The Seybold Report

ISSN 1533-9211

DOI: 10.5281/zenodo.10276427

REMOTE ENTITY AUTHENTICATION USING CHAOTIC MAPS IN TELEMEDICINE (REACT)

K. S. TAMILKODI

Associate Professor, Computer Science, Presidency College (Autonomous), Chennai.

Dr. N. RAMA

Principal, Quaid – E – Millath Government College for Women (Autonomous), Chennai.

Abstract

Just a few years ago, Alexa, ChatGPT, Driverless cars, UAV (Unmanned Aerial Vehicle), Telemedicine, Telesurgery, and so forth were undemonstrative and unapproachable and they were part of science fiction magazines or movies. Today, the rapid advancement of technology transformed individuals' living standards forcefully to a great extent. With the revolution of ICT (Information and Communication Technology), Telemedicine offers remote health care services like Teleconsultation, Teledermatology, Telecardiology, Telepsychiatry, and so on to protect lives or identify ailments. In order to obtain the best services from Telemedicine, the patients, and doctors who reside in geographically separated locations should be authenticated. Telemedicine is a remote access solution that allows patients to connect to any doctors or hospitals around the world within a few seconds by clicking a button. While utilizing it, patients can transfer health-related files and medical images**.** Compromise of these medical images could affect patient privacy and the exactness of the identification of diseases. Authentication is the most important part of any communication system to secure sensitive information against compromising security goals like confidentiality and integrity. Login credentials (the 'User ID' and 'Password') with the CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart), is considered the most common authentication method. Afterward, a number of Biometric authentication techniques were recommended by the researchers. REACT is a novel hybrid authentication method in which both text and image-based passwords are used. In REACT, biometrics (fingerprint/face/iris/ear) can also be used as cryptographic keys to verify their authenticity and prevent unauthorized access. Chaotic maps are used to encrypt these keys and exchange them between the patient and physician before the actual medical image transmission. REACT is a variant of the Diffie-Hellman key exchange algorithm and it considers important attributes like password update, session key agreement, and mutual authentication. Security analysis exhibits that REACT can withstand known attacks and is efficient in terms of authentication.

Keywords: Telemedicine, Biometrics, Authentication, Chaotic Maps, Image-Based Password.

1. INTRODUCTION

Information and Communication Technology (ICT) advancements and their rapid revolution have provided manifold advantages that are beyond imagination. It has also helped us to connect and communicate virtually with anyone, anytime around the world rapidly. As per the definition of the Cambridge Dictionary, authentication is the process of proving that something is real, true, or what people say it is. Along similar lines, message authentication is a technique used to verify the integrity of a message. It asserts that the data received is not changed (inserted/deleted) or replayed during the course of communication. Telemedicine is a boon for the differently abled, elderly, chronic patients, or remote patients with limited access to hospitals. During the course of consultation between the patient and Doctor, they share a secret key for authentication. The authentication mechanism is required to verify whether the identity

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10276427

of the claimed principal is valid or not. Telemedicine was very useful during the COVID-19 lockdown when Patients and Doctors were connected with the help of ICT. Though technology helps us to keep moving, it also has its weaknesses like the breach of patient health records and their related demographic and financial details. Hence a secure authenticated protocol for the transmission of diagnosed details of the patients in Telemedicine is a must and this need has interested many researchers. Many research papers have been published in the last few years on this topic. Telemedicine desperately depends on the internet for sharing patient's medical information anywhere and anytime [22]. A user has to sign on to acquire the service provided by Telemedicine whenever they require it. Undeniably authentication is a must for accessing those services in Telemedicine [6, 9, 17, 24] in order to gain confidence with communicating partners.

The password-based mechanism [40] is the conventional way of authentication in which the patient has to select their login credentials at the time of registration. The method of identifying the patients by their password for further login falls under the category of Single Factor Authentication (SFA). However, the patients use strong passwords susceptible to attacks like eavesdropping, dictionary attacks, shoulder surfing attacks, and many more. Individuals are forced to remember passwords for accessing their electronic devices (mobile phones, laptops, desktops, cameras, etc.,), online accounts like e-mail, financial transactions, social media, and so on. Text-based password for authentication has many shortcomings. To overcome the drawbacks of text passwords [1,4, 5, 10, 34], graphical password authentication techniques came into use and image-based passwords were proved to be easier to memorize than long text. Even the graphical passwords were susceptible to attacks. Hence researchers started using a combination of text, graphical, and new passwords for each and every session.

Preventing an adversary from modifying a message sent by the Patient to the Doctor or vice versa is the main aim of the REACT. REACT is a novel initiative of using the combination of text and image as a password and it belongs to private-key cryptography since the participants share the same key for encryption. For efficient encryption, chaotic maps are used because of their proven characteristics like ergodicity, randomness, sensitivity to initial conditions, and so on. The cryptographic key has to be shared before the actual encryption for authentication.

