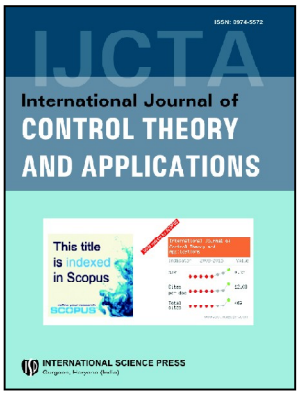

International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 10 • Number 26 • 2017

Three Tier security for the Financial Services & e-Commerce Applications

[1]T. Sridevi, [2]P. Mallikarjuna Rao, [3]P V Ramaraju and [4]G. Nagaraju

[1] Research scholar, Dept. of ECE, AU College of Engineering, Andhra University, Visakhapatnam, A.P., India
E-mail: sridevi.dsp@gmail.com
[2] Professor & Chairman, BoS, Dept. Of ECE, AU College of Engineering, Andhra University, Visakhapatnam, A.P. India
E-mail: pmraoauece@yahoo.com
[3] Professor and Head, Dept. of ECE, SRKR Engineering College, Bhimavaram, A.P.,India, E-mail: pvrraju50@gmail.com
[4] Assistant Professor, Dept. of ECE, SRKR Engineering College, Bhimavaram, A.P., India, E-mail: bhanu.raj.nikhil@gmail.com

Abstract: Information hiding is the most important criteria today in several sectors, due to security issues. Mostly for the security applications used in Finance & banking sectors, hiding the information about users and their transactions are necessary at present from the hackers in all high security zones. In this consequence biometrics is progressively considered as foundation component for an extensive array of personal authentication solutions, both at the national level (E.g. India UIDAI) and the smaller-scale (E.g. banking ATMs, school lunch payment systems). Biometric fraud is also an area of increasing concern, as the number of deployed biometric systems increases and fraudsters become aware of the potential to compromise them. Organizations are increasingly deploying process and technology solutions to stay one step ahead. At present Bankers are using different single Biometric Modalities for different services. All Biometric features are not suitable for all services because of various artifacts while extracting features from the sensors due to background noise, lighting conditions, ease of access etc. This paper proposes a multi model system that will show a onetime single solution to meet all their security problems. This paper particularly handles how to incorporate cryptography and steganography in biometric applications.

Keywords: cryptography, steganography, biometric applications, security.

1. INTRODUCTION

To date, biometric technologies have been most widely adopted by the Government / public sector, primarily for policing / security and border control / travel facilitation. The general flow diagram for the biometric process shown in Figure 1. Fingerprint recognition, Face recognition, eye recognition and voice recognition are different areas of biometrics technologies. Fingerprint recognition dominates due to low cost, high speed, high accuracy and dense data characteristics, apart from its use in background checking. Market size for Face recognition was USD 912 million in 2012 and is expected to touch USD 2.15 billion by 2018, primary reasons being adoption in e-Passport gates, and growth in mobile based applications for face recognition. So securing biometric information

is very important today. This is done by applying different cryptography algorithms and Steganography algorithms for avoiding information hacking. Bio-metric technology comes with strongest force of authentication that provides very fast and accurate identification there by protecting from unauthorized access [2, 3]. This technology helps financial organizations to mitigate the risk of unauthorized access through secured and strong employee authentication. It avoids various customer complexities and facilitates tracking & monitoring of employee activities. Considering the necessity to provide add-on security for biometrics, Cryptography and Steganography algorithms are factored-in to fulfill the need.

