ISSN: 2395-7852

International Journal of Advanced Research in Arts, Science, Engineering & Management

Volume 10, Issue 3, May 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 6.551

+91 9940572462 +91 9940572462 ijarasem@gmail.com www.ijarasem.com

International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 6.551 |Bimonthly, Peer Reviewed & Referred Journal|

| Volume 10, Issue 3, May 2023 |

Utilizing Visual Cryptography for Secure Biometric Authentication in Healthcare sector

Dr. J. Alphas Jeba Singh[1] , M. Parvathi Priya[2] , C. Petchikani[3] , R. Santhiya[4] , M. Selvamathi[5]

Associate Professor, ECE Department, Thamirabharani Engineering College, Thatchanallur, Tirunelveli, India[1]

UG Student, ECE Department, Thamirabharani Engineering College, Thatchanallur, Tirunelveli, India[2,3,4,5]

ABSTRACT: A growth in the usage of biometric authentication has become quite popular and is being utilised widely in many applications. A technique for identifying an individual's behavioral or physical traits is the use of biometric authentication. This project is a suggestion for employing visual cryptography to provide safe biometric authentication in healthcare systems. The system will use biometric authentication using facial recognition that is used to capture the image and store it using secured symmetric encryption technique. In this study, color visual cryptography for biometric applications is implemented. To further enhance security, initial encryption processes based on pseudo random sequence generators and shares concealment processes based on least significant bits (LSB) are also used. In order to increase security, this paper provides a security system that combines cryptography and stegnography. The project modules are authenticated strongly.

I.INTRODUCTION

Biometric authentication is considered as the science of verifying the identity of an individual based on their appearance such as face, iris, voice, or fingerprints. Visual Cryptography for Biometric authentication system operates by developing data from Face images which is going to be the main subject, to obtain the data and compare the data stored in the database in order to identify or verify the identity of a person or patient.

Talking about Visual cryptography, it was originated in the year 1994 and was designed for secure image transfer, handwritten documents, text images, maps, or financial doc uments. The way encrypts a secret image for example encrypting patients' image into binary image such that assembling a necessary number of binary images would reveal the secret image. In the case of facial recognition there is a private face image that is dithered into two host images that are stored in two different databases. Binary image could also be referred as shares. The decryption of the secret image is simply done by overlaying each person's shares to get back to the original image. The overlaying is only done when both the shares are available simultaneously.

II.LITERATURE REVIEW

A critical assessment of the work has been done so far on secure biometric authentication to show how the current study related to what has already been done. There have been a lot of continuous survey[8] on providing security based authentication There have been lots of works before in this and variety of methods to provide security using IoT[6]and Cloud with PPG[7], ECG and fingerprint[10] yet there is a huge room for improvement that needs to be carried forward into the research to provide security.

Farhad Ahamed, Farnaz Farid, Basem Suleiman, Zohaib Jan, Luay A. Wahsheh and Seyed Shahrestani proposed a An Intelligent Multimodal Biometric Authentication Model for Personalised Healthcare Services [1].

Relevance to current Research

In this paper, the authors proposed an AI-based multimodal biometric authentication model for single and group-based users' device-level authentication that increases protection against the traditional single modal approach. The models are tested using physiological biometric features such as ECG and PPG signals from five public datasets available in Physionet and Mendeley data repositories. The multimodal fusion authentication model shows promising results with 99.8% accuracy. They showed the feasibility of multimodal single and group-based authentication mechanisms in network. They

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 6.551 |Bimonthly, Peer Reviewed & Referred Journal|

| Volume 10, Issue 3, May 2023 |

used both time domain and joint time-frequency domain feature extraction methods to extract useful features from ECG, PPG and fused ECG-PPG signals. Then they tested the performance of each type of signal with different classifications as well as deep learning algorithms with fused data to enhance the performance of the model.

Yuwen Huang, Gongping Yang, Kuikui Wang, Yilong Yin proposed a Multi-view discriminant analysis with sample diversity for ECG biometric recognition [2].