Authentication [7, 8, 11, 13,] can be accomplished by one or a combination of the following four factors in general:

a) **Knowledge:** Something the user knows (passwords, PIN codes, graphical patterns, etc.)

b) **Ownership:** Something the user possesses (hardware tokens, ID cards, keys, etc.)

c) **Inherence:** Something the user is (physiological biometric, e.g., fingerprint, face, iris, hand geometry, vein patterns or behavioural biometric, e.g., gait, signature, speech, lip movement, keystroke)

d) **Location:** Where the user is (Geo-Fencing - Grants access only when the user is in a specific geographical area, IP address verification - Allows access only from certain IP addresses, Geographical location of the user e.g., Global Positioning System (GPS))

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10276427

In REACT, entity (Patient and Doctor) authentication is done by the combination of both text and image-based passwords. Once the patient registration (enrolment and verification of the patient) is completed, the hospital authorities will send the array of images to the patient which are later used by the patient for authentication. REACT encompasses three levels of authentication with three types of passwords. They are

a) KEK: ACM parameters (P, Q and N)

b) Session Key: IDs of the two images selected by the source.

c) Encrypted Key Exchange: Encryption of the image after mixing 50% of the step **(b)** images. The suggested REACT methodology is resistant to shoulder surfing and to other possible attacks. It is a combination of recognition and recall-based approach [4].

The rest of this paper is summarised as follows: In Section 2, background about cryptographic encryption, image encryption, chaotic maps, and different types of keys are presented. Section 3 gives the details about the existing authentication methods. A complete description of the REACT with flowchart and algorithm is given in Section 4. The efficiency of REACT to withstand various attacks that are used to disrupt is discussed in Section 5. Finally, conclusions are drawn in section 6.

2. BACKGROUND

Adequate authentication is the primary task of confidence for protecting the privacy and resources of a patient and Doctor. This paper makes use of several key concepts like symmetric encryption, chaotic maps, different types of keys, and image passwords for remote entity authentication. The notations used in REACT are given in Table 1.

Table 1: Notations used in REACT

$\mathcal{ACM}$	Arnold Cat Map
$\mathcal{CIPHC}$	Encrypted Image of $\mathcal{PHC}$
$\mathcal{CIRHP}$	Encrypted Image of $\mathcal{CIRHP}$
$\mathcal{D}_d(\ )$	Decryption Algorithm
$\mathcal{DIPHC}$	Decrypted Image of $\mathcal{PHC}$
$\mathcal{DIRHP}$	Decrypted Image of $\mathcal{CIRHP}$
$\mathcal{E}_e(\ )$	Encryption Algorithm
$\mathcal{EVE}$	Adversary/Hacker/intruder/opponent/enemy/attacker/eavesdropper/impersonator
$\mathcal{IA}$	Image Array
$\mathcal{IM1}$	Image 1
$\mathcal{IM2}$	Image 2
$\mathcal{KEK}$	Key Encryption Key
$\mathcal{MIX1}$	Fusion of Image 1 and Image 2 at $\mathcal{PHC}$
$\mathcal{MIX2}$	Fusion of Image 1 and Image 2 at $\mathcal{RHP}$
$\mathcal{MK}$	Master Key
$\mathcal{PHC}$	Primary Health Centre / Patient
$\mathcal{PWD}$	Password
$\mathcal{SK}$	Session Key
$\mathcal{RHP}$	Remote Hospital Physician

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10276427

Encryption

Any encryption scheme has the following five components. They are **Plain / Original Text**: This is the actual message or data that is fed into the encryption algorithm as input.

Encryption Algorithm: An encryption algorithm [23] converts plaintext into cipher text using a key (Denning.) (Douglas R. Stinson) By performing various substitution (replacing the original text with another) and permutation (rearranging the original text elements) operations.

Key: The substitutions and transpositions are accomplished by the encryption algorithm with the help of the key (random bits) known only to the sender and receiver. These keys can be used to encrypt, decrypt, or both [13, 15, 16, 25, 28].

Cipher Text: This is the output of the encryption algorithm which is transformed into unreadable and depends on the plaintext and secret key. Different keys produce different cipher texts for a given plaintext.

Decryption Algorithm: This is the reverse of the encryption algorithm which converts ciphertext back into plaintext only by using a matching key.

Image Encryption

The process of transforming an understandable (visually meaningful) image into a scrambled (visually meaningless) image is said to be image encryption [38]. The reverse process of encryption is known as decryption. Encryption can be classified as symmetric and asymmetric [15, 16, 23]. If the same or single key is used for encryption and decryption, then it is called a symmetric key, otherwise, it is said to be an asymmetric key.