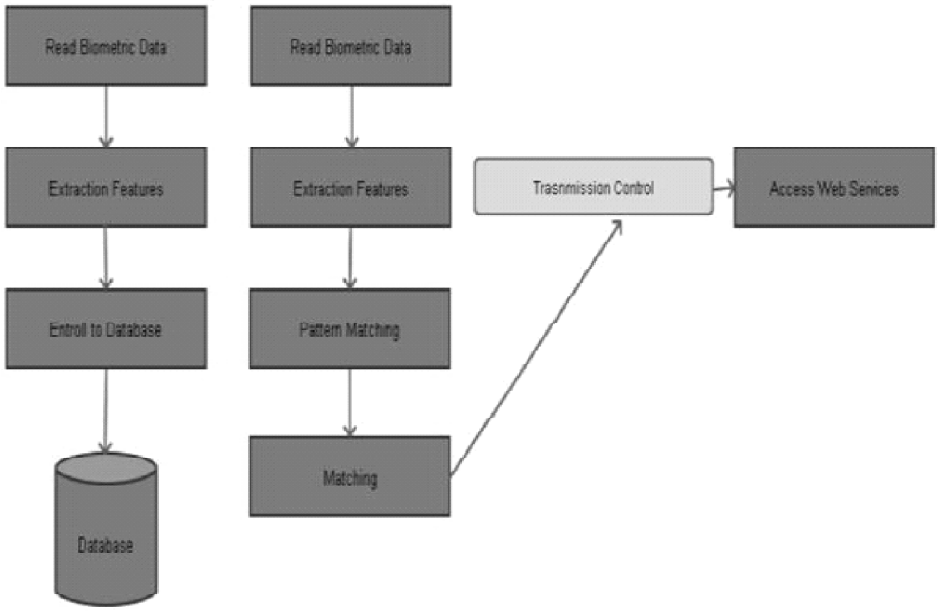

Figure 1: Flow chart for the general biometric process system

Cryptography is the phase where information is modified and made unreadable. Whereas Steganography is the phase where the information is overlaid by dummy and unattractive information (image in this case). The latter hides the main information and will not attract the audience attention. Having their own unique features of securing information, a combination of these two algorithms will add-on the best security layers to avoid unauthorized access of key information.

As a POC and reference, a paper by Faizan Ahmad, Aaima Najam, and Zeeshan Ahmed [1] explains that human face is a dynamic object having high degree of variability in its appearance, and they introduced Image-based Face Detection and Recognition. Renu Bhatia [4] discussed different biometrics techniques such as Iris scan, retina scan and face recognition techniques. G. Nagaraju and T. V. Hyma Lakshmi [5] explained that the procedure to apply scanning techniques for the image and adding key-based carrier image to get better encryption. Dr. P.V. Rama Raju, T. Anvesh Gandhi, G. Naga Raju [10] discussed how to get encryption through zigzag pixel indicator and scan techniques and applying steganography. A paper by Sridevi Thota, Phanindra Sai Srinivas Gudipudi, Bhanu Prakash Panchakarla includes enhanced version of 'Matrix Approach' algorithm, through which huge data can be hid behind an image file, ensuring its safety and security [11]. A paper by Abikoye Oluwakemi C, Adewole Kayode S, Oladipupo Ayotunde J [13] elaborates about a system that has been analyzed for effectiveness and the results convey that the encryption and decryption methods used for developing the security system are more efficient in avoiding unauthorized access. Hence, it is recommended for establishing more secure communication for internet users. The main objectives of this paper are:

1) To show that hiding data and making it invisible is better than just encrypting it and making it visible.

2) To avoid hackers attention by hiding data in a popular object. In case, if the data is decoded from the stego image, it will be encrypted.

To achieve these objectives, 'image' is the right object to apply the proposed algorithms. The reason why only image is considered is because; it can contain enough information to hide, while not appearing to be modified. It is efficient enough to not attract any attention.

2. METHODOLOGY

A general procedure to secure biometric information is shown in Figure 2: To protect this information, adding crypto mechanism is necessary. In unprotected process, it is very easy to hack the biometric information, because there is no special secret key used. In protected procedure, with a secret key there is a perfect protection. This process is shown in Figure 3. Taking the biometric information from the user and storing it on the memory device and retrieving the information from the memory whenever required are common steps in biometric technology. Similarly there is a possibility of hiding data in images just by LSB replacement method. This method with example is shown in Figure 4. Personal Authentication using Biometrics involve person's unique information, such as Face, Hand geometry, Retinal, IRIS, Fingerprint or DNA features which are popular for providing the security in new IT world. One of the multi model biometric security systems is shown in Figure 5. This technology catches the attention of hackers whose primary target is to bypass the biometric security. The hackers breach the biometrics security through biometric scanning technology. The technology used for acquiring biometric information still has many concerns such as physical privacy. The hackers managed to hack various biometric security layers several times by manipulating templates in the Data base, by placing the finger print and Iris images in front of the scanner etc. This emerges the need to add the extra security to biometric systems especially for financial services involved like e-commerce, banking sectors and defense sectors. In pursuit of finding out a remedy, we found out a solution for 'manipulating templates in a database' and partially succeeded to address the second problem which is using biometric images instead of physical biometrics. This procedure is explained with example of enrollment at bank in Figure 6.

