A Lightweight Multi-factor Authentication Scheme based on Digital Watermarking Technique

Trong–Minh Hoang
Telecommunication Faculty
Posts and Telecoms Inst of Technology
Hanoi, Vietnam
hoangtrongminh@ptit.edu.vn

Van–Hau Bui
Electronic Faculty
The Uni of Econ-Tech for Industries
Hanoi, Vietnam
bvhau@uneti.edu.vn

Ngoc–Tan Nguyen
Mathematics and Informatics Faculty
Thang Long University
Hanoi, Vietnam
tannn@thanglong.edu.vn

***Abstract*—Security in today's IoT applications becomes extremely important because it is strongly related to social and human life. The authentication problem is the most important problem and the first step in establishing reliable communication sessions. Biometric authentication solutions including network face recognition have many advantages such as fast, accurate, and user-friendly. Traditional authentication solutions using only device identification have always had to deal with increasingly sophisticated forms of spoofing or sabotage attacks, especially for environments with low-complexity hardware devices. Thus, this paper proposes a novel multi-factor authentication solution to increase the trustworthiness of the authentication process. Moreover, combined with the watermarking technique, the proposed scheme is lightweight and suitable for resource-constrained computing environments. By using BAN logic, the security of the proposed scheme has been analyzed to prove the reliability of the algorithms.**

***Index Terms*—Security, authentication, watermark technique, face recognition.**

I. Introduction

The robust expansion of IoT devices along with applications has been developing in many fields both civil and industrial. While the massive deployment of these objects can enrich people's lives, unauthorized access to such devices has the potential to be dangerous. Thus, authentication mechanisms are always prioritized to be developed to the highest possible level of security. However, theses mechanisms also need to be human-friendly, seamless, and compatible with the constraints of the communication infrastructure (e.g., hardware-constrained wireless sensor network (WSN)).

To improve the reliability and security of the accesses, multi-factor authentication protocols are proposed to guarantee different levels of security in the literature. In conventional authentication protocols, only one authentication factor is used by users such as personal stuffs (e.g., IC cards, tokens, or keys) or user identity (e.g., a PIN or password). By contrast, multi-factor authentication protocols typically add an extra layer of security such as biometric information verification (e.g., fingerprints, retina scans, or facial/voice recognition). The facial recognition method brings several advantages such as remote access, simple operation, high accuracy, and fast detection. However, some issues related to security need to be solved by special techniques or combined with other methods [1]- [2].

To ensure the security of authentication protocols, a lightweight protocol combined secured encryption mechanisms and data integrity checking techniques must be implemented. Such protocol must meet basic constraints of the application configuration and can be deployed in practical scenarios. To reach this aim, a seed key of symmetric encryption method is embedded in the original facial picture and is used to create a session key to against key attacks. This type of symmetric encryption uses lower computation resources than the asymmetric encryption method in [3]. The key attack issue can be avoided by hiding and changing the position of the secret key on watermarked data. We adopt a one-way hash function to protect the IoT devices' secret keys and biometric data by proposing a lightweight multi-factor authentication protocol. It is based on digital watermarking for IoT applications. It can resist a variety of known attacks by establishing a secure session key. To our best knowledge, the proposed protocol based on digital watermarking for IoT applications has not studied in the literature yet. Moreover, Burrows–Abadi–Needham (BAN) logic is utilized to verify the security of the proposed protocol.

The rest of this paper is organized as follows. Session II briefs related studies in this field. The proposed multi-factor authentication protocol is presented in Session III. Evaluating the security of the proposed protocol is conducted in Session IV. Last but not least, our conclusion and future works are shown in the last session.

II. Related Work

In this section, we survey conventional multi-factor authentication protocols for IoT systems from different perspectives. Authors in [2] propose an incognito authenticated key agreement protocol that meets the requirements of authentication while ensuring anonymity, low computational cost and security. The proposed protocol uses pairing-based cryptography that reduces the amount of computation to improve computational efficiency for resource-constrained smart home devices. Physically unclonable functions and the characteristics of the wireless signal of an IoT device are used as two factors for authentication in [3]. Based on the security analysis and results on MICAz motes, the authors show that the proposed protocol can be used as an effective tool to secure IoT systems from