Relevance to current Research

The authors proposed a multi-view discriminant analysis approach in the consideration of sample diversity for ECG biometric recognition. Firstly, they proposed a method of generating multiple views by using single lead ECG signal and presented a multi-views learning framework, which takes sample diversity to generate a more discriminative subspace then to obtain robust solution, they introduced a denoising constraint to learn the relationships between different views, to create a stable representation against ECG noise. Finally the experimental results demonstrated the proposed method can achieve competitive performance compared to state-of-the-art ECG biometric recognition methods.

Lucas Bastos, Thais Tavares, Denis Rosario, Eduardo Cerqueira, Aldri Santos, and Michele Nogueira proposed a Double Authentication Model based on PPG and ECG Signals [3].

Relevance to current Research

The authors introduced a model for double authentication based on PPG and ECG signals for promoting another layer of security to the user, ensuring data security, and avoid weak dependence on a single biosignal for validation. They proposed model has a algorithm with two zones, namely the Algorithm for PPG and ECG Signals and Error Rate zones. The experimental results indicated that the proposed model presented up to 99.98% of accuracy. The work presented a model of user authentication on wearable devices. The model consists of an algorithm and a mathematical equation to calculate the authentication error rate using the features of the ECG and PPG signals collected from 53 individuals in a non-intrusive way and a controlled location. These signals are stored in a public dataset and served as reference data for the calculation. The accuracy for the PPG signal was 99.98%, and for the ECG signal was equal to 88.79%. For all users, we acquired all true positives, proportionally few false positives, and no false negatives, due to the quality of the vital signs used. Our results indicate the feasibility of using PPG and ECG signals as biometric authenticators.

C.L.P. Lim, W.L. Woo, S.S. Dlay and Bin Gao proposed a Heartrate-Dependent Heartwave Biometric Identification with Thresholding-Based GMM- HMM Methodology [4].

Relevance to current Research

The authors presented an adaptive heartrate dependent heartwave signal based biometric identification. A reliable and continuous heartwave extraction method featuring hybridized Discrete Waveform Transform method with heartrate adaptive QT and PR interval to perform comprehensive heartwave features extractions on more than 35,000 heartwave signal. The size of training data was determined and hybridized GMM-HMM classification method was used in the classification. the results have shown the feasibility of using heartwave signal as biometric mode with varying heartrate. The work has demonstrated that at varying heartrate, the heartwave signal exhibited unique characteristic features that can be used to discriminate individual.

Kalsoom Fatima, Sumbal Nawaz, Sobia Mehrban proposed a Biometric Authentication in Health Care Sector: A Survey [5].

Relevance to current Research

In this survey, the authors reviewed different 5 physical and behavioral biometric techniques that described in a different research paper in past decades; then they analyze findings and future direction of different papers separately based on physical and behavioral biometric methods. They provide a comparative analysis of all biometric techniques it will help out readers to get a better idea about different biometric technologies that which one will suit according to their needs and budget. They conclude that for identification, authentication, in healthcare sector there is a need of proper implementation

of any of these biometric authentication techniques or the combination of different techniques properly, to provide advanced security and prevention from any security threats to patient records.

