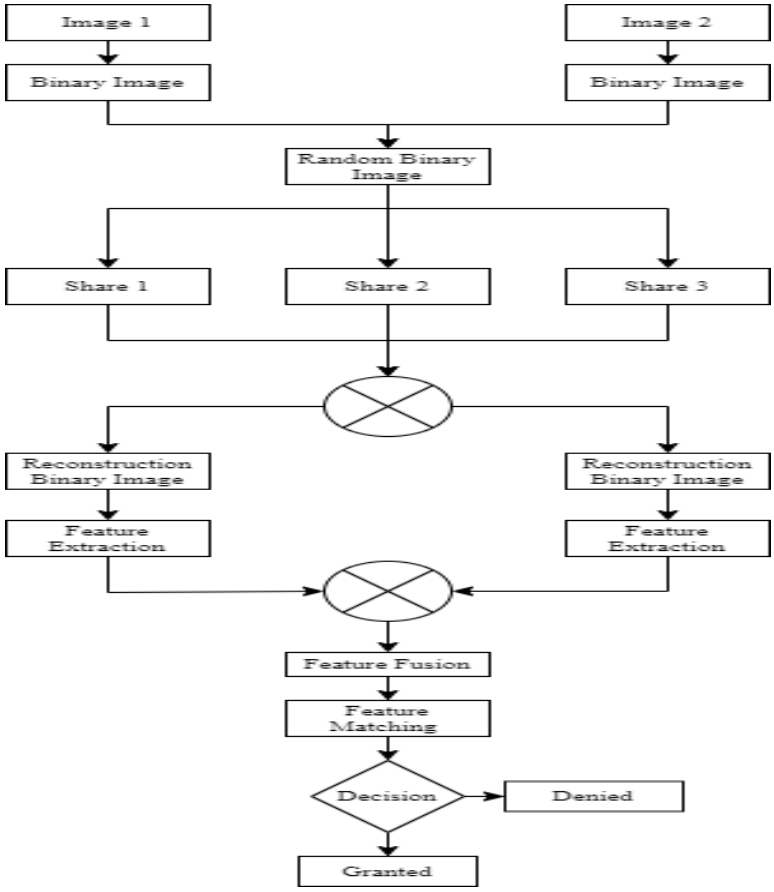

Figure 2. Proposed Frame Work

Form the flow diagram as in figure 2 the two biometric modalities are input to the model. The image is converted into binary image using the Local Binary Pattern algorithm. Random binary matrix is created by the size of the image. Then the three images are combined and shuffled to create the shares. Three shares are created using the three images. The proposed algorithm used for sharing is Reverse Index Shuffling (RIS). The shares are reconstructed back into images using the Inverse Reverse Index Shuffling (IRIS). From reconstructed images, the features are extracted. Using the local binary pattern feature extraction, the features are extracted from the reconstructed image. The feature values are fused then using the feature fusion-matching algorithm, recognition of the biometrics is recognized.

In phase 1 securing the data in the transmission and storage in database of a biometric system is imperative in order to avoid data thefts and mal practice of the data. Various cryptographic techniques exist which Address to this need. However, the process of securing the data adds up to the consumption of memory and speed of the authentication process. We have proposed new technique of securing the data in our work called RIS. The algorithm takes two images as input and one random binary matrix to produce a set of shares as output. This is based on the principle of Visual Cryptography in which shares of an image can be stacked on top of each other to see the original image through naked eye. Partial set of shares are shared with the user through the network and the rest are stored in a secured database. The user can access these shares during the decryption by authentication. The original images can only be visible after combining all the shares.

The original reconstructed image is used extract the features using the LBP feature extraction algorithm. These features values are used for the feature fusion-matching algorithm. Using the matching algorithm, the authentication of the biometric is completed. First input image is shown Figure 3. The proposed methodology two modality are used. Iris and finger print images are used. These images are taken form the CASIA dataset.