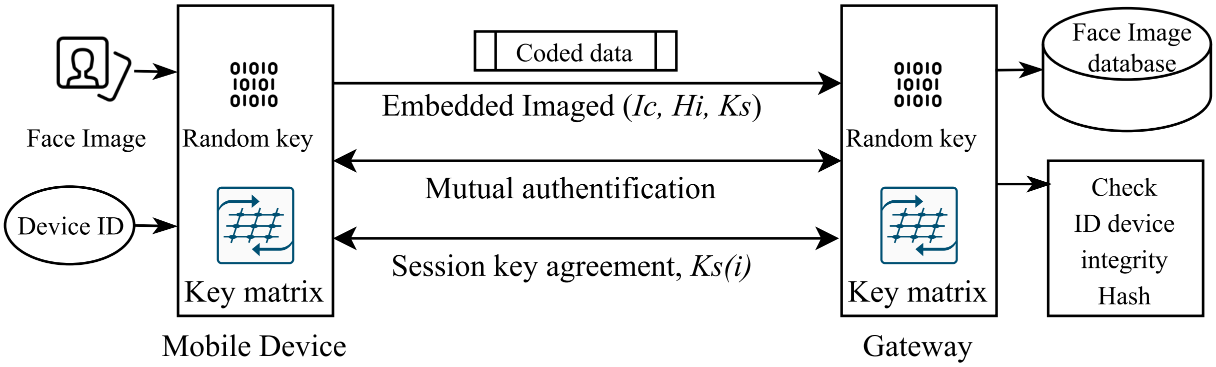

Fig. 1. System model.

spoofing as well as various other attacks. To deal with the complexity of heterogeneous IoT devices, the authors in [4] propose an advanced authentication protocol based on two factors, i.e., Rabin cipher and hash function. This scheme enhances the security properties of data secrecy and device identification through secret key distribution and one-way authentication. However, the aforementioned protocols are just focused on the performance network side.

In [5], authors propose a multi-factor authentication key agreement model (e.g., password, biometric, and smart card) to enable authorized users to remotely access sensor devices in industrial IoT (IIoT) systems. The proposed model uses the secret key method and Chinese Reminder Theorem (CTR) theory to build group keys for sensor devices. Then, group keys is utilized to create a secure session key with the user. The proposed scheme is suitable for the resource-constrained IIoT as it only uses a hash function, bitwise XOR operation, and symmetric cryptography. Although the proposed algorithm is proven to be lightweight, and suitable for resource-constrained systems, direct attacks on biometrics are not covered in this proposal.

During media transmission and storage, data can be altered for illegal use by attackers. Watermarking is an effective way to protect vulnerable data in a digital environment against tampering, intellectual property rights, and enhanced security [6]. In [7], authors propose a watermarking algorithm based on a lossy compression algorithm to ensure authentication and forgery detection. A cryptography-based bit-pair matching watermarking mechanism in the spatial domain is proposed in [8]. Besides, the authors in [8] use the symmetric key cryptography for watermark encryption to protect information from intruders on the communication channel. The goal of the proposed mechanism is to improve the security while minimizing the security traffic increase.

To avoid being exposed the embedded bits of an image to attackers, the authors in [9] proposes a block-based image watermarking algorithm. It generates two different keys by using Diffie Hellman Key Exchange to find the position of the cover image to which the watermark bits are to be embedded. However, this method is vulnerable to jamming attacks because it cannot ensure data integrity. The authors in [10] propose a security technology based on the behavior of MAC layer for digital watermarking. The algorithm takes advantages of physical layer parameters to build embedded watermark values to improve security while ensuring network performance. The proof shows that the algorithm provides a lightweight watermarking mechanism that can work well for resource and power-constrained devices in WSNs.

Based on two concepts of configurable physical unlockable function (PUF) and channel-based parameters, authors in [11] propose a lightweight secure multi-factor device authentication protocol. In the unique value protocol, PUF is used as a secret identifier between pairs of users and changes after each session. Besides, the proposed protocol also exploits the characteristics of the random channel to provide high certainty against various attacks while keeping the low computational complexity. Through studying the aforementioned proposals, we recognize that the multi-factor authentication approach using the watermarking technique based on facial recognition have been not considered in the literature. Thus, we propose a novel authentication protocol for smart home applications. Our contribution consists of two folds:

- We proposed a multi-factor authentication protocol based on face recognition, devices' IDs, and private keys.
- The security strength of the proposed lightweight multi-factor authentication protocol based on watermarking technique is proven by BAN logic.