No.	Paper Title	Author Name	Key Points	Remark
1	An Intelligent Multimodal Biometric Authentication Model for Personalised Healthcare Services	Farhad Ahamed, Farnaz Farid, Basem Suleiman, Zohaib Jan, Luay A. Wahsheh and Seyed Shahrestani, 2022	The paper proposes an AI-based multimodal biometric authentication model for single and group-based users' device-level authentication that increases protection against the traditional single modal approach [1]	Shows the feasibility of multimodal single and group-based authentication mechanisms in security network.
2	Multi-view discriminant analysis with sample diversity for ECG biometric recognition	Yuwen Huang, Gongping Yang, Kuikui Wang, Yilong Yin, 2021	The papers propose a method of generating multiple views by using single lead ECG signal. Then present a multi-views learning framework, which takes same diversity into account to generate a more discriminative subspace. [2].	The method can achieve competitive performance compared to state-of-the-art ECG biometric recognition methods.
3	Double Authentication Model based on PPG and ECG Signals	Lucas Bastos, Thais Tavares, Denis Rosario, Eduardo Cerqueira, Aldri Santos, and Michele Nogueira, 2020	A model for double authentication based on PPG and ECG signals for promoting another layer of security to the user was introduced. [3]	indicates the feasibility of using PPG and ECG signals as biometric authenticators.
4	Heartrate-Dependent Heartwave Biometric Identification with Thresholding-Based GMM-HMM Methodology	C.L.P. Lim, W.L. Woo, S.S. Dlay and Bin Gao , 2018	The papers presents the use of individual heartwave signal as a biometric mode and have ascertained that heartwave signal indeed has the characteristics to be used as a biometric mode [4].	The heartwave signal exhibited unique characteristic features that can be used to discriminate individual.
5	Biometric Authentication in Health Care Sector: A Survey	Kalsoom Fatima, Sumbal Nawaz, Sobia Mehrban, 2019	The paper presents different physical and behavioral biometric techniques and concluded that for identification in healthcare sector needs a proper implementation of biometric techniques to provide advanced security. [5].	To provide advanced security and prevention from any security threats to patient records proper implementation is needed.

In summary, the work presented in this paper is built on previous research to provide secure biometric authentication in health care sector.

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 6.551 |Bimonthly, Peer Reviewed & Referred Journal|

| Volume 10, Issue 3, May 2023 |

III.METHODOLOGY OF PROPOSED SURVEY

For this work visual cryptography will be used to store patient's data using their images, for instance when in hospital a new patients record gets created, it is saved by their name and their image to recognize them easily. So, to secure that information, patient's image can be saved by encrypting shares of the image and when in need can decrypt the data. Image will be captured using biometric authentication.

MODULES:

1. Enrollment Process
2. Authentication Process

MODULE DESCRIPTION:

1. Enrollment Process:

- In enrollment process, first private face image was acquired.
- Next, acquired face image is initially encrypted by pseudo random sequence generator.
- Then, visual cryptography is applied to shares generation of encrypted image.
- After that, to increase the security generated shares are embedded into cover images using LSB. Finally generated stego shares are stored in database for further process.

2. Authentication Process:

- In authentication process, initially stored shares are loaded from database.
- Then, reverse steganographic process is applied to get the shares from stego shares.
- Next, shares are merged to reconstruct the initial encrypted image using XOR.
- Finally, decryption process implemented to reconstruct the private face image and then matching process implemented for authentication with private and probe face image.

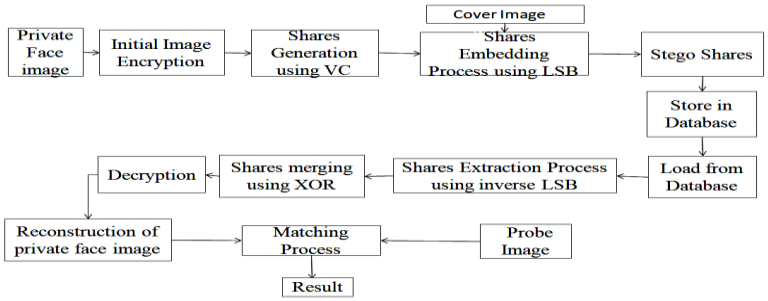

Image Acquisition:

In enrollment process, Image acquisition is the first step in image processing. This step is also known as preprocessing in image processing. It involves retrieving the image from a source, usually a hardware-based source. It's always the foundation step in the workflow since no process available before obtaining an image. In this proposed method, image acquisition is used to retrieve private image of the patients from the image folder.

Initial Image Encryption:

Image encryption is the process of converting plain image into an cipher image utilizing an encryption approach and a secret key. In the proposed method private image is encrypted by using PSRG (Pseudo-Random bit Generator). PRSG is a deterministic program used to generate long bit sequences that look like random sequences given a short random sequence as input.

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 6.551 |Bimonthly, Peer Reviewed & Referred Journal|

| Volume 10, Issue 3, May 2023 |

Shares Generation Using VC:

Visual cryptography uses the characteristics of human vision to decrypt encrypted images and in it the secret image is split into two or more separate random images called shares. To decrypt the encrypted information, the shares are stacked one on top of the other, and the hidden secret image appears. In this Visual Cryptography takes binary image or encrypted image and divides it into two or more pieces known as shares and stored it as share1 and share2. The process of dividing image into shares is called share generation.