Chaos-based Image Encryption

Confusion and Diffusion [12, 14] are the two main principles of chaos-based encryption. In confusion, the image pixel locations are shuffled, and in diffusion, the image pixel values are changed. Chaotic maps are used as a key in chaos-based encryption [18]. Chaos-based encryption is more suitable for image encryption due to its intrinsic characteristics like ergodicity, sensitivity, random nature, and unpredictability [21, 27, 29, 30, 36, 40, 42]. It is used to convert the highly correlated image pixels into low correlated image pixels.

Chaotic Map - Arnold Cat Map

Chaotic maps are used to generate random numbers, which is the basic requirement for cryptographic keys. Chaotic maps are sensitive to their parameters and initial conditions. After a certain number of iterations, it will return to its original state. Hence it is stated as order in disorder. Arnold Cat map was introduced by Vladimir Arnold, who used the cat image for his research. ACM works by stretching and folding principles [19, 20, 30]. After a predetermined number of iterations, the cat image gets reconstructed.

ISSN 1533-9211

DOI: 10.5281/zenodo.10276427

The image pixels are confused by using the ACM equation (1).

$$\begin{bmatrix} Xn' \\ Yn' \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} Xn \\ Yn \end{bmatrix} \text{ mod N ---------- (1)}$$

Where p and q are the parameters

Xn', and Yn' are the new pixel locations

Xn and Yn are the original pixel locations

N is the image dimension.

Key Management

Key Management is associated with the creation, exchange, storage, deletion, and refreshing of keys [35]. If the size of the key is lengthier then it will be more difficult for the hackers to decode the encoded information and if the lifetime of the key is longer then it will be more comfortable for the hackers to decode the encoded information. The security of the key is more, if the key is divided into a number of shares and distributed through different channels. Key establishment is a process whereby a shared secret becomes available to two communicating parties, for future cryptographic use. One of the communicating parties creates the secret key and securely transfers it to the other one is called key transport. Key agreement means both parties are involved in the generation of the secret keys so that no one can predict the encryption key. Key Encryption Key $(\mathcal{KEK})$ is a cryptographic key that is used for encrypting other cryptographic keys. A session key $\mathcal{SK}$ is a symmetric/asymmetric key used to encrypt each set of data only one time.

Two image IDs from the $\mathcal{IA}$ are used as a $\mathcal{SK}$ in REACT and for every single session, new IDs and passwords will be used. Once the $\mathcal{IM1}$ and $\mathcal{IM2}$ are selected by the $\mathcal{RHP}$, the $\mathcal{SK}$s (IDs) are then coded with the $\mathcal{PWD}$. This $\mathcal{PWD}$-encoded $\mathcal{SK}$ is communicated to the $\mathcal{PHC}$. The advantage of this $\mathcal{SK}$ is that $\mathcal{RHP}$ can effortlessly add and remove entities from their network and each $\mathcal{PHC}$ needs to store only one long-term key.

Graphical / Image Passwords

A graphical password is one of many authentication methods available in order to overcome the drawbacks of textual passwords [33]. Also, it encourages a more visually pleasing and personalized authentication capability. For added security, it can be combined with other authentication methods. Graphical password techniques are classified as recognition-based and recall-based graphical techniques and recall-based graphical techniques.

3. ASSOCIATED WORK

In this section, some of the recently published papers related to entity authentication and key distribution in Telemedicine are demonstrated. This section concentrates on the research work based on SFA (Single Factor Authentication), TWA (Two Factor Authentication), MFA (Multi Factor Authentication), and GPA (Graphical Password Authentication).

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10276427

Leslie Lamport [32] portrayed a method of user password authentication that is secure even if an intruder reads the system's data, or tamper with or eavesdrop on the communication by means of a secure one-way encryption function.

Shimizu, A. [37] proposed a dynamic password authentication system CINON, which uses a one-way function to sequentially authenticate and confirm communicating users. CINON claims that it is able to maintain its security even when the channel is secretly monitored or password file theft, and it can be realized with only a few computations. He compares CINON with the Lamport authentication system which uses a one-way data transformation, and estimates that its execution speed is faster by several hundred to a thousand.

Steven M. Bellovin and Michael Merritt [40] designed a classical cryptographic protocol based on user-chosen keys by initiating a novel combination of asymmetric and symmetric cryptography that allows two parties to share a common password to exchange confidential and authenticated information over an insecure network. These protocols are secure against active attacks, and off-line dictionary attacks. The main aim of the authors is to protect users with weak passwords using EKE (Encrypted Key Exchange).