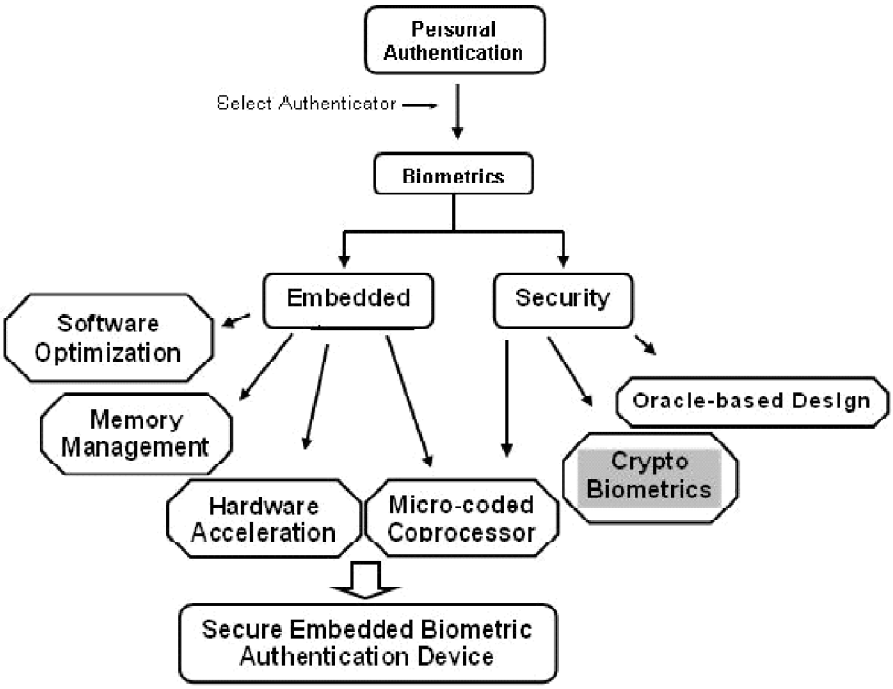

Figure 2: Flow diagram for secure biometric information

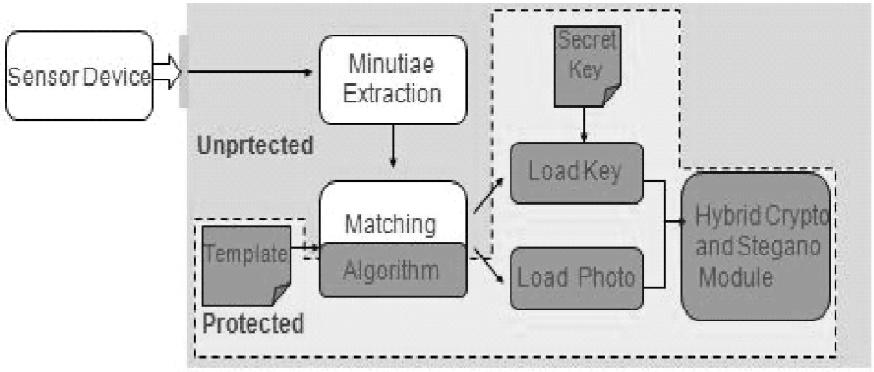

Figure 3: Flow diagram for the data security

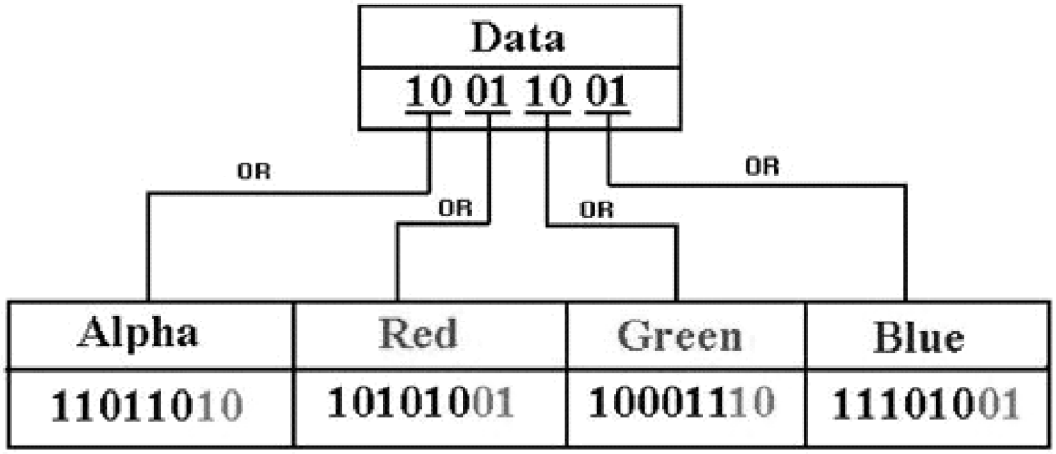

Figure 4: Example of LSB Replacement method

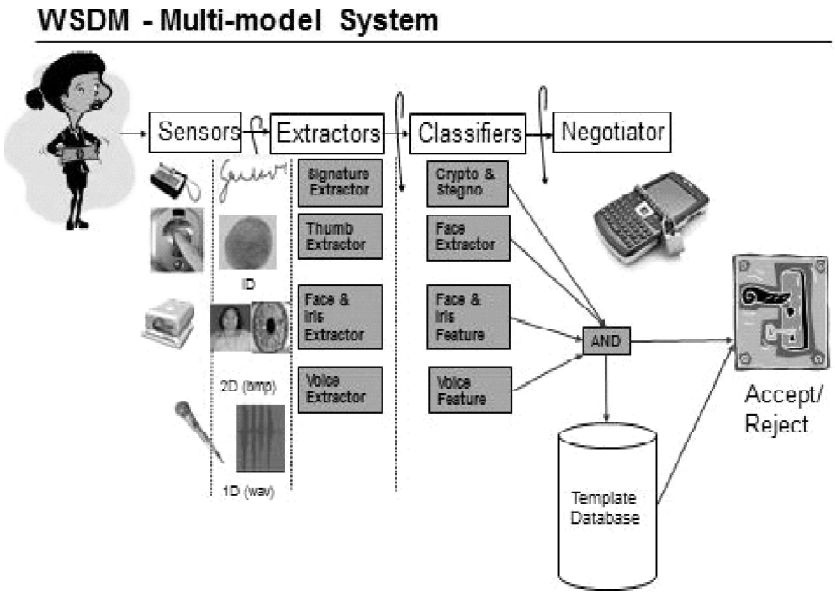

Figure 5: Multimodal biometric system

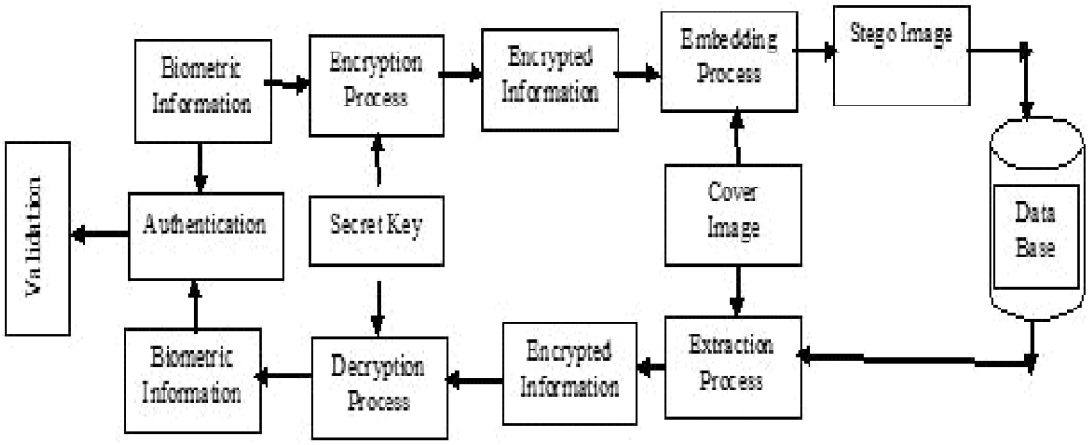

Figure 6: Bank enrollment example for proposed methodology

3. PROPOSED ALGORITHM (DESIGN PROCEDURE)

The proposed system shown in Figure 7 adds additional two layers of security on top of the biometric security. Cryptography and steganography technologies are providing these two layers of security. The application will operate basically in two processes. One is the Registration process and the second one is the Authentication process. The registration is a one-time process which has to be done at the enrollment, whereas the authentication process is required every time