Wireless sensor data mining for e-commerce applications

T. Sridevi[1], P. Mallikarjuna Rao[2], P. V Ramaraju[3]
[1,2]Department of Electronics & Communication Engineering, Andhra University College of Engineering (A), Visakhapatnam, Andhra Pradesh, India
[3]Department of Electronics & Communication Engineering, SRKR Engineering College, Bhimavaram, Andhra Pradesh, India

Article Info

Article history:

Received Jun 24, 2018
Revised Oct 15, 2018
Accepted Jan 7, 2018

Keywords:

Biometric applications
Cryptography
E-commerce
Security
Steganography

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.

Corresponding Author:

T. Sridevi,
Department of Electronics and Communication Engineering,
Andhra University College of Engineering (A),
Visakhapatnam, Andhra Pradesh, India.
Email: sridevi.dsp@gmail.com

1. INTRODUCTION

To date, biometric technologies [1] have been most widely adopted by the Government/public sector, primarily for policing/security and border control/travel facilitation. Fingerprint recognition [2], Face recognition, eye recognition and voice recognition are different areas of biometrics technologies. Finger print 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. Biometric information is very important and Facing Problem of security in todays. This is done by applying different cryptography algorithms and Stegaanography algorithms [2], [3] for avoiding information hacking.

1.1. Benefits of Using Biometrics in Banking

The benefits are,

a. Biometric technology provides the strongest method of authentication that protects banking information from being compromised by unauthorized personnel.

b. Biometric technology provides fast and accurate identification for the banking industry. Customers can be quickly authenticated in seconds through a fast biometric scan.
c. A biometric voice recognition system [4] for example provides a secure and flexible solution to verify any customer executing communication outside of a brick and mortar environment.

These days, it is necessary to apply cryptography algorithms and Steganography algorithms [5] for better security. In cryptography, the message is scrambled and unreadable. However, when the communication happens, it can be noticed that the information is encrypted. Although the information is hidden in the cipher, an interception of the message can be damaging, as it still shows that there is communication between the sender and receiver. In contrast, steganography takes a different approach in hiding the evidence. In Steganography, one information is hidden in other information, that's way it is highly impossible to notice that the information visible on the communication line contains invisible hidden information. Compared to cryptography, steganography has its advantage because the message itself will not attract the audience, as the very nature of a steganography system is to hide the message in an unnoticeable manner. By combining these Cryptography (For Encryption & Decryption) [6], [7] and Steganography (For Data hiding in a multimedia object) security techniques information can be secured more effectively.

As a POC and reference, a paper by Faizan Ahmad, Aaima Najam, and Zeeshan Ahmed 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 [8]. Renu Bhatia discussed different biometrics techniques such as Iris scan, retina scan and face recognition techniques [9]. G. Nagaraju and T. V. Hyma Lakshmi explained the procedure to apply scanning techniques for the image and adding key-based carrier image to get better encryptio. Dr. P.V.Rama Raju, T. Anvesh Gandhi, G. Naga Raju 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 explains an enhanced matrix approach algorithm through which large amount of data can be hidden inside an image file. This algorithm ensures the security and safety of hidden data. Thus the algorithm can be extended to the fields of Defense, Internet and other applications where data security is of primary concern. A paper by Abikoye Oluwakemi C, Adewole Kayode S, Oladipupo Ayotunde J discusses a system that was evaluated for effectiveness and the result shows that, the encryption and decryption methods used for developing the system make the security of the proposed system more efficient in securing data from unauthorized access. The system is, recommended to be used by the Internet users for establishing a more secure communication. In [10] explained integration of Adaptive Weight Ranking Policy (AWRP) with intelligent classifiers (NB-AWRP-DA and J48-AWRP-DA) via dynamic aging factor to improve classifiers power of prediction. The methods are used to choose the best subset of features. The confidential awareness based on cryptoanalysis for two factor authentication process is presented in [11]. The comparison of various crypto analyses procedures are discussed. In [12], there are three categories of cryptographic algorithms. They are as follows: Hash algorithms, in which hashing functions are used to map data of random or predefined sizes. To further improve the security this algorithm is implemented.