Chen et al. [11] suggested an efficient and secure dynamic ID-based authentication scheme suitable for the telecare environment. To solve Khan et al.'s scheme drawbacks (user anonymity and shortage of double secret keys), they proposed an enhanced authentication scheme and showed that their scheme is more secure and robust for use in a TMIS (Telecare Medical Information System).

Their scheme provides a reversal mechanism for stolen or lost smart cards and withstands impersonation attacks, replay attacks, man-in-the-middle attacks, and insider attacks.

Wu et al. [44] proposed a novel password-based user authentication scheme appropriate for mobile telecare medicine environments to avoid costly, time-consuming exponential computations. Their scheme consists of the registration phase, the pre-computing phase, the authentication phase, and the password change phase. It is demonstrated to be more efficient, secure, and practical for telecare medicine environments. Also, it is shown to be secure against various attacks, such as replay attacks, online and offline password-guessing attacks, stolen-verifier attacks, and impersonation attacks.

He et al. [24] proposed an improved scheme to eliminate the weakness of the Wu et al. scheme and it has four phases like Wu et al. et al.'s scheme but with better performance. Their scheme is more efficient and can withstand many common attacks.

Jiang et al. [26] proposed a robust chaotic-map-based authentication and key agreement scheme. They performed a cryptanalysis of Hao et al.'s scheme and pointed out its security weaknesses.

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10276427

4. REACT METHODOLOGY

Keys used for encryption, decryption, and user authentication are the most important components of any security system. If these keys get compromised while in transit, then the *EVE* is able to decrypt sensitive data and authenticate themselves as privileged users. Entity authentication is used to verify that an entity is the one being claimed.

In Telemedicine, it is more important that communications be authenticated. The receiver (*RHP*) of a request for consultation wants proof that a request comes from a *PHC* (certain entity) and not from someone else. Both *PHC* and *RHP* should be convinced of each other's identity before the discussion. Authentication is identical to an individual's signature. Entity (*PHC* and *RHP*) authentication is done by the combination of both knowledge and ownership factors in REACT.

PHC initiates the request and registers for consultation. As soon as the user request is verified and accepted as an authentic user, *RHP* sends the *IA* as demonstrated in Table 2 to *PHC*. *PHC* chooses a random number **P, Q,** and **N** such that $2 < P, Q \leq Max$. This will act as a master key (*MK*) and it is enclosed with *PWD*. *PHC* sends this password-protected *MK* to *RHP* through the key channel. When *PWD* (*MK*) is received by *RHP*, *RHP* sends the *PWD* request to *PHC*. *PHC* sends the password *PWD* to *RHP*. *RHP* sends the password-protected image IDs of the two images (*IM1* and *IM2)* selected as the *SK*s from *IA* (Table 2). All these transmissions are carried out through the key channel or the private or secured channel. These images are split into two halves. The even column of *IM1* and odd column of *IM2* are mixed (*MIX1*) by *PHC* and the even column of *IM2* and odd column of *IM1* are mixed (*MIX2*) by *RHP*. *PHC* and *RHP* encrypt the mixed images (*MIX1 and MIX2*) by Arnold Cat Map. They then exchange the encrypted images as exhibited in Figure 2 through the Internet or public channels. By doing this they can authenticate each other.

Table 1: Image Array

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10276427

Since, separating encrypted images is challenging, even if an intruder (*EVE*) were to obtain these mixed encrypted images. Hence, it would be impossible to acquire the original *SK*s from *CIPHC* or *CIRHP*. Once they have exchanged their *SK*s, *PHC*, and *RHP* decrypt the *SK* obtained. After that, they split the *SK* into two half images and combined each image fragment with the other half taken from *IA*. Then the resultant images are equated with those available in *IA*. If both the images are the same (*IM1* = *IA[IM1]* and *IM2*= *IA[IM2]*) then carry out further communication or else terminate the communication.

In doing so, both *PHC* and *RHP* now have the same shared *SK*. Using this *SK*, they can encrypt their biometric keys for robust authentication. Figure 1 depicts the overall architecture of REACT and its equivalent algorithmic steps are elucidated in the REACT Algorithm.

REACT Algorithm

1. *PHC* initiates a request and registers for consultation. (Steps 1 to 7 carried out through key channel)
2. Once the user request is verified and accepted as an authentic user, *RHP* sends the *IA* to *PHC*.
3. *PHC* chooses a random number **P, Q,** and **N** such that 2 < **P, Q** ≤ *Max*. This will act as *MK*.
4. *PHC* sends the password-protected master key to *RHP*.

   PWD (*MK*) ➔ *RHP*.
5. After *PWD* (*MK*) is received by *RHP*, *RHP* sends the *PWD* request to *PHC*.
6. *PHC* sends the password *PWD* ➔ *RHP*.
7. *RHP* sends the password-protected IDs of *IM1* and *IM2* to *PHC*. *IM1* and *IM2* will act as a *SK*.