III. The Proposed Protocol

As illustrated in Fig. 1, the proposed system performs communications between a mobile user U_d and a gateway G_{auth}. To provide reliability communications for the proposed system, an authentication protocol using two authentication factors, i.e., device identity and user face, is proposed in this paper. The user's device U_d is authenticated through a key negotiation process between the device and gateway. The session key K_s after key agreement process is used to ensure the confidentiality of facial recognition information between U_d and G_{auth}. The gateway G_{auth} contains a functional block that processes key information and the user's face authentication. The proposed multi-factor authentication protocol includes four phases, i.e., registration, precomputation, authentication, and key agreement which are presented below.

A. Registration phase

User authentication is an important part of user-to-gateway communication. However, with a large number of IoT devices, diverse types of faking and cloning attacks becomes the most challenge of device authentication. Thus, to enhance the secure of device authentication process, a cover image pre-loaded by both of user device application *Uapp* and gateway is used to generate an ID image I_{id}. The device identification is generated by unique ID (e.g., MAC address). Furthermore, the device identity is continuously changed over time and the session between the user device and the gateway to avoid device identity attacks.

A cover image $I_c(M \times N \times K)$ (e.g., $I_c(512 \times 512 \times 8)$) is created and stored on both the user and gateway sides. A matrix generated by the predefined algorithm on both the user device U_i and gateway G_{auth} sides has a size $I_k(m \times n \times k)$, e.g., $I_k(48 \times 48 \times 8)$. Where m, n are the number of rows and columns of the image, and k is the number of bits used to represent a pixel.

Face recognition authentication process is performed to match the user face obtained through the user's camera and the featured face information is stored on the database. The image data in the database is pre-collected and kept secure at the gateway. To avoid communication attacks, the information of facial data will be encrypted according to the key generated after authenticating the device.

B. Precomputation

From the cover image matrix, we have an image matrix that identifies I_k and is represented by a binary bit matrix $D_k(N \times N)$, e.g., $D_k(48 \times 48)$. This matrix is generated by random selection using a predetermined algorithm and is safe from brute-force attacks when the search length is up to $2^{48 \times 48}$. A chosen initialization key $K(1 \times N)$ is the MAC address of the device (48 bits) that is embedded in the matrix D_k. It is then changed by bit shifting to obtain randomness at any time. To avoid jamming or the man in the middle attacks, the timestamps (t_i, t_j) are added to authentication messages as the same manner in both U_d and G_{auth}. Furthermore, message integrity is assured by hash function $h(.)$ in the proposed algorithms. The following algorithms perform message integrity at both the user device and the gateway.

At the gateway side, G_{auth} carries out a random left-shift of the key by one bit and at the same time insert bit 1 in the right position. After receiving data from U_d, the random key is extracted the watermark. The extracted data is compared with the $D_k(N \times N)$ at the Gateway. If it is not true, we try the case $K(1, N) = 0$ and try until it succeeds. We repeat the transmission sessions until we have received enough N random bits at the receiver and transmitter. At the end, the system has a K_s key which only known by both U_d and G_{auth}.

Algorithm 1 : The $\boldsymbol{K_s}$ generation algorithm at $\boldsymbol{U_d}$.

```
Function: UserAuthGen
Input: $K(1 \times N), D_k(N \times N)$
Output: $K_s$
For: $i = 1; i < N; i++$
    Shift one bit left on $K$;
    $result = false$;
    $DP = K \oplus D_k(i,:)$;
    While: $result = false$
        $T_i =$ system time;
        $H_s = h(DP \| T_i \| K \| D_k(1,:))$;
        Send $H\{DP, T_i, K\}$ to the Gateway;
        While: not received the response message;
            $t_j =$ time between receiving the response messages;
            $H_r = h(result \| t_j \| K \| D_k(1,:))$;
            If: $H_r = H_s | T_i - t_j > 0$
            Then: $result = success$;
$K_s = K$.
```

Algorithm 2 : The $\boldsymbol{K_s}$ generation algorithm on the Gateway's side.

```
Function: GatewayAuthGen
Input: $K(1 \times N), D_k(N \times N), DP(1 \times N)$
Output: $K_s$
For: $i = 1; i < N; i++$
    Shift one bit left on $K$;
    $K(i) = 1$;
    $DP' = DP$;
    $t_j^{'} =$ time between receiving messages ;
    $H_r = h(DP' \| t_i^{'} \| K \| D_k(i,:))$ ;
    If: $H_r = H_s | T_i - t_i^{'} > 0$
    Then: Continue;
    Otherwise: Request $U_d$ to resend;
    $DR = DP'$;
    $DC = K \oplus DR$;
    If: $DC = D_k(i,:)$
    Then: $result = success$;
    Otherwise: $K(i) = 0; DC = K \oplus DR$;
$K_s = K$.
```