1.2. Objectives

The main objectives of this paper are:

a. To show that hiding data and making it invisible is better than just encrypting it and making it visible.
b. To hide data in a popular object that will not attract any attention. In case the data is extracted, 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 draw any attention.

2. PROPOSED METHODOLOGY

A general procedure to secure biometric information is shown in Figure 1. Taking the biometric information [13] 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. 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 [14]. In protected procedure, with a secret key there is a perfect protection. This is shown in Figure 2.

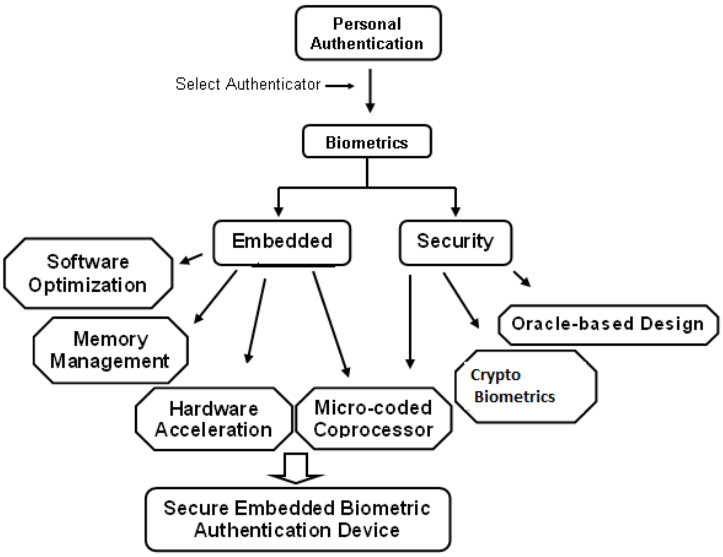

Figure 1. Flow diagram for secure biometric information

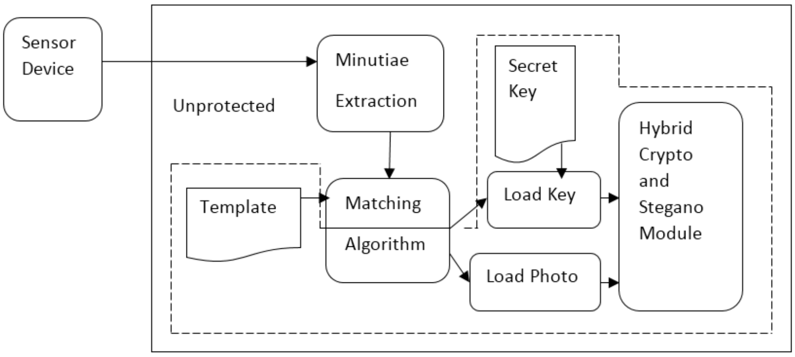

Figure 2. Protecting algorithm flow diagram for the data security

Similarly there is a possibility of hiding data in images just by LSB replacement method. This method with example is shown in Figure 3.

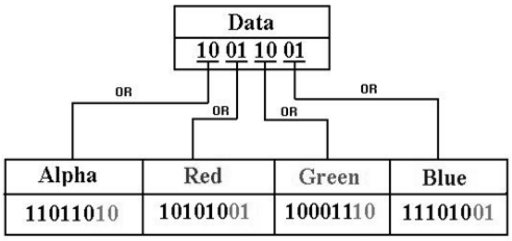

Figure 3. Example of LSB replacement method

2.1. Biometric Security Systems

This system involves person's unique identification (ID), such as Face, Hand geometry, Retinal, IRIS, Fingerprint or DNA, it is becoming popular for providing the security in new IT world. One of the multi model biometric security systems is shown as in Figure 4.

