Future Generation Computer Systems 100 (2019) 938–951

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Robust secure communication protocol for smart healthcare system with FPGA implementation

Venkatasamy Sureshkumar [a], Ruhul Amin [b,*], V.R. Vijaykumar [c], S. Raja Sekar [d]

[a] Department of Applied Mathematics and Computational Sciences, PSG College of Technology, Coimbatore, Tamilnadu, India
[b] Department of Computer Science and Engineering, Dr. Shyama Prasad Mukherjee International Institute of Information Technology, Naya Raipur, India
[c] Department of Electronics and Communication Engineering, Anna University, Coimbatore, Tamilnadu, India
[d] Department of Electronics and Communication Engineering, Bannari Amman Institute of Technology, Sathyamangalam, Tamilnadu, India

HIGHLIGHTS

- We have proposed a robust authentication and key establishment protocol for MWSN.
- Mutual authentication of the proposed protocol has been verified using BAN logic.
- An informal analysis of the protocol confirms high level security protection.
- We have compared and provided complexity overhead comparison.
- We presented the implementation results of protocol using Altera Quartus II simulation tool.

ARTICLE INFO

Article history:
Received 30 December 2018
Received in revised form 15 April 2019
Accepted 21 May 2019
Available online 29 May 2019

Keywords:
Mutual authentication
MWSN
BAN logic
Gateway node
Sensor node

ABSTRACT

Vast development of wireless technology and cloud computing has given lots of benefit to the society in a variety of ways. One such application using this technology is telemedicine or mobile healthcare and in this, security is one of the most important concern. In recent times, multimedia applications include mobile networks, integrated sensors and Internet-of-Things (IoT) services. In the landscape of IoT systems, the problem of privacy, security and trust has remained a challenge since several years. There are only few works proposed to support secure communication in the IoT-enabled Medical Wireless Sensor Networks (MWSNs). However, the existing protocols have some design flaws and are vulnerable to several security attacks including sensor and user impersonation attacks. In this paper, a novel architecture in the MWSNs is proposed and a suitable authenticated key establishment protocol using the light weight Elliptic Curve Cryptography (ECC) for the architecture is designed. The proposed authentication protocol solves the security issues found in existing protocols. The formal method Burrows–Abadi–Needham (BAN) logic is enforced to prove the correctness of the protocol. Further investigation has led to the claim that the protocol is safe from known security attacks. In addition, the proposed protocol is described in Verilog Hardware Description Language (HDL) and its functionalities are checked using Altera Quartus II simulation tool for Field-Programmable Gate Array (FPGA) implementation. The analysis of our protocol and comparison of it with similar protocols show that the proposed protocol is more efficient and robust than the existing protocols.

1. Introduction

In recent days, electronic health (E-health) and mobile health (M-health) plays a vital role in healthcare/telemedicine management systems by assisting the doctors as well as the patients to assess the data at their fingertips [1]. In that system, patients confidential medical data are need to transferred and stored in cloud server for remote access but the secure way of transmission in the unsecure channel is a challenging task [2]. In addition, the medical data of a patient is stored either in the form of hardcopy or softcopy in the hospital premises itself. The main problem in this kind of medical data storage is that, there is a scope to steal the data in an unauthorized manner for clinical and educational research or by the insurance agencies [3]. This unauthorized access of medical data severely affects the privacy of the patient [1,4–6]. Hence the main challenge is to safeguard the medical data of an individual.

* Corresponding author.
E-mail addresses: sand@amc.psgtech.ac.in (V. Sureshkumar), amin_ruhul@live.com (R. Amin), vr_vijay@yahoo.com (V.R. Vijaykumar), srajasekarbeece@gmail.com (S.R. Sekar).

https://doi.org/10.1016/j.future.2019.05.058
0167-739X/

The development of wireless technologies particularly smart devices play a crucial role in the e-health applications. Recently, the notion of Wireless Body Area Network (WBAN) is incorporated in the real time monitoring of a patient health by implanting intelligent medical sensors in the body to acquire the medical data such as blood glucose level, heart rate, cholesterol level and so on [7]. In addition, MWSN gives freedom to the patient for moving in the hospital surrounding area and also it reduces the cost of medication. In this technology, some intelligent medical sensors are implanted in the patient body to collect medical data and the same will be transmitted to the remote hospital or doctor through wireless medium [8,9]. This will provide a quicker way to diagnose and safeguard the life of a patient.