C. Authentication and key agreement

In this part, the random key in the previous step is used to watermark the facial image of the user. Assume the user' image is I_c, the data of the authenticated image is divided into R parts, each of length N bits, $I_c \rightarrow I_c(R \times N)$. The watermark insertion algorithm is stated as follows:

At this stage, U_d has done watermarked R on the facial authentication image, then send to G_{auth}. G_{auth} recovers the authentication image from watermarked image to authenticate the user's face. This process is presented in the following algorithm. The recover authentication image algorithm collects each part of the authenticated image. If successful, it proceeds to partially solve the watermark and then merge it into a complete authentication image in Step 14. G_{auth} compares the

Algorithm 3 : Watermark insertion to User's images.

```
Function: WatermarkedAuth
Input: $K_s(1 \times N), I_c(R \times N)$
For: $i = 1; i < R + 1; i + +$
    $DP = K_s \oplus I_c(i, :)$;
    $result = false$;
    While: $result == false$
        $T_i =$ system time;
        $H_s = h(DP \parallel t_i \parallel K_s \parallel D_k(i, :))$;
        Send $H\{DP, t_i, K_s\}$;
        result' = $H\{DP', t_j^{'}, K_s, D_k\}$ from $G_{auth}$;
        If: $HR' = HR$
        Then: $result = success$.
```

Algorithm 4 : Authenticated image recovery.

```
Function: GautRec-Ir
Input: $K_s(1, 1 \ldots N)$
Output: $I_r(m, n)$
 1: $i = 1$;
 2: While: Receive a watermarked image $DP'$
 3:     $H^{'} = hash(DP^{'} \parallel t_i^{'} \parallel K \parallel D)$ ;
 4:     If: $H^{'} = H | t_i^{'} \leq T_i$
 5:     Then: Continue;
 6:     Otherwise: Request to resend;
 7:     $DR = DP^{'}$;
 8:     Set the transmission time $t_j$;
 9:     $HR = h(result \parallel t_j \parallel K_s \parallel D_k)$;
10:     Send back to $U_d$ a message $\{result, t_j, HR\}$;
11:     If: $result = false$;
12:     Then: Go to Step 1;
13:     Else If: $result = success$ and $i < R + 1$;
14:     Then: $I_r(i, :) = DR \oplus K_s, i + +$;
15:     If: $i = R$;
16:     Then: $I_r(m, n) = \cup_{i-1}^{R}(i, 1 \ldots N)$.
```

received authentication image with the authentication database recorded in G_{auth} and make a decision unlock or not. The identification process can use one of the popular methods such as PCA, LDA, or SVM.

IV. Security Analysis

In this session, the main secure aspects is analyzed to verify the proposed scheme. Based on BAN logic, we validate the proposed algorithms are safe. Consider a round of the executed algorithm, we have:

Message 1 (APP → LOCK): $\{DP, t_i, h(DP \parallel t_i \parallel K \parallel D)\}$

Message 2 (LOCK → APP): $\{result, t_j, h(result \parallel t_j \parallel K \parallel D)\}$

Idelizing the message as

Message 1 (APP → LOCK): $\langle DP, t_i \rangle_{K,D}$

Message 2 (LOCK → APP): $\langle result, t_j \rangle_{K,D}$

With assumptions:

A1. $APP \mid\equiv K, D$

A2. $LOCK \mid\equiv K, D$

A3. $APP \mid\equiv \#(t_i)$

A4. $LOCK \mid\equiv \#(t_j)$

A5. $APP \mid\equiv \#(t_j)$

A6. $LOCK \mid\equiv \#(t_i)$

A7. $LOCK \mid\equiv APP \mid\Rightarrow \langle DP, t_i \rangle$

A8. $APP \mid\equiv LOCK \mid\Rightarrow \langle result, t_j \rangle$

We need to prove

G1. $APP \mid\equiv K_s$

G2. $LOCK \mid\equiv K_s$

The progress is expressed as

S1. From Message 1, we have:

$$LOCK \triangleleft \langle DP, t_i \rangle_{APP \overset{K,D}{\leftrightarrow} LOCK}$$