the user needs to access the application. The Block diagram shown in Figure 7 includes the combination of Registration and authentication process. The proposed system consists of the following units. Acquisition system, Encryption and Decryption (known as Cryptography), embedding and extracting the image (known as steganography) and template matching for face identification. The system is integrated with front end GUI.

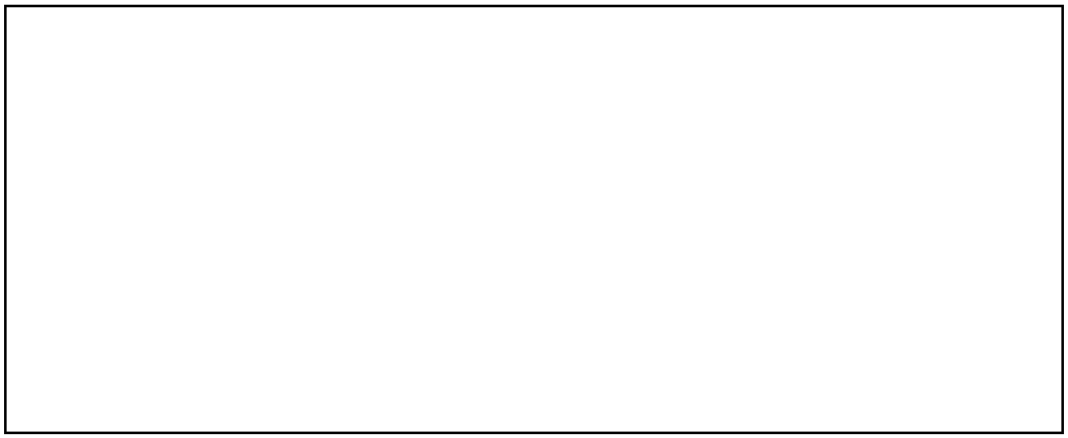

Figure 7: Block diagram of the proposed system

In this proposed algorithm, following steps are implemented.

1. Face Recognition using cognitive services
2. Cryptography: AES Encryption and Decryption using .NET
3. Steganography and De-steganography using Matrix approach with 3D channels in R
4. Application Integration in C# .Net

5. Corresponding User Interface (UI)

Technologies used for the implemented solution so far are:

- Microsoft C# .Net and R.Net
- SQL Data base
- R

4. DESIGN EXAMPLES (RESULTS)

(A) Cryptography

In the present scenario e commerce applications emerged the need of internet banking and electronic bill payments. Such remote operations through wired/ wireless public networks demand data security during transmission and storage. Such type of transactions requires confidentiality to ensure data authentication, accountability, integrity and availability. Cryptography is one proved best method to make sure identification of user and data can be maintained securely, assuring privacy of data. Cryptography is a method of encoding data in an un-readable format that can only be read and processed by the intended authorized users. The popular data encryption algorithms are DES, RSA, Blowfish, Twofish and AES etc [9]. These algorithms are different based on the key cipher text size and mathematical transformations. Among these we use AES Algorithm for our system [7]. With AES algorithm the forming of encrypted image is shown in Figure 8.