However, security is the main concern in the real time monitoring and transmitting the medical data of an individual from unauthorized access [10,11]. During this transmission normally different security attacks such as eavesdropping, impersonation attack and replay attacks are possible [10,11]. In order to provide the security by means of proposing a robust protocol which has the basic entities as sensor nodes, gateway nodes and portable handheld devices. The security of the protocol is maintained by generating the time based same session key at three entities through registration phase, authentication and communication phases [9,12,13]. The communication among the connected medical devices and sensors need proper authentication to confirm the truth of the data. Hence, there is a requirement of mutual authentication and key agreement between the users before transmitting the medical information [12,14,15]. Authentication protocols are useful in this case for the confirmation of valid medical data [12,16]. Currently many such authentication protocols are been discussed by the research community [17–19]. Such protocols are susceptible to several security attacks like identity and password guessing attacks, sensor node impersonation attack and so on. A robust authentication protocol which could withstand various attacks is needed for this purpose.

Now-a-days, it is a very difficult task to monitor the patients by doctor continuously, due to the huge or more number of persons are admitted in the hospital. Sensor technology provides one of the solutions for such type of problem by interconnecting the sensors and save the data in the common area such as cloud server. In our proposed solution, it is clearly mentioned that the sensed medical data by the sensor is being stored in the cloud server and the doctors can also directly access required data either from hospital or home. Therefore, the application of smart health care system enhance the quality of our life by monitoring the health condition of patients. Different types of sensor node such as ECG sensor, blood pressure sensor, pulse oximetry sensor, inertial sensor etc. can be implanted into the parts of the body for sensing medical information which is very useful for the detection of disease. The smart health care system can be used for early detection of disease, health monitoring, post-surgery feedback etc. It is also feasible to use machine learning approach for data analytics on medical information for the detection of very unsafe disease like cancer, Parkinsons, asthma etc. in advance. In this way, health care industry can use our proposed solution for the real-life implementation in order to provide standard platform for smart health care system.

1.1. Motivation and contribution

Based on the literature review it is found that, improvement is still required in terms of security attacks. Most of the literatures have their own limitation such as not providing user anonymity and other ideal functions. In addition, it is being vulnerable to some attacks. In general, to provide secure communication for MWSN, the security protocol needs to be attacks free; in this manuscript, we have presented a user authentication protocol with privacy protection for MWSN which is robust against the security threats. In addition, to ensure compatibility for real time implementation, the designed protocol needs to be supported by the hardware realization. The existing authentication and key establishment schemes fail to provide hardware implementation results whereas our proposed scheme is described using Verilog Hardware Description Language (HDL) and simulated using Altera Quartus II for FPGA implementation. Finally, the entire protocol is implemented in Altera DE2 FPGA development board.

1.2. Roadmap

Section 2 gives a complete overview of the existing related works with their merits and demerits. Section 3 presents a novel architecture suitable for the MWSNs and description of the proposed protocol in various phases. Section 4 provides the formal proof for the correctness of the proposed protocol using BAN logic and an informal security analysis of the scheme. In Section 5, a comparative analysis of the proposed scheme with several existing similar schemes is done and a hardware implementation using Altera Quartus II tool is carried out. Section 6 concludes the work with future directions.