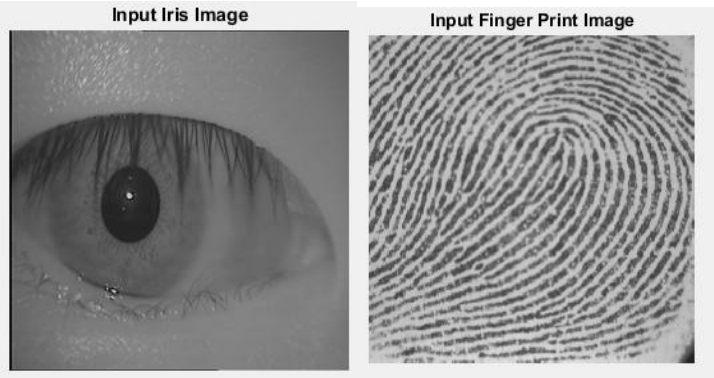

Figure 3. Input Images

Then the input image is converted into binary image using the Local Binary Pattern. The binary image shown in the figure 4.

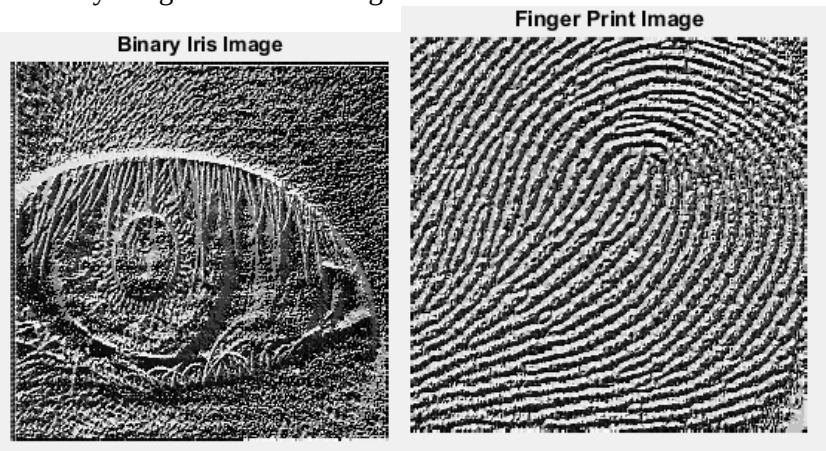

Figure 4. Binary Input Image

For creating the share the random binary matrix is created. The size of the random binary iamge is same as the input image. In figure 5 shows the random binary image. This image is usde for ensure the data security form the attackers.

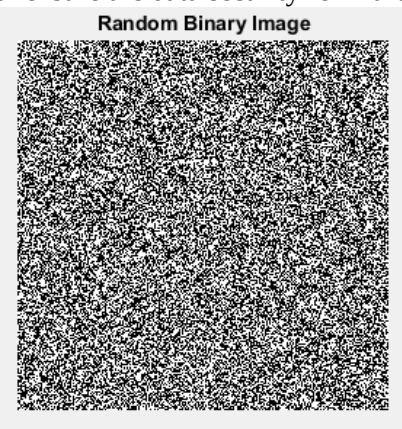

Figure 5. Random Binary Image

The image shares are created using the random matrix and two binary matrix. The algorithmof sharing is proposed by RIS. The shares are reconstructed and the binary features are extracted from the reconstructed binary image using IRIS. The share of image from RIS is shown in the figure 6.