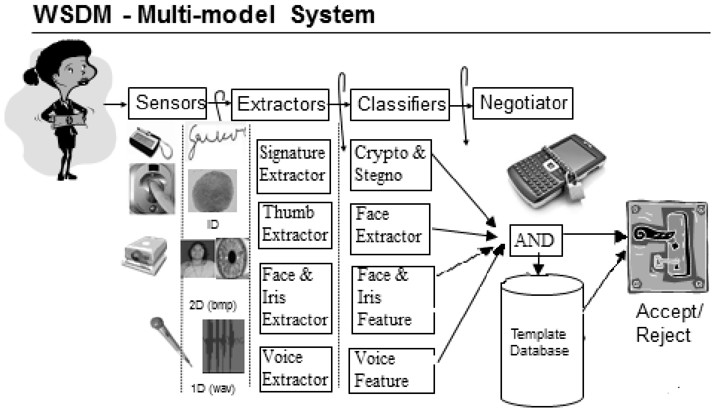

Figure 4. Multimodal biometric system

This technology catches the attention of hackers whose primary target is to bypass the biometric security. The hackers break the biometrics security through biometric scanning technology. The biometric scanning technology still has many concerns such as information and physical privacy. The hackers managed to hack various biometric security layers [15] several times by manipulating templates in the Data base, which is collected from a person of his finger print and Iris images by using a 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 5.

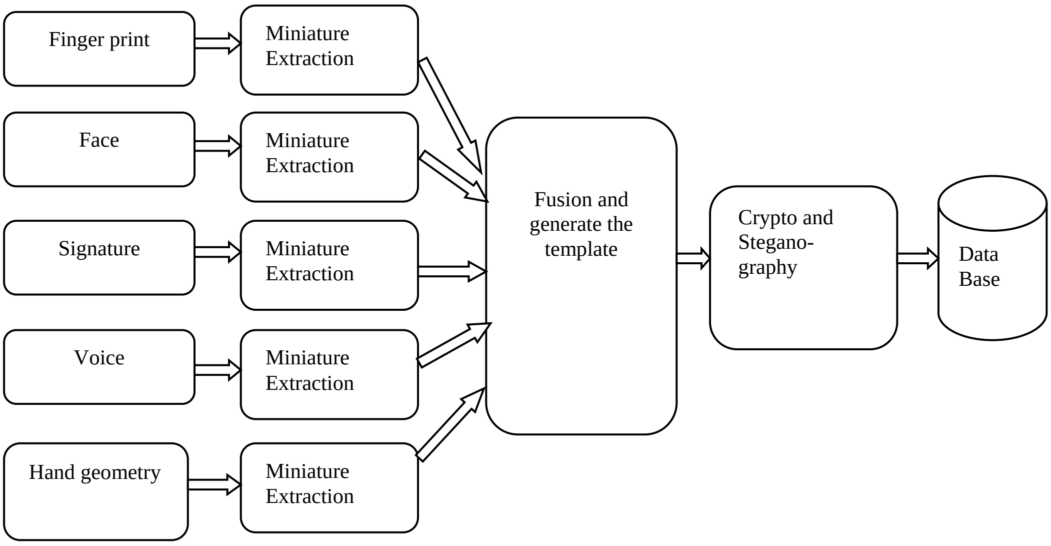

Figure 5. Bank enrollment example for proposed methodology

2.2. Proposed Algorithm (Design Procedure)

The proposed system shown in Figure 6, adds two layers of security on top of the biometric security. Cryptography and steganography technologies are providing the two layers of security. The application will operate basically in two processes.

Registration Process: The registration is a one-time process which has to be done at the enrollment.

Authentication Process: the authentication process is required every time the user needs to access the application.