2. Related works

In 2009 Das [20] proposed two-factor authentication protocol for wireless sensor network in which the user needs to store some of the secrete credentials in the mobile device. In 2010 He et al. [21] showed that Das [20] scheme is vulnerable to impersonation attack, insider attack and it is proven to be infeasible for the user to change the password. As a remedy, He et al. [21] suggested a two-factor authentication protocol that overcomes the weakness found in [20]. In 2011, Kumar et al. [22] demonstrated that He et al. [21] scheme does not provide user anonymity, mutual authentication between sensor node and user, fails to establish session key and do not withstands information leakage attack.

In 2012 Kumar et al. [23] proposed a robust authentication protocol using medical wireless sensor network for health care applications and claimed that it withstands several security attacks. Unfortunately in 2014, Khan–Kumari [24] mentioned that the scheme by Kumar et al. [23] is vulnerable to stolen smart card attack. Also in 2015 He et al. [25] pointed out that the scheme in [23] does not withstand insider attack, off-line guessing attack and fails to provide user anonymity. Later in 2016 Li et al. [26] found that the scheme [25] by He et al. is incorrect in authentication and session key agreement phase, and their scheme has no wrong password detection mechanism which will cause Denial of service attack. In 2017 Wu et al. [27] also, demonstrated that He et al. [25] scheme fails to withstand user impersonation attack, off-line guessing attack and sensor node capture attack.

In 2016 Farash et al. [28] come up with a robust user authentication and key agreement scheme in the environment IoT using heterogeneous wireless sensor network. In the same year, Amin–Biswas [29] pointed out that the architecture in [28] scheme is not suitable for practical application because in their scheme user directly contacted the sensor node and it wastes sensor energy. And Amin–Biswas [29] suggested a novel multi-gateway based authentication protocol that can overcome the mentioned drawbacks. But, later in [30] Amin et al. pointed out that the scheme in [29] had also a unfavourable weakness that the user contacts the sensor at the end in the authentication and they suggested a novel two factor authentication protocol for MWSN. Unfortunately in 2018, Ali et al. [31] found that the scheme by Amin et al. [30] is susceptible to user impersonation attack,

off-line password guessing attack, identity guessing attack and known session-key temporary information attack. In the same year, Wu et al. in [32] mentioned that the scheme in [30] is still vulnerable to de-synchronization attack and off-line guessing attacks. As a remedy, Wu et al. [32] have come up with a relatively robust and lightweight two-factor authentication protocol for MWSNs. Recently, Li et al. [33] demonstrated that the scheme by Wu et al. [32] fails to achieve forward secrecy and the scheme has no provision of user friendliness.

In 2017, Liu and Chung [18] designed a bilinear pairing based authentication protocol for wireless healthcare sensor networks. The scheme requires a trusted authority for user authentication and also to build secure communication between a sensor node and a user. In recent, Challa et al. [19] proved that Liu–Chung's [18] scheme is susceptible to many known security threats including stolen smart card attack, off-line password guessing attack and user impersonation attack.

In order to over come existing limitations and vulnerabilities, we propose a resilient ECC based three-factor mutual authentication protocol with key establishment technique for WSN in the medical environment.

3. Proposed protocol

In this section, we present an architecture suitable for the medical wireless sensor networks. This section also presents the proposed protocol which is designed so that the security issues and vulnerabilities found in the literature are rectified. With reference to the architecture designed, all the protocol entities(Medical professional, sensor node and gateway node) must be authentic before communications take place. The proposed protocol consists of seven phases, (1) System setup, (2) Registration of the sensor and gateway nodes, (3) User/professional registration, (4) User-login, (5) Gateway-sensor authentication, (6) Password renewal, and (7) Sensor node inclusion phase.