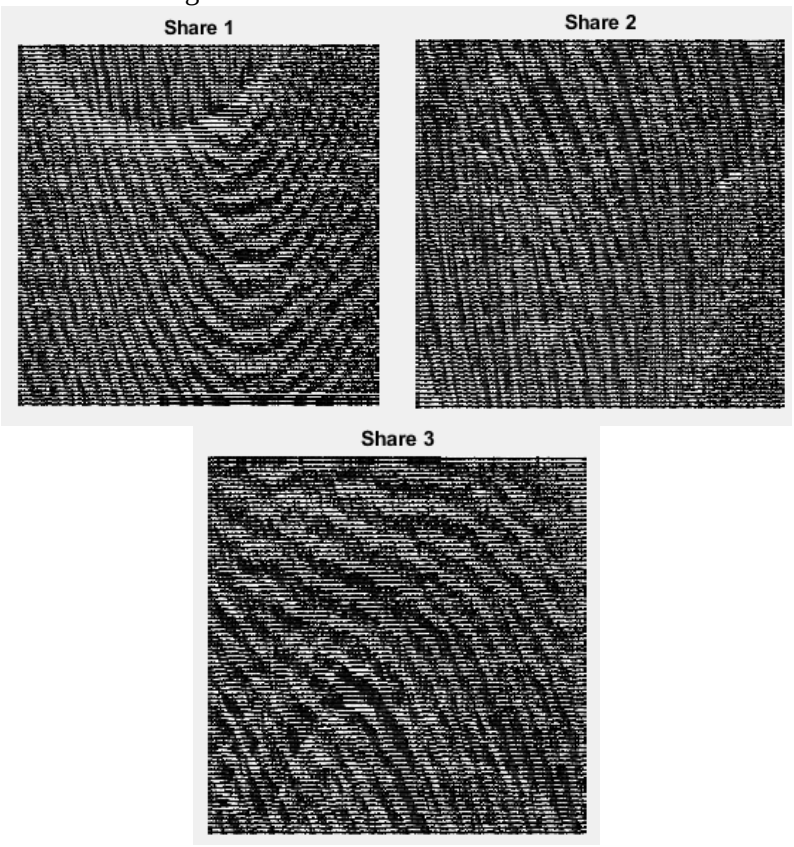

Figure 5. Shares

From the 3 shares the original image is reconstructed using the IRIS algorithm. The reconstructed orignal image is shown in the figure 7.

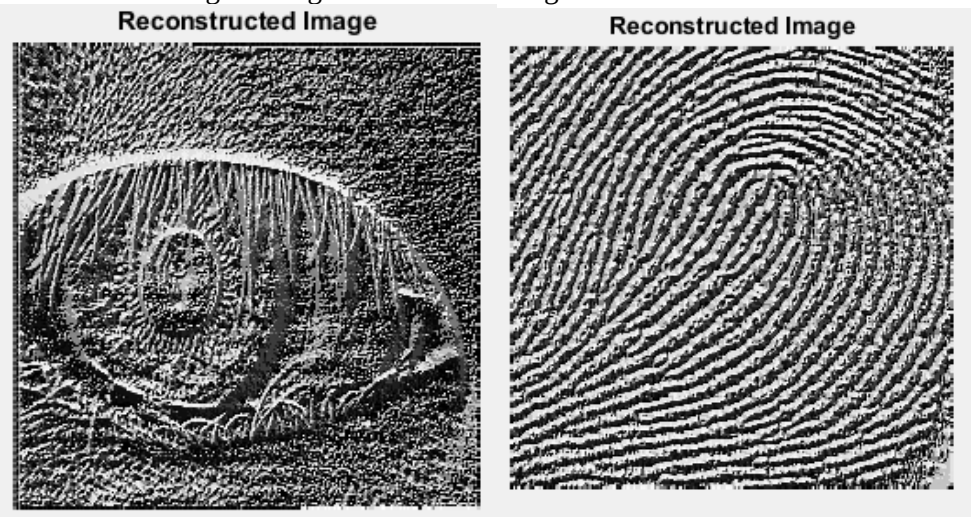

Figure 7. Reconstructed Orignal Image

Form the reconstructed image the values are features values are extracted using the local binary pattern feature extraction and the feature values are matching with the matching algorithm for image matching and recognition.

3.6 Proposed Pseudo code Algorithm:

STEP 1: Input the Iris and Finger print image
STEP 2: Convert the input image into binary image using the local binary pattern algorithm
STEP 3: Create the random binary matrix image with the size of input image
STEP 4: Shares are created using the three images by Reverse Index Shuffling algorithm
STEP 5: The original image reconstructed form the shares using the Inverse Reverse Index Shuffling Algorithm
STEP 6: Features are extracted from the reconstructed image using the Local Binary Pattern Feature Extraction
STEP 7: Using the Feature fusion rule the matching process is completed for authentication

4. Result and Discussion

This section shows the Result and discussion of the proposed methodology compared with existing methodology. The evaluation and comparison performed using the quality metrics introduced by each challenge organizer.