Embedding Process:

Embedding is the process in which the tissues or the specimens are enclosed in a mass of the embedding medium using a mould. In this the share images are embedded by a cover image using LSB(Least Significant Bit) and generate stego shares then stored it in database.

Extraction Process and Shares merging:

In Authentication process the process of extraction of stego shares from database is called extraction process and then the shares are merged using XOR method. The XOR operator typically takes two binary encrypted share images as input, and outputs a third image whose pixel values are just those of the first image, XORed with the corresponding pixels from the second.

Decryption and Matching Process:

The encrypted merged share image is converted into a private image utilizing a decryption approach and the process is known as Decryption. Biometric matching refers to the process of the degree of match between two biometric images, one collected at enrollment process and other at identification process. In this work, matching is done between probe image and decrypted image.

IV.CONCLUSION AND FUTURE WORK

An overview of the work has been presented in this document with the outcome that is to be expected. The proposed techniques and algorithms are to show the accuracy of the biometric authentication used in healthcare sector using visual cryptography. Realistic and few assumptions have been made on how the system will look or suppose to work. A discussion regarding visual cryptography and biometric authentication was seen earlier and as a result of which it is clear that it is quite a task to implement facial recognition using visual cryptography and stegnography. It is also the secure method so to increase security level combining of visual cryptography and stegnography is used. The security analysis results demonstrated and proved the proposed scheme can achieve perception security and cryptographic security. Our future work is to implement the proposed system with iris recognition and fingerprint scanning.

REFERENCES

[1] Farhad Ahamed, Farnaz Farid, Basem Suleiman, Zohaib Jan, Luay A. Wahsheh and Seyed Shahrestani "An Intelligent Multimodal Biometric Authentication Model for Personalised Healthcare Services" Future Internet, 2022.

[2] Yuwen Huang, Gongping Yang, Kuikui Wang and Yilong Yin "Multi-view discriminant analysis with sample diversity for ECG biometric recognition" Pattern Recognition letters, 2021.

[3] Lucas Bastos, Thais Tavares, Denis Rosario, Eduardo Cerqueira, Aldri Santos, and Michele Nogue "Double Authentication Model based on PPG and ECG Signals, 2020.

[4] C.L.P. Lim, W.L. Woo, S.S. Dlay and Bin Gao "Heartrate-Dependent Heartwave Biometric Identification with Thresholding-Based GMM- HMM Methodology" IEEE Transactions on Industrial Informatics, 2018.

[5] Kalsoom Fatima, Sumbal Nawaz and Sobia Mehrban "Biometric Authentication in Health Care Sector: A Survey" International Conference on Innovative Computing (ICIC), 2019.

[6] Farid. F, Elkhodr. M, Sabrina. F, Ahamed. F and Gide. E "A Smart Biometric Identity Management Framework for Personalised IoT and Cloud Computing-Based Healthcare Services" Sensors, 2021.

[7] Sancho. J Alesanco and García. J "Biometric authentication using the PPG: A long-term feasibility study" Sensors,

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 6.551 |Bimonthly, Peer Reviewed & Referred Journal|

| Volume 10, Issue 3, May 2023 |

2018.

[8] Al-Naji. F.H and Zagrouba. R, "A survey on continuous authentication methods in Internet of Things environment", Comput. Commun. 2020.

[9] Hossain. M.S, Muhammad. G, Rahman. S.M.M, Abdul. W, Alelaiwi. A, and Alamri. A, "Toward end-to-end biometrics-based security for IoT infrastructure" IEEE Wirel. Commun. 2016.

[10] Kwon. Y.B and Kim. J "Multi-modal authentication using score fusion of ECG and fingerprint" Inf. Commun. Converg. Eng., 2020.

International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)

| Mobile No: +91-9940572462 | Whatsapp: +91-9940572462 | ijarasem@gmail.com |

www.ijarasem.com