   PWD (*IM1*, *IM2*) ➔ *PHC*.
8. *PHC* sends the encrypted blended image to *RHP*.

   $CIPHC = E_d(MIX1) = (\text{EvenCol}[IM1] + \text{OddCol}[IM2])$.
9. *RHP* sends the encrypted blended image to *PHC*.

   $CIRHP = E_d(MIX2) = (\text{OddCol}[IM1] + \text{EvenCol}[IM2])$.
10. *PHC* decrypts the received image *CIRHP*.

    $DIPHC = D_d(CIRHP) = D_d(E_d(MIX2))$.

    10.1. Detach the two half images from *DIPHC*. (*IM2* even column of and *IM1* odd column)

    10.2. Combine each image fragment with its other half of *IM1* and *IM2* from *IA*.

    $IM1 = \text{EvenCol}(IA[IM1]) + \text{OddCol}[IM1]$.

    $IM2 = \text{EvenCol}[IM2]) + \text{OddCol}(IA(IM2))$.

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10276427

11. PHC equates $IM1 = IA[IM1]$ and $IM2 = IA[IM2]$.
    11.1. If ($IM1 = IA[IM1]$ *and* $IM2 = IA[IM2]$) Then proceed for further communication.
    Else "Terminate the communication".
12. RHP decrypts the received image $CIPHC$.
    $DIRHP = D_d(CIPHC) = D_d(E_d(MIX1))$.
    12.1. Detach the two half images from $DIRHP$. ($IM1$ even column of and $IM2$ odd column)
    12.2. Combine the resultant image fragment with the other half of $IM1$ and $IM2$ from IA.
    $IM1$ = EvenCol(IA[$IM1$]) + OddCol[$IM1$].
    $IM2$ = EvenCol[$IM2$] + OddCol(IA[$IM2$]).
13. RHP equates $IM1 = IA[IM1]$ and $IM2 = IA[IM2]$.
    13.1. If ($IM1 = IA[IM1]$ and $IM2 = IA[IM2]$) Then proceed for further communication.
    Else "Terminate the communication".

5. RESULTS AND SECURITY ANALYSIS

The recommended REACT is implemented using Java (Eclipse - Photon), on a Windows 8.1 Laptop (Intel i5-4210U CPU @ 1.70GHz) and has been tested for 50 different downloaded images. These images are converted into 60 X 60 pixels. Presently, the results were given only for the PNG type. This section evaluates the proposed scheme REACT against attacks like Password guessing attacks, Shoulder Surfing attacks, PHC impersonation attacks, RHP impersonation attacks, replay attacks, man-in-the-middle attacks, session key disclosure attacks, and mutual authentication.

(a) Replay attacks

Assume that an adversary Eve records the session and replays SK to the RHP aiming to impersonate the patient PHC. Eve cannot fabricate exact $MIX1$ ($IM1$ and $IM2$) and can under no circumstances succeed in the verification process of the RHP.

(b) Shoulder Surfing attack

REACT is a shoulder-surfing resistant scheme because the algorithm steps 1 to 7 are carried out through key channels (direct communication through mobile or E-mail). Eve cannot decrypt the $CIPHC$ or $CIRHP$ without the knowledge of MK and SK.

(c) Man-in-the-middle attack

The first half (steps 1 to 7) of REACT, are achieved through secured key channels between the PHC and RHP without any arbitrator entity. In the second half of REACT, authentication is even though through an open network, Eve has no possibility to impersonate anyone of them without having MK and SK. Therefore, the man-in-the-middle attack is highly impracticable.

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10276427

(d) Password guessing attack

REACT is not vulnerable to password-guessing attacks since it uses encrypted $\mathcal{MK}$ and $\mathcal{SK}$ which are known only to them.