Table: 1 Parameter in algorithm

Parameter	**Jia et al. [1]**	**Lin et al. [2]**	**Fang and Lin [3]**	**Chen and Wu [4]**	**Yang et al. [5]**	**Deshmukh et al. [6]**	**Proposed method**
Achieving threshold	Yes	Yes	Yes	No	Yes	No	***No***
Property Hiding method	VC	RG	Polynomial	Boolean	Boolean	Additive modulo	***Index arithmetic***
Recovery type	Recognizable	Recognizable	Loss	Lossless	Lossless	Lossless	***Lossless***
Alignment	Hard	Hard	Easy	Easy	Easy	Easy	***Easy***
Pixel expansion	Yes	No	No	No	No	No	***No***
Codebook Requirement	Yes	No	No	No	No	No	***No***
Share shape	Rectangle	Circle	Rectangle	Rectangle	Rectangle	Rectangle	***Rectangle***

The table 1. Show the proposed method description with other existing methodology. In achieving threshold, parameter is methodology based on the threshold method. Proposed method not using the achieving threshold. The property hiding or shuffling the two images is using the index arithmetic operation. The recovery of the image is lossless when compared to existing methods. In proposed methodology, the pixel expansion is not processing due to the one random binary image. Codebook is no required for run the program. The shape of the share is in rectangle shape

Table 2: Image quality validation

Scheme	**PSNR (dB)**	**Scheme**	**PSNR (dB)**
Lin & Tsai [7]	39.21	Yang et al. [8]	40.59
Chang et al. [9]	40.97	Wu et al. [10]	43.54
Ulutas et al. [11]	48.62	Eslami et al. [12]	48.13
Khosravi et al. [13]	43.11	Li et al. [14]	48.14
Ahmadian, er.al [15]	49.74	**Proposed**	***53.14***

The PSNR value represents the peak signal to noise ratio. It shows the quality of original image recovered image. The PSNR block generates the peak signal-to-noise ratio, which is used to measure the quality between the original input image and the obtained output image (reconstructed image). If the PSNR is higher, the quality of the reconstructed image is good. The mean-square error (MSE) and the peak signal-to-noise ratio (PSNR) are used to measure the quality metrics. The table 2 shows the PSNR value of proposed methodology with existing methods.

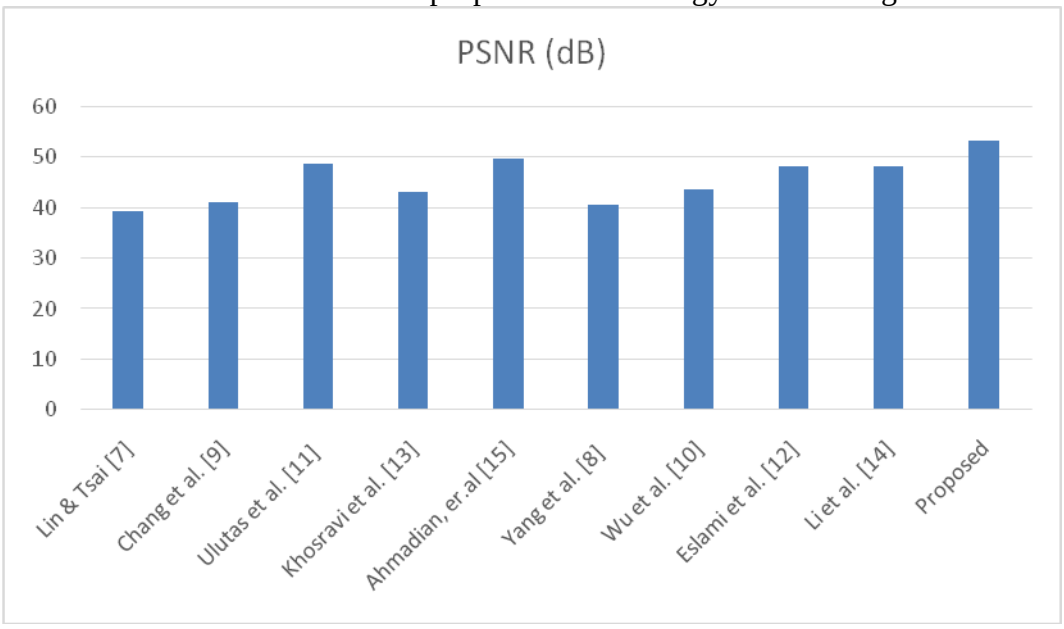

Figure 7. PSNR Comparison

When the PSNR is high in number shows the recovered image is in good quality. It clearly shows in the graph as shown in the figure 7. The proposed method shows the higher value of 53.14 db.