3.1. Network architecture

We propose a novel architecture to one such telemedicine system explained in Section 1 and the proposed architecture is depicted in Fig. 1. In the architecture, wireless low power intelligent medical sensors such as pace maker, brain neuro simulator, blood glucose level sensors etc are implanted on the patient body. These sensors regularly update the data to the nearby smart devices using bluetooth, zigbee or infrared communication technologies. Since the smart devices are near to the patient, in general the security aspects need not be considered. Any medical practitioner/relatives can access the medical data stored in the smart device via internet through the nearby gateway or access point. In the proposed architecture, it is regarded that the patient is inside the hospital, the doctor can either inside the hospital or in the home or anywhere roaming out side the hospital. Periodically, the gateway 1 gets the data from the sensor node via the cluster head (smart device) and stores in the cloud server. The doctor can access the patient data when the doctor is inside the hospital through the gateway 1 from the sensor node. If the doctor is out side the hospital, s/he can access the patient's off-line data from the cloud server through the gateway 2 or gateway 3 whichever is within his/her coverage. In this scenario, communication between smart devices and medical practitioner will be always through insecure channel. Thus, before establishing the communication or accessing the medical information of a patient via smart devices, the user and the smart devices must be authenticated mutually. Hence there is a need for developing a lightweight hardware mutual authentication protocol for secure communications.

3.2. System setup phase

For the authentication between protocol entities, it is necessary that there should be some secret credentials which need to be shared between them [34,35]. System Administrator (SA) manually completes the setup phase and stores all the credentials in the cloud server. Using these credentials, the entities can complete their registration part and hence share the credentials. The proposed protocol is designed using light weight cryptosystem ECC for the purpose of implementation in the smart device. A server in the cloud, construct an ECC $E(F_q) = \langle P, q, a, b, n, G(P)\rangle$ with a long term secret value $S_{SA} \in F_q$.

3.3. Gateway and sensor node registration phase

Gateway and sensor nodes are objects, they requires manual assistance for their registration purpose. This phase is executed by the SA to make them registered by performing the following steps.

Step SGR1. SA selects an identity GW_{ID_j} for jth gateway node GW_j, which is a unique identity for that gateway node. SA computes the secret value $S_{GW_j} = h(S_{SA}||GW_{ID_j})$ and stores in the database so that it corresponds to the gateway node GW_j. Further SA sores the pair $\langle GW_{ID_j}, S_{GW_j}\rangle$ into the memory of gateway node GW_j.

Step SGR2. SA selects an identity SN_{ID_k} for kth sensor node SN_k and computes a secret value $S_{SN_k} = h(S_{SA}||SN_{ID_k})$. This kth sensor node is accessible only for the jth gateway node GW_j. Thus, the SA stores $\langle SN_{ID_k}, S_{SN_k}\rangle$ in both the gateway node GW_j's and sensor node SN_k's memory . The procedure to complete the gateway and sensor node registration is also compiled in the Algorithm 1

Algorithm 1 Gateway and Sensor node registration process

1: SA selects an identity GW_{ID_j} for GW_j
2: SA computes $S_{GW_j} = h(S_{SA}||GW_{ID_j})$ and stores it in the database corresponds to GW_j
3: SA sores the pair $\langle GW_{ID_j}, S_{GW_j}\rangle$ into the memory of GW_j
4: SA selects an identity SN_{ID_k} for kth sensor node SN_k
5: SA computes $S_{SN_k} = h(S_{SA}||SN_{ID_k})$
6: SA stores $\langle SN_{ID_k}, S_{SN_k}\rangle$ in both GW_j's and SN_k's memory

These shared secret credentials are useful for authenticating the entities gateway node and sensor node while user login authentication.

Finally SA publishes the list of IDs of registered gateway nodes for the user access. Sensor node identities are kept secret to achieve sensor node anonymity.

3.4. User registration phase

Usually a legitimate user accesses the sensed data from the sensor node via the gateway node after proper authentication. As the authentication requires some shared credentials of the user with sensor and gateway nodes, in this phase user shares his/her credentials through the system administrator by making an one time registration. The details of this phase is described as below.

Step UR1. The user U_i chooses an identity ID_i, a password PW_i and computes the bio-hashing $b_i = H(B_i)$ with his/her biometric B_i. The user also computes $HID_i = h(ID_i||b_i)$, $HPW_i = h(PW_i||b_i)$ and transmits the registration details $\langle HID_i, HPW_i, GW_{ID_j}\rangle$ to SA.