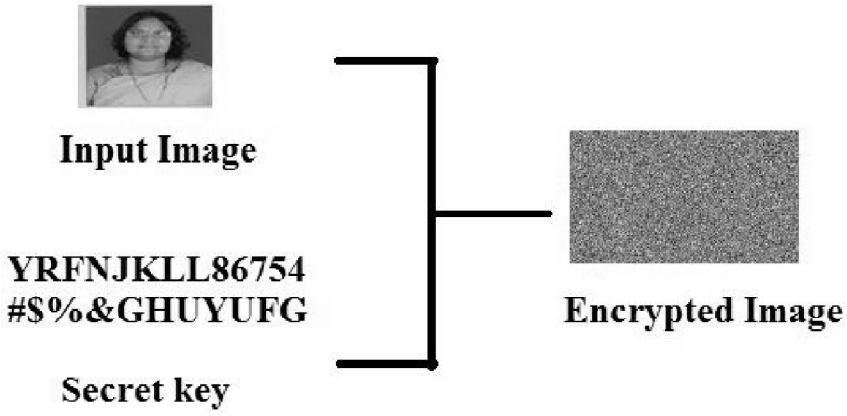

Figure 8: Forming an encrypted image

Advanced Encryption Standard (AES) is a symmetric block cipher technique which is used to protect sensitive information throughout the world in various security applications, where the information is transferred through wired/ wireless means and is stored for further processing. AES uses AES-128, AES-192 and AES-256 block ciphers. Each cipher encrypts and decrypts 128 bits of data using cryptographic keys of 128 bits or 192 bits or 256 bits and decides number of rounds i.e., 10/ 12 and 14 respectively. The basic components of Encryption and decryption process are mathematical, logical, and table lookup operations. This procedure is shown in Figure 9. This encryption process in turn consists of four steps viz., Substitute byte(S-bytes), Shift rows, Mix Column and Add round key, as shown in Figure 10. The process completes all the steps till 'n-1' rounds and leaves mix column step in nth round. Substitution Bytes(S-box) is a lookup table transformation process of a Cipher. It is done by using a nonlinear byte substitution table composed of all combinations of 256 8bit values. Shift rows are a transformation of the Cipher bytes between the columns. This is done by simple permutations of State by circular byte shifting the last three rows of the State by different offsets. Mix Column transforms each byte of a column into a new value which is a function of all four bytes in the column. The combination of shift

rows with mix columns provides the diffusion. In Add Round Key Transformation process is done by XOR operations of state with round key [6]. The state and round key length should be of equal size. In the decryption exactly inverse the process steps i.e. Add round keys, Inverse mix columns, Inverse shift rows, Inverse substitute bytes to get the inverse cipher.