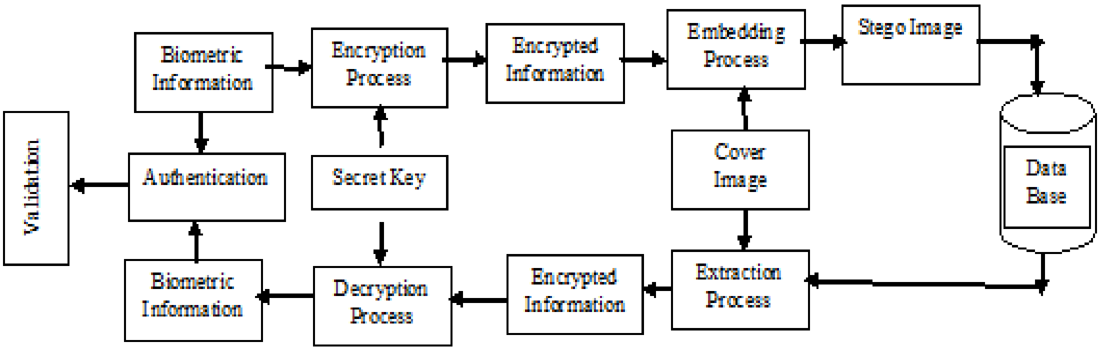

Figure 6. Block diagram of the proposed system

The Block diagram shown in Figure 6 includes the combination of Registration and Authentication process. The proposed system consists of the following units. The Acquisition system, the Encryption and the Decryption (are known as Cryptography), embedding and the extracting the image (are known as steganography) [16], [17] and template matching for face identification. The system is integrated with front end GUI.

In this proposed algorithm, following steps are implemented.

a. Face Recognition using cognitive services
b. Cryptography: AES Encryption and Decryption using .NET
c. Steganography and De-steganography using R Coding.
d. Application Integration
e. Corresponding User Interface

Technologies used for the implemented so far are mentioned below

a. Microsoft C# .Net
b. SQL Data base
c. R.Net
d. Cryptography AES- Rijindal
e. Steganography-Matrix approach with 3D channels

3. RESULTS & DISCUSSIONS

3.1. Cryptography

In the present scenariomost of the people are adapting online shopping and stock trading. That's why most of the applications based on internet are emerged as e-commerce applications. Because of this emerging online market trading, the money transactions are also tacking place through internet banking and electronic bill payment etc. Such transactions, over wire or wireless public networks demand end-to-end secure connections, should be confidential, to ensure data authentication, accountability confidentiality, integrity and availability. All above mentioned are going to be provided by a process called as Cryptography. Cryptography is a method of storing and transmitting data in an encoded format (un readable form) that only read and process by the intended users. The popular data encryption algorithms are DES, Triple DES, RSA, AES, ECC, BLOWFISH, TWOFISH, THREEFISH, RC5 and IDEA etc. These algorithms are differ based on the key, cipher text size and mathematical transformations. Among these we use AES Algorithm for our system because of its novelty as explained as below.

AES (Advanced Encryption Standard): The Advanced Encryption Standard is a replacement to DES and 3DES. AES is a symmetric block cipher used to protect sensitive data information throughout the world in various security applications where the information is transferred through wire, as well as wireless. It also stores the information for further processing.

AES is actually, three block ciphers, AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128 bits, 192 bits and 256 bits, respectively. According to the key length such as 128bits, 192 bits and 256 bits the respective rounds are of 10, 12, 14.

The basic components of Rijndel Encryption and decryption process which is used here is a simple mathematical, logical, and table lookup operations. It is based on AES Key Expansion in which the encryption process is a bit wise exclusive OR operation of a set of image pixels along with a key which changes for every set of pixels in every round as shown in Figure 7.

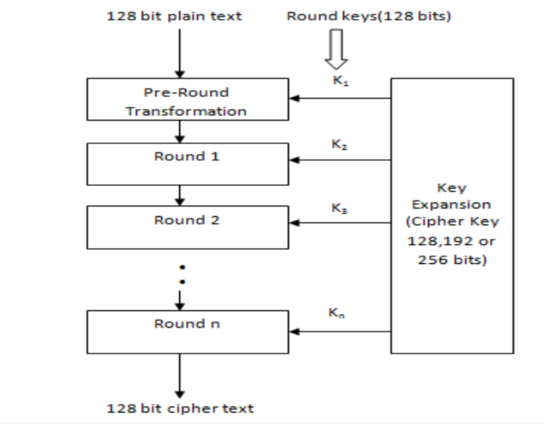

Figure 7. A bit wise exclusive OR operation

In each case, all other rounds are identical, except for the last round. Each round in encryption process further follows some steps to complete each round till n. Each round in encryption possess four steps i.e. Substitute byte, Shift rows, Mix Column and Add round key as follows in Figure 8.