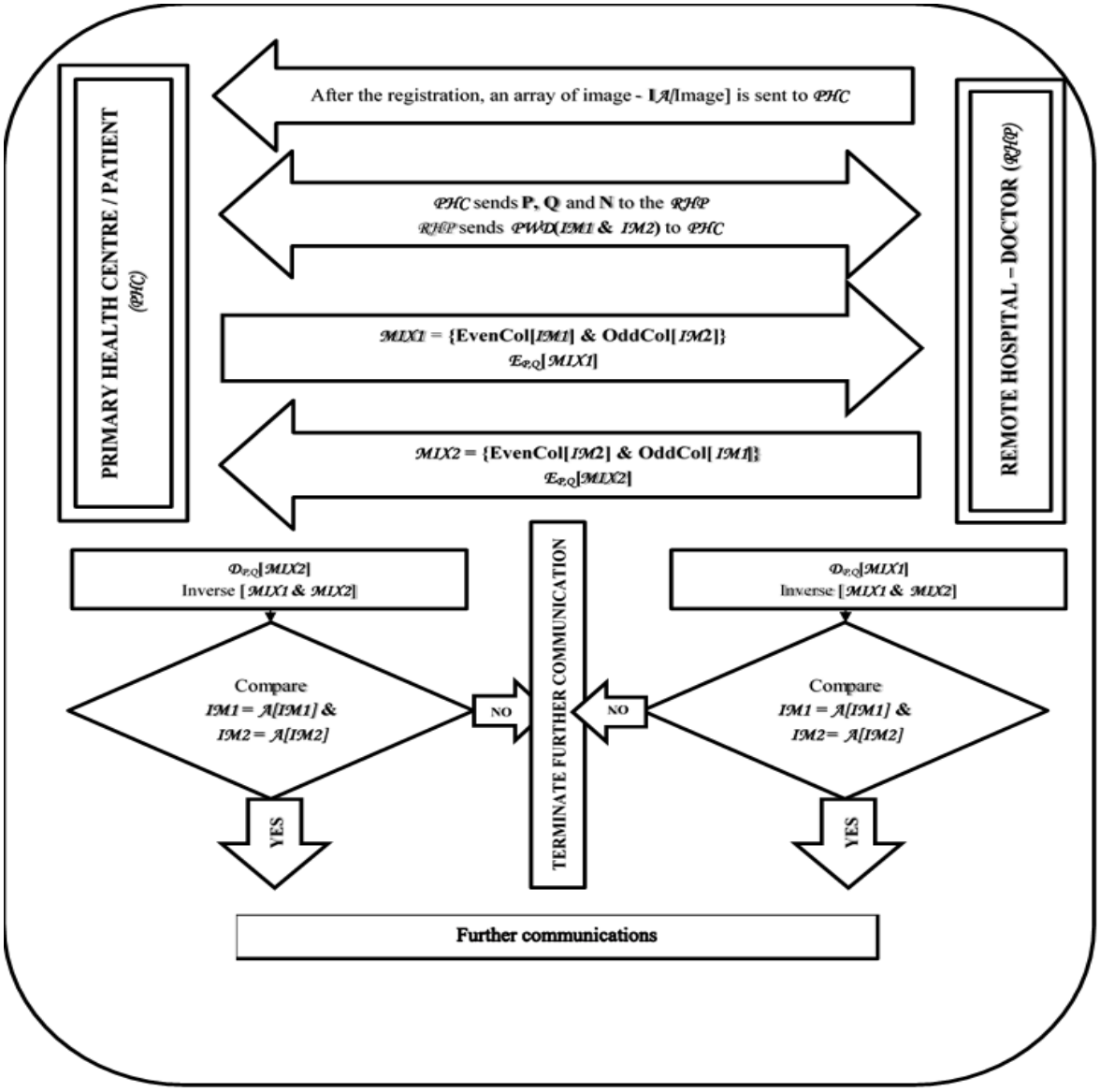

Figure 1: REACT Architecture

(e) Mutual authentication

In React, for each and every consultation, both the $\mathcal{PHC}$ and $\mathcal{RHP}$ must verify the trustworthiness of others by means of the steps given in the algorithm.

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10276427

6. CONCLUSION

This paper presented a novel secure efficient remote entity mutual authentication scheme (REACT) suitable for Telemedicine systems using chaotic $\mathcal{ACM}$. The design rationale of REACT includes accomplishing a provable security against unauthorized access to the patient's personal information in Telemedicine. REACT suggested new authenticated encryption ideas with the help of encrypted text and image-based passwords to encrypt the biometric key. The security analysis showed that the REACT is secure against a range of attacks like brute force attacks, dictionary attacks, password guessing attacks, both $\mathcal{PHC}$ and $\mathcal{RHP}$ impersonation attacks, replay attacks, man-in-the-middle attacks, session key disclosure attacks, and mutual authentication. REACT provides authentication and confidentiality. Since REACT is user-friendly and achieves the best result, it is appropriate for authenticating the principals ($\mathcal{PHC}$ and $\mathcal{RHP}$) involved in Telemedicine.