Table 3: Equal Error Rate

Method [16]	**EER**
Gabor (fingerprint)	1.23

SURF (fingerprint)	8.2
SS (Gabor + SURF) (FKP)	2.48
MIN (Gabor + SURF) (fingerprint)	3.25
MAX (Gabor + SURF) (fingerprint)	4.13
MW (Gabor + SURF) (fingerprint)	0.31
(Gabor + SVM) (FKP)	0.19
Proposed (Iris and Finger Print)	***0.15***

The error rate is much reduced in the proposed methodology as compared to the existing methods. The existing methods uses the different modalities in the methodology. The proposed methodology uses the iris and fingerprint shows the better error rate as mention in the table 3.

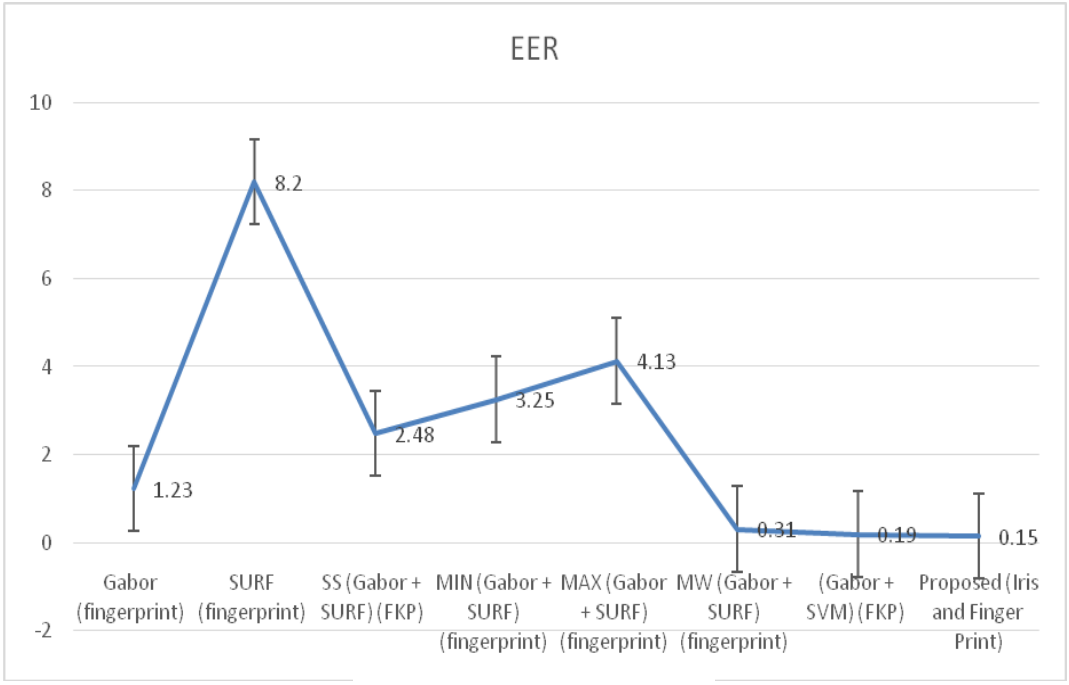

Figure 8. Equal Error Rate

The figure 8. Shows the EER of different methods. Form graphical representation the EER of the proposed method is 0.15, which is much better with the existing methods.

5. Conclusion

Our work aims at providing an algorithm that can securely send and store sensitive information like biometric data, which is used by various domains to authenticate its users. After sufficient research about multi-modal Biometrics and Visual cryptography, we have devised a suitable algorithm that function more efficient than the existing algorithms. The algorithm has proved to successfully reduce storage complexity by half

and increase the security during transmission. The sensitive images like biometric data are divided into shares during transmission, and are authenticated later and are stored securely in distributed environment. The shares are also encrypted before storage to create greater security for them. We have implemented the idea in a small scale but we believe this will have a substantial preference at a large scale.