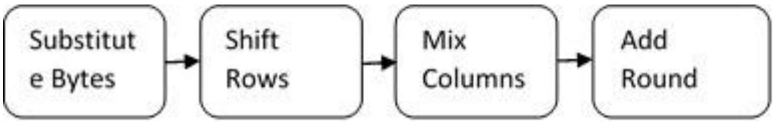

Figure 8. AES algorithm round steps

Substitution Bytes is a transformation in the Cipher that processes the State using a nonlinear byte substitution table (S-box) that operates on each of the State bytes independently. Shift rows are a transformation in the Cipher that processes the State by cyclically shifting the last three rows of the State by different offsets. Mix columns is a transformation in the Cipher that takes all of the columns of the State and mixes their data (independently of one another) to produce new columns.

Adding Round Key is a Transformation in the Cipher and Inverse Cipher in which a Round Key is added to the State using an XOR operation. The length of a Round Key equals the size of the State. In the decryption exactly inverse the process steps I.e Add round keys, Inverse mix columns, Inverse shift rows, inverse substitute bytes are used for getting the inverse cipher. Then the result will be as shown in Figure 9.

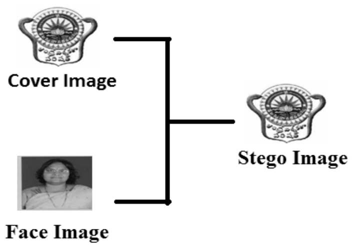

Figure 9. Result of Cryptography

3.2. Steganography

Images are one of the preferred media to hide the information due to their high capacity and low impact on the visibility. We can use the common image format like GIF (Graphics Interchange Format), BMP (Windows Bitmap), JPEG (Joint Photographic Expert Group) etc. There are many approaches to hide the images like Least Significant Bit substitution (LSB), Transform techniques, Masking and filtering. We use bmp color images with LSB technique. LSB (Least Significant Bit) Substitution is the process of modifying the least significant bit of the pixels of the cover media. LSB Substitution lends itself to become a very powerful Steganography method with few limitations. Popular steganographic tools based on LSB embedding vary in their approach for hiding information. Some algorithms change LSB of pixels visited in a random walk, others modify pixels in certain areas of images, or instead of just changing the last bit they increment or decrement the pixel value.

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 8 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 the LSB technique, the LSB of the pixels is replaced by the face image pixels. The face image pixel bits are permuted before embedding, this has the effect of distributing the bits evenly, thus on an average 25 pixels of cover image contains two pixels of face image. Our optimized algorithm will modify the least four significant bits of the cover image. For embedding the face image into the 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). Results of Steganography are shown in Figure 10.

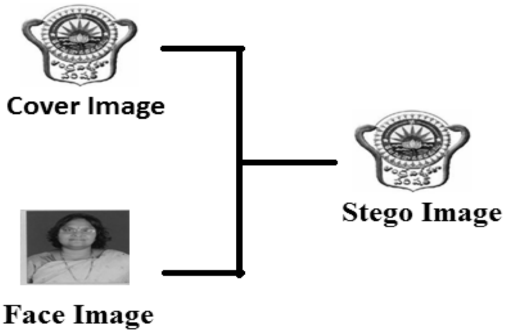

Figure 10. Results of Steganography**:**

3.3. Face Detection and Recognition – Cognitive Web Services

Microsoft Cognitive Services let you build apps with powerful algorithms using just a few lines of code. They work across devices and platforms such as iOS, Android, and Windows, keep improving, and are easy to set up. The Microsoft Face API, 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.