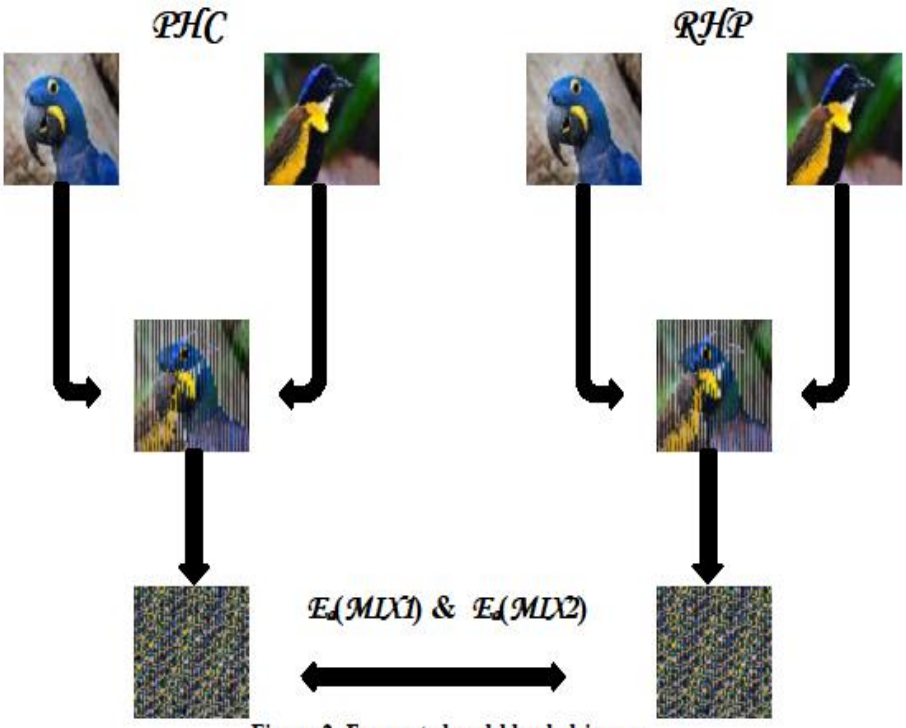

Figure 2: Encrypted and blended image

References

1) Aakansha S. Gokhalea, Vijaya S.Waghmareb. (2016). The Shoulder Surfing Resistant Graphical Password Authentication Technique. *Elsevier B.V.*

2) Alfred J. Menezes Paul C. van Oorschot and Scott A. Vanstone. (2017). Handbook of Applied Cryptography. *CRC PRESS*

3) Alligood, K.T., Sauer, T.D., Yorke, J.A. (1997). Chaos: An introduction to Dynamical Systems, Textbooks in Mathematical Sciences. Springer, New York.

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10276427

4) Amanul Islam, Lip Yee Por, Fazidah Othman, Chin Soon Ku. (2019). A Review on Recognition-Based Graphical Password Techniques. Springer Nature Singapore Pvt Ltd.

5) Agrawal S, Ansari A. Z. and Umar M. S. (2016). Multimedia graphical grid based text password authentication: For advanced users. *Thirteenth International Conference on Wireless and Optical Communications Networks (WOCN), Hyderabad, pp. 1-5.*

6) Ashok Kumar Das and Adrijit Goswami. (2013). A Secure and Efficient Uniqueness-and-Anonymity-Preserving Remote User Authentication Scheme for Connected Health Care. *Springer.*

7) B. Schneier. (1996). Applied Cryptography Protocols, Algorithms, and Source Code in C.

8) *Second Ed., John Wiley & Sons, Inc., New York*.

9) Behrouz A. Forouzan. (2008). Introduction To Cryptography And Network Security. *McGraw-Hill.*

10) Bernard Fong, A. C. M. Fong, C.K. Li. (2010). Telemedicine Technologies Information Technologies in Medicine and Telehealth. *John Wiley & Sons*

11) Bulganmaa Togookhuu, Wuyungerile Li, Yifan Sun and Junxing Zhang. (2017). New graphical password scheme containing questions - background-pattern and implementation. *Procedia Computer Science. 107:148-156*

12) Chen H.-M., Lo J.-W., and Yeh C.-K. (2012). An efficient and secure dynamic id-based authentication scheme for telecare medical information systems. *J. Med. Syst.* 36(6):3907–3915.

13) Claude E. Shannon. (1949), Communication Theory of Secrecy Systems. *Bell System Technical Journal.*

14) David Bishop. (1963). Introduction to Cryptography with Java Applets. *Jones And Bartlett Publishers.*

15) Devaney L. Robert. (1985). An Introduction to Chaotic Dynamical Systems. *Addison –Wesley.*

16) Dorothy Elizabeth Robling Denning. (1945). Cryptography and Data Security. *Addison-Wesley Publishing Company.*

17) Douglas R. Stinson, Maura B. Paterson. (2019). Cryptography Theory and Practice Fourth Edition, *CRC PRESS.S*

18) Debiao H, Jianhua C and Rui Z. (2012). A more secure authentication scheme for telecare medicine information systems.