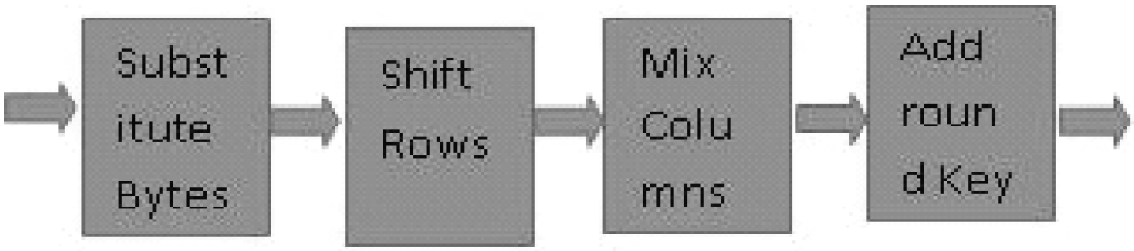

Figure 9: Diagram for AES Key Expansion

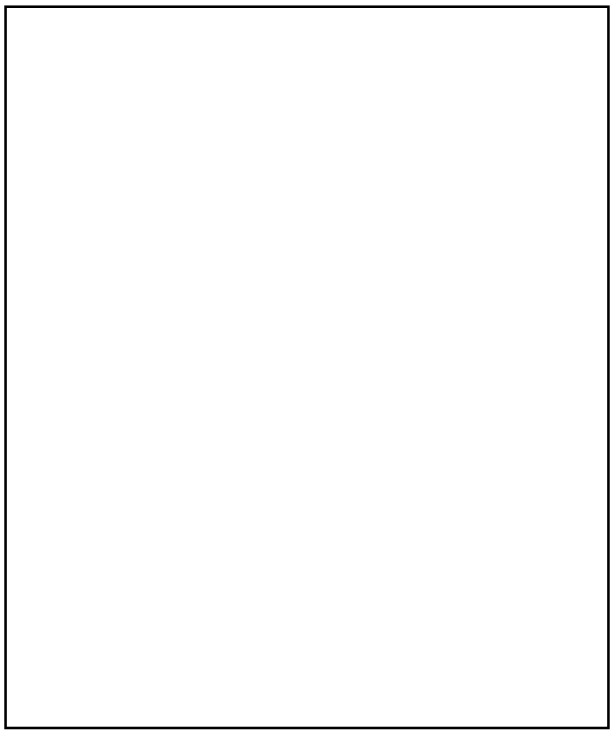

Figure 10: AES Algorithm round steps

(B) Steganography

Image [8] is one of the right tool to hide the information due to their high capacity and low visible impact with general image format viz.GIF (Graphics Interchange Format), BMP (Windows Bitmap), JPEG (Joint Photographic Expert Group) etc., There are several ways to do this, few being Least Significant Bit substitution (LSB), Transform techniques, Masking and filtering. In LSB substitution process, least significant bit of pixel is modified and it becomes extremely powerful tool with fewer limitations. For hiding the information, many popular steganographic tools are developed based on LSB embedding. Few algorithms modify pixels in random, few in particular areas of images, and few, instead of changing last significant bit, the pixel value is incremented or decremented. To form the stego-image we require two files, first one is the image (called cover image) into which the data is to be hidden and second one is the data file which is to be hidden (ex: face image).

Figure 11 shows an example where the cover image is combined with face image to produce the stego-image. This substitution technique will modify the last significant bit of the cover image. Before embedding process, the system must know the size of the cover image file. The standard size of this image is 800*600 pixels, which can embed up to 60kb size of message. In LSB technique, the least significant bits of each cover image pixel is replaced by face image pixels, which are permuted before embedding. This allows distribution of bits evenly, thus averaging 25 pixels of cover image for 2 pixels of face image. Our optimized algorithm will modify the least four significant bits of the cover image. For embedding face image into cover image, the cover image should be greater than or equal to 12.5 times of the face image. So we use the face image size of 60 x 80 x 3 (14KB) and cover image size of 750 x 1000 x 3(2197KB).

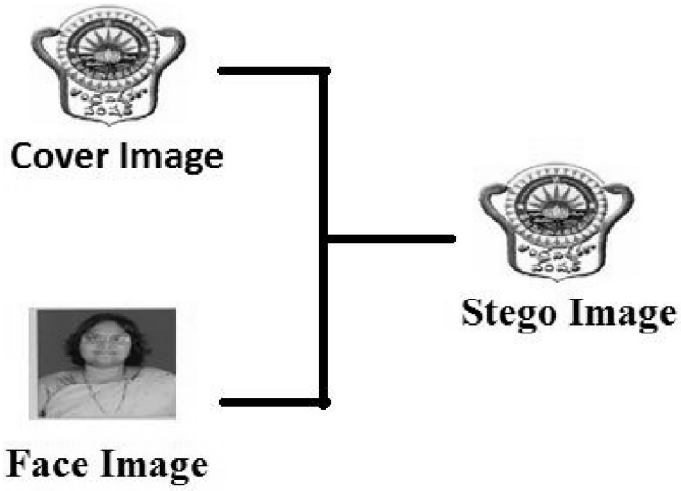

Figure 11: Forming a stego-image

(C) Face Detection and Recognition –Cognitive web services

Microsoft Cognitive web Services help us building the rapid proto type apps with powerful algorithms for POC's without much minimal efforts of programming. The web services can work with devices and platforms such as iOS, Android, and Windows, keep improving, and are easy to set up. The Microsoft Face API is a cloud-based service that provides the most advanced face algorithms. Face API has two main functions: face detection with attributes and face recognition. Face API detects up to 64 human faces with high precision face location in an image. And the image can be specified by file in bytes or valid URL. Face rectangle (left, top, width and height) indicating the face location in the image is returned along with each detected face. Optionally, face detection extracts a series of face related attributes such as pose, gender, age, head pose, facial hair and glasses. It provides four face recognition functions such as face verification, finding similar faces, face grouping, and person identification. Face API verification performs an authentication against two detected faces or authentication from one detected face to one person object. We integrated this cognitive web service with our integrated C#.net platform along with the cryptography and steganography modules.