S2. Use **S1** and **A2**, we have:

$$LOCK \mid\equiv APP \mid\sim \langle DP, t_i \rangle$$

S3. Use **S2** and **A6**, we have: $LOCK \mid\equiv APP \mid\Rightarrow \langle DP, t_i \rangle$

S4. Use **S3** and **A7** we have: $LOCK \mid\equiv \langle DP, t_i \rangle$

S5. From **S4**, we have: $LOCK \mid\equiv DP$

S6. From Message 2, we have:

$$APP \triangleleft \langle result, t_j \rangle_{APP \overset{K,D}{\leftrightarrow} LOCK}$$

S7. Use **S6** and **S1** we have:

$$APP \mid\equiv LOCK \mid\sim \langle result, t_j \rangle$$

S8. Use **S7**, **A5**, and **A8**, we have: $APP \mid\equiv result$

From results of **S5** and **S8**, we have

$APP \mid\equiv K_s$ (**G1**)

$LOCK \mid\equiv K_s$ (**G2**)

Conclusion: The proposed algorithms are safe.

V. Conclusion

In this paper, we have proposed a multi-factor authentication protocol using device identification and facial recognition. For the former, the finite length device identification is processed to enhance the security level through the image embedding solution and act as an authentication element to verify the user. This technique can resist spoofing or identity theft attacks of the IoT device. The latter, facial recognition is an effective approach today. To avoid biometric attacks, the facial recognition data is encrypted and verified through the key generated from the device authentication process. Moreover, the proposed scheme uses watermaking technique to bring convenience and lightness to the proposed protocol. The security of the proposed scheme has been proven by BAN logic. In future work, we aim to deploy the proposed protocol a door lock system using facial recognition on the user's smartphone in home/office environments.

References

[1] S. Challa et al., "lSecure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications," in *IEEE Access*, vol. 5, pp. 3028-3043, 2017.

[2] B. Yu, and H. Li, "Anonymous authentication key agreement scheme with pairing-based cryptography for home-based multi-sensor Internet of Things," in *Int. J. Distrib. Sens. Netw*, vol. 15, no. 9, Sep. 2019.

[3] M. N. Aman, M. H. Basheer, and B. Sikdar, "Two-Factor Authentication for IoT With Location Information," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3335-3351, Apr. 2019.

[4] A. Attkan, and P. Ahlawat, "Lightweight Two-factor Authentication Protocol and Session Key Generation Scheme for WSN in IoT Deployment,".

[5] H. Guo, Y. Gao, T. Xu, X. Zhang, and J. Ye, “A secure and efficient three-factor multi-gateway authentication protocol for wireless sensor networks,” in *Ad Hoc Networks*, vol. 95, 2019.

[6] A. Mohanarathinam et al., “Digital watermarking techniques for image security: a review,” in *J. Ambient Intell. Human Comput.* , Sep. 2019, pp. 3221–3229.

[7] M. A. Kabir, “An efficient low bit rate image watermarking and tamper detection for image authentication,” in *SN Appl. Sci.*,2021.

[8] S. Bal et al., “On the implementation of a secured watermarking mechanism based on cryptography and bit pairs matching,” in *J. King Saud Univ. - Comput. Inf. Sci.*, 2018.

[9] J. Aparna and S. Ayyappan, “Image Watermarking Using Diffie Hellman Key Exchange Algorithm,” in *Procedia Comput. Sci.*, vol. 46, pp. 1684-1691, 2015.

[10] V. Nguyen, T. Hoang, T. Duong, Q. Nguyen, and V. Bui, “A Lightweight Watermark Scheme Utilizing MAC Layer Behaviors for Wireless Sensor Networks,” in *Proc. Int. Conf. Recent Adv. Signal Process. Telecommun. Comput.* (SigTelCom), 2019, pp. 176-180.

[11] R. Melki, H. N. Noura, and A. Chehab, “Lightweight multi-factor mutual authentication protocol for IoT devices,” in *Int. J. Inf. Secur.*, vol. 19, pp. 679-694, 2020.

[12] M. G. Galterio, S. A. Shavit, and T. Hayajneh, “A Review of Facial Biometrics Security for Smart Devices,” *Computers*, vol. 37, no.3, 2018.

[13] E. Anaya, J. Patel, P. Shah, V. Shah, and Y. Cheng, “A Performance Study on Cryptographic Algorithms for IoT Devices,” *Proceedings of the Tenth ACM Conference on Data and Application Security and Privacy*, pp. 159-161, NY, USA, 2020.