3.4. Performance Metrics

False Acceptance Rate (FAR) and False Rejection Rate (FRR) are the 2 standard metrics used to rate the performance of a biometric system. 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.

3.5. Application

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.

4. CONCLUSION

The proposed security layers can be used for any biometric modality for any type of information such as text, image, and audio / video files. The application is helpful to all security wings from the financial sector to Military security.The system 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, A., Aaima, N., and Zeeshan, A., “Image-based Face Detection and Recognition: State of the Art”, *International Journal of Computer Science Issues,* vol. 9, Issue 6, no 1, November 2012,

[2] Donny, J. O., Liza, P., and Lei, C.,”Preventing Cell Phone Intrusion and Theft using Biometrics Fingerprint Biometric Security utilizing Dongle and Solid State Relay Technology”, *IEEE Security and Privacy Workshops,* 2013.

[3] Smita S. M., Pradnya, M., and Shende, M. V. S., “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] Nagaraju, G., and Hyma Lakshmi, T. V., “Image encryption using secret-key images and SCAN patterns”, *International Journal in Advances in Computer, Electrical,& Electronics Engg.,* vol. 02, pp. 13-18, 2012.

[5] Renu B., “Biometrics and Face Recognition Techniques”, *International Journal of Advanced Research in Computer Science and Software Engineering,* vol. 3, Issue 5, May 2013.

[6] Reza, M. R., Abdolrahman, A., and Reza, E. A., “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, PP:275-290. 2013.

[7] Ramaraju, P. V., Nagaraju, G., and Chaitanya, R. K., “Image Encryption and Decryption using Advanced Encryption Algorithm”, Discovery, 2015, *The International Daily journal,* vol. 29, no. 107, Pp:2-28, 2015.

[8] Sakthidasan, K. S., and Santhosh, Krishna, B. V., “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, P., Vijay, K. T., and Vineet, R., “A Survey On Different Image Encryption and Decryption Techniques”, *(IJCSIT) International Journal of Computer Science and Information Technologies,* vol. 4, no. 1, pp. 113 – 116, 2013.

[10] Dr. Rama Raju, P.V., Anvesh Gandhi, T., and Naga Raju, G., “RGB Image Steganography using Zigzag Pixel Indicator and Scan Techniques“ *International Journal Of Research In Electronics And Computer Engineering.,* vol. 3, Issue 3, pp. 103- 107, 2015.

[11] Mrs. Sridevi, T., Phanindra, S. S., Gudipudi, B., and Panchakarla, P., “An Enhanced Data Hiding Technique of Steganography Using Matrix Approach Method”, *International journal of Systems and Technologies*.

[12] Saleh, S., “Secure Data Communication System Using Cryptography And Steganography”, *International Journal of Computer Networks & Communications (IJCNC),* vol.5, no.3, May 2013.

[13] Abikoye, O. C., Adewole, K. S., and Oladipupo, A. J., ”Efficient Data Hiding System using Cryptography and Steganography”, *International Journal of Applied Information Systems (IJAIS),* vol. 4, no.11, 2012.

[14] Olanrewaju, R. F., and Azman, A. W., “Intelligent Cooperative Adaptive Weight Ranking Policy via dynamic aging based on NB and J48 classifiers”, *Indonesian Journal of Electrical Engineering and Informatics (IJEEI),*vol. 5, no.4, 357-365, 2017.

[15] Choi, Y., "Cryptanalysis on Privacy-aware two-factor Authentication Protocol for Wireless Sensor Networks", *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 8, no. 2, pp. 296-301, 2017.

[16] Singh, P., and Chauhan, R. K., "A Survey on Comparisons of Cryptographic Algorithms Using Certain Parameters in WSN." *International Journal of Electrical and Computer Engineering,* vol. 7, no. 4, pp. 2232, 2017.

[17] Saxena, S., “Extension to HiRLoc Algorithm for Localization Error Computation in Wireless Sensor Networks”, *Indonesian Journal of Electrical Engineering and Informatics*, vol. 1, no. 4, pp. 119-126, 2013.