(D) Performance Metrics

To rate the performance of a biometric system, False Acceptance Rate (FAR) and False Rejection Rate (FRR) are used. FAR is considered serious issue than FRR because, authorizing an un-authorized personnel is critical than un-authorizing an authorized personnel. FAR of the system with the proposed combination of two biometric techniques (Cryptography and Steganography) can undoubtedly be lesser (much closer to zero) than that of FAR of a system functioning with only Cryptography or only Steganography. A simple test verified that FAR of the

proposed system is close to zero. The test is as follows. Some random stego-encrypted images are considered. For example, say img1 belongs to Mr. A. If 'A' uses the proposed system, he is authorized. Now, the actual image file of 'A' that was used for developing stego-encrypted image of 'A' is taken and 2 bits in 2 pixels of that image are changed. This change is equivalent to the image of a different person but with most of the similar features expect those 2 pixels. Now the newly formed image is used with the system to see if the system can authorize the person. The system ended in not authorizing the newly formed image of 'A'. The same test has been conducted on the remaining images as well and the results hold good for all those images as well.

5. APPLICATION CONCLUSION AND FUTURE SCOPE

The application is helpful to all security wings from the financial sector to Military security. The proposed security layers can be used for any biometric modality. We can enhance the features of the proposed techniques for the bimodal biometric authentication systems. The algorithms can be incorporated into the future upcoming technologies like Robotics as well.

REFERENCES

[1] Faizan Ahmad, Aaima Najam, and Zeeshan Ahmed, "Image-based Face Detection and Recognition: State of the Art", International Journal of Computer Science Issues, Vol. 9, Issue 6, No 1, November 2012, ISSN (Online): 1694-0814.

[2] Donny Jacob Ohana, Liza Phillips, Lei Chen, "Preventing Cell Phone Intrusion and Theft using Biometrics Fingerprint Biometric Security utilizing Dongle and Solid State Relay Technology", 2013 IEEE Security and Privacy Workshops.

[3] Smita S. Mudholkar , Pradnya M. Shende, Milind V. Sarode,"Biometrics Authentication Technique For Intrusion Detection Systems Using Fingerprint Recognition", International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.2, No.1, February 2012.

[4] Renu Bhatia, "Biometrics and Face Recognition Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013 ISSN: 2277 128X.

[5] G. Nagaraju and T. V. Hyma Lakshmi, "Image encryption using secret-key images and SCAN patterns", International Journal in Advances in Computer, Electrical,& Electronics Engg., Vol. 02, 2012, pp. 13-18.

[6] Reza Moradi Rad, Abdolrahman Attar, and Reza Ebrahimi Atani, "A New Fast and Simple Image Encryption Algorithm Using Scan Patterns and XOR", International Journal of Signal Processing, Image Processing and Pattern Recognition Vol.6, No. 5(2013), PP: 275-290. http://dx.doi.org/10.14257/ijsip.2013.6.5.25.

[7] Ramaraju PV, Nagaraju G, Chaitanya RK, "Image Encryption and Decryption using Advanced Encryption Algorithm", Discovery, 2015, The International Daily journal, ISSN 2278 – 5469 EISSN 2278 – 5450, 29(107), PP: 21-28.

[8] K. Sakthidasan@Sankaran and B. V. Santhosh Krishna, "A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images", International Journal of Information and Education Technology, Vol. 1, No. 2, June 2011.

[9] Rinki Pakshwar, Vijay Kumar Trivedi, Vineet Richhariya ,"A Survey On Different Image Encryption and Decryption Techniques", Rinki Pakshwar et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (1) , 2013, 113 – 116,ISSN:0975-9646.

[10] Dr. P.V.Rama Raju, T. Anvesh Gandhi, G. Naga Raju, "RGB Image Steganography using Zigzag Pixel Indicator and Scan Techniques", International Journal Of Research In Electronics And Computer Engineering., Vol. 3 Issue 3, July-Sept. 2015, ISSN: 2393-9028 (print) | ISSN: 2348-2281 (online) Pp103-Pp107.

[11] Mrs. Sridevi Thota, Phanindra Sai Srinivas Gudipudi, Bhanu Prakash Panchakarla, "An Enhanced Data Hiding Technique of Steganography Using Matrix Approach Method", International journal of Systems and Technologies ISSN 0974 – 2107.

[12] Saleh Saraireh, "Secure Data Communication System Using Cryptography And Steganography", International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.3, May 2013.

[13] Abikoye Oluwakemi C, Adewole Kayode S., Oladipupo Ayotunde J., "Efficient Data Hiding System using Cryptography and Steganography", International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 4– No.11, December 2012 – *www.ijais.org*