References

[1] Jia, X., Wang, D., Nie, D., & Zhang, C. Collaborative visual cryptography schemes. IEEE Transactions on Circuits and Systems for Video Technology, 28(5), (2016). ,1056-1070.
[2] Lin, K. S., Lin, C. H., & Chen, T. H.. Distortionless visual multi-secret sharing based on random grid. Information Sciences, 288, (2014)330-346.
[3] Fang, W. P., & Lin, J. C. Universal share for the sharing of multiple images. Journal of the Chinese Institute of Engineers, 30(4), (2007). 753-757.
[4] Chen, T. H., & Wu, C. S. Efficient multi-secret image sharing based on Boolean operations. Signal Processing, 91(1), (2011). 90-97.
[5] Yang, C. N., Chen, C. H., & Cai, S. R. Enhanced Boolean-based multi secret image sharing scheme. Journal of Systems and software, 116, (2016). 22-34.
[6] Deshmukh, M., Nain, N., & Ahmed, M. Efficient and secure multi secret sharing schemes based on boolean XOR and arithmetic modulo. Multimedia Tools and Applications, 77(1), (2018). , 89-107.
[7] Lin, C. C., & Tsai, W. H. Secret image sharing with steganography and authentication. Journal of Systems and software, 73(3), (2004). 405-414.
[8] Yang, C. N., Chen, T. S., Yu, K. H., & Wang, C. C. Improvements of image sharing with steganography and authentication. Journal of Systems and software, 80(7), (2007). 1070-1076.
[9] Chang, C. C., Hsieh, Y. P., & Lin, C. H. (2008). Sharing secrets in stego images with authentication. Pattern Recognition, 41(10), 3130-3137.
[10] Wu, C. C., Kao, S. J., & Hwang, M. S. ,A high quality image sharing with steganography an adaptive authentication scheme. Journal of Systems and Software, 84(12), (2011). 2196-2207.
[11] Ulutas, G., Ulutas, M., & Nabiyev, V. V,Secret image sharing scheme with adaptive authentication strength. Pattern Recognition Letters, 34(3),(2013). 283-291.
[12] Eslami, Z., & Ahmadabadi, J. Z. Secret image sharing with authentication-chaining and dynamic embedding. Journal of Systems and Software, 84(5), (2011). 803 -809.
[13] Arscott, S. (2018). Intrusion detection technique for security statistics. Philippine Statistician, 67(1), 1-8.
[14] Li, P., Kong, Q., & Ma, Y. Image secret sharing and hiding with authentication based on PSNR estimation. Journal of Information Hiding and Multimedia Signal Processing, 5(3), (2014). 353-366
[15] Ahmadian, A. M., & Amirmazlaghani, M.. A novel secret image sharing with steganography scheme utilizing Optimal Asymmetric Encryption Padding and Information Dispersal Algorithms. Signal Processing: Image Communication, 74, (2019),78-88.
[16] Muthukumar, A., & Kavipriya, A. (2019). A biometric system based on Gabor feature extraction with SVM classifier for Finger-Knuckle-Print. Pattern Recognition Letters, 125, 150-156.
[17] A. Godil, Y. Ressler, and P. Grother. Face recognition using 3d facial shape and color map information: comparison and combination. In Proceedings of the SPIE The International Society for Optical Engineering, (2005). pages 351-361,
[18] Suvarnsing G. Bhable, Sangramsing Kayte, Jaypalsing N. Kayte, Dr. Charansing Kayte"Robust Multimodal Biometrics Recognition: A Review" International Journal of Advanced Research in Computer Science and Software Engineering -Volume 5(2015)., Issue 10,

[19] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, Boca Raton, 1997.

[20] Smitha Jacob, Mereya Baby, "Visual Cryptography with Chaotic Encryption for Biometric Templates" International Journal on Recent and Innovation Trends in Computing and Communication. (2003).

[21] Ross, A., Otheman, A.: Visual cryptography for biometric privacy. IEEE Trans. Information forensic and Security 6(1), (2011).

Authors

Gayathri.M is an Assistant Professor in Department of Computer Science and Engineering S.R.M Institute of Science and Technology, Kattankulathur campus, Chennai, India. Currently she is pursing Ph.D(CSE) in S.R.M Institute of Science and Technology, Chennai . She has over eight years of experience in Teaching. Her research interest is Security and Privacy in Biometrics, Network Security, Internet of Things and Cryptography.

CMALATHYis a Professor in Department of Computer Science and Engineering, S.R.M Institute of Science and Technology, Kattankulathur campus, Chennai, India. She earned Ph.D. in Computer Science & Engineering from S.R.M Institute of Science and Technology, Chennai. She has over Twenty-eight years of experience in Teaching and Research. Her areas of interest are Image processing, Data Mining and Computer architecture. She has published research papers in many international conferences and refereed journals.