19) Edward N. Lorenz. (2005). The Essence of Chaos. *CRC Press. Taylor & Francis e-Library, 2005.*

20) Eko Hariyanto, Robbi Rahim. (2013). Arnold's Cat Map Algorithm in Digital Image Encryption. *International Journal of Science and Research*.

21) Elham Hasani, Mohammad Eshghi. (2012). Image Encryption Using Tent Chaotic Map and Arnold Cat Map. *International Journal of Information and Communication Technology Research*.

22) Garnett P. Williams. (1997). Chaos Theory Tamed. *Joseph Henry Press. Washington, D.C.*

23) Georgi Graschew and Stefan Rakowsky. (2010). Telemedicine Techniques and Applications. *InTech.* www.intechopen.com.

24) Hamid R. Nemati, Li Yang. (2010). Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering. *IGI Global.*

25) He Debiao, Chen Jianhua, Zhang Rui. (2012). A More Secure Authentication Scheme for Telecare Medicine Information Systems. *J Med Syst 36:1989–1995*

26) Jean-Philippe Aumasson. (2018). Serious Cryptography A Practical Introduction to Modern Encryption. *ISBN-10: 1-59327-826-8, Published by William Pollock.*

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10276427

27) Jiang, Qi, Jianfeng Ma, Xiang Lu, Youliang Tian. (2014). Robust chaotic map-based authentication and key agreement scheme with strong anonymity for telecare medicine information systems. *J. Med. Syst.* 38(2):1–8.

28) Jizhao Liu, Yide Ma, Shouliang Li, Jing Lian, Xinguo Zhang. (2017). A new simple chaotic system and its application in medical image encryption. *Springer*

29) Jonathan B. Knudsen. (May 1998). Java Cryptography. *O'Reilly & Associates.*

30) K. S. Tamilkodi, Dr. N. Rama. (January 2019). A Distinctive AFO Algorithm For Secured Medical Image Transmission Using Chaotic Crypto Technique. Volume-11, Issue-1, pp. 14-22. *International Journal of Advanced Research in Engineering and Technology (IJARET)*, ISSN: 0976-6480.

31) K. S. Tamilkodi and Dr. (Mrs) N Rama. (2015). Comprehensive Performance Analysis Of Chaotic Colour Image Encryption Algorithms Based On Its Cryptographic Requirements. *International Journal of Information Technology, Control, and Automation (IJITCA)*.

32) Khalid Hamdnaalla, Abubaker Wahaballa, Osman Wahballa. (2013). Digital Image Confidentiality Depends Upon Arnold Transformation And RC4 Algorithms. *International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS, 13*(4).

33) Lamport, L., Password authentication with insecure communication. (1981). *ACM* 24(11):770–772.

34) Mohamed Mohammedi, Mawloud Omar, Wassila Aitabdelmalek, Abla Mansouri1, and Abdelmadjid Bouabdallah. (2018). Secure and Lightweight Biometric-Based Remote Patient Authentication Scheme for Home Healthcare Systems. *IEEE.*

35) Muhammad Umair Aslam, Abdelouahid Derhab, Kashif Saleem, Haider Abbas, Mehmet Orgun, Waseem Iqbal, Baber Aslam. (November 2016). A Survey of Authentication Schemes in Telecare Medicine Information Systems. *Springer.*

36) Nigel Smart. (2013). Cryptography: An Introduction. eBook (3rd Edition).

37) Ruelle David. (1989). Chaotic Evolution and Strange Attractors. *Cambridge University Press*.

38) Shimizu, A. (1991). A dynamic password authentication method using a one-way function. *Systems and computers in Japan* 22(7):32–40.

39) Shivendra Shivani, Suneeta Agarwal, Jasjit S. Suri. (2018). Handbook of Image-Based Security Techniques. *CRC Press Taylor & Francis Group.*

40) Steven D. Galbraith. (March 2018). Authenticated key exchange for SIDH.

41) Steven H. Strogatz. (2018). Nonlinear Dynamics And Chaos with Applications to Physics, Biology, Chemistry, and Engineering. *CRC Press Taylor & Francis Group*

42) Steven M. Bellovin, Michael Merritt. Augmented Encrypted Key Exchange: a Password-Based Protocol Secure Against Dictionary Attacks and Password File Compromise. *AT&T Bell Laboratories.*

43) Tsonis Anastasios A. (1992). Chaos: From Theory to Applications. *Plenum Press*.

44) Wenbo Mao. (2012). Modern Cryptography Theory and Practice. *Pearson, Fifth Impression*.

45) William Stallings. (2007). Cryptography and Network Security Principles and Practices. *Prentice-Hall of India, Fourth Edition*.

46) Zhen-Yu Wu, Yueh-Chun Lee, Feipei Lai, Hung-Chang Lee, Yufang Chung. (2012). A secure authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36(3):1529–1535.