Step UR2. After receiving the user request, SA computes the following

$A_1 = h(HID_i||HPW_i) \cdot P$

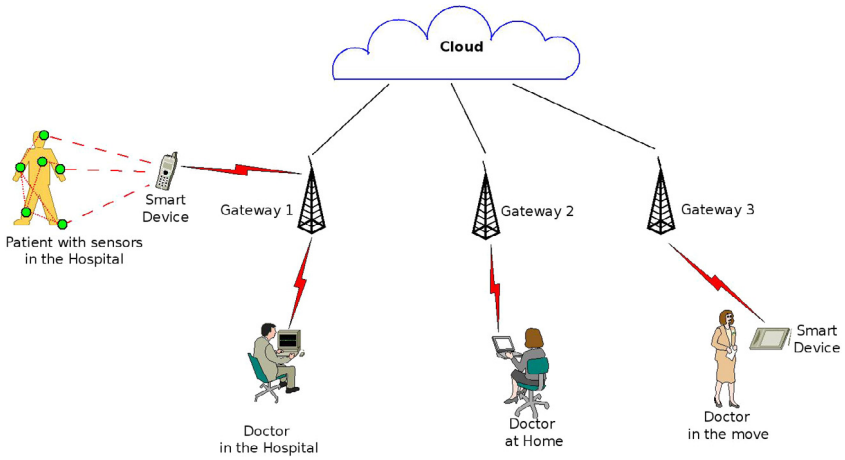


Fig. 1. Network architecture.

$$A_2 = h(HID_i||S_{GW_j}) \cdot P$$
$$A_3 = A_2 \oplus A_1$$
$$A_4 = S_{GW_j} \cdot P$$

SA constructs the smart card $SC = \langle A_3, A_4, h(\cdot), P\rangle$ and send the smart card to the user via a secured channel.

Step UR3. Upon the receipt of the smart card from SA, the user computes

$$HPID_i = h(HID_i||PW_i)$$
$$A_5 = h(HID||HPID_i) \cdot P$$
$$A_2^* = A_3 \oplus A_1$$
$$A_6 = A_2^* \oplus A_4$$

User stores A_5 and replace A_4 with A_6 in the smart card. Now user's smart card becomes $SC = \langle A_3, A_5, A_6, h(\cdot), P\rangle$.

This set of steps for the user registration is also provided in the Algorithm 2.

Algorithm 2 User registration process

1: The user U_i chooses ID_i and PW_i
2: U_i computes $b_i = H(B_i)$
3: U_i computes $HID_i = h(ID_i||b_i)$ and $HPW_i = h(PW_i||b_i)$
4: U_i sends $\langle HID_i, HPW_i, GW_{ID_j}\rangle$ to SA
5: SA computes $A_1 = h(HID_i||HPW_i) \cdot P$, $A_2 = h(HID_i||S_{GW_j}) \cdot P$, $A_3 = A_2 \oplus A_1$ and $A_4 = S_{GW_j} \cdot P$
6: SA constructs $SC = \langle A_3, A_4, h(\cdot), P\rangle$
7: SA sends SC to U_i

3.5. Login phase

When the user needs to access sensed data from the sensor node SN_k, s/he needs to login through the gateway node GW_{ID_j}. For which the following are the steps carried out by the user U_i.

Step UL1. U_i inputs SC into the terminal (card reader) and enters ID_i, PW_i with the biometric B_i.

Step UL2. SC computes $b_i = H(B_i)$, $HID_i = h(ID_i||b_i)$ and $HPID = h(HID_i||PW_i)$. SC also computes $A_5^* = h(HID_i||HPID_i).P$ and checks whether $A_5^* \stackrel{?}{=} A_5$. If it is false, the smart card terminates the session otherwise chooses a random number $r_u \in F_q$ and computes

$$HPW_i = h(PW_i||b_i)$$
$$A_1^* = h(HID_i||HPW_i) \cdot P$$
$$A_2^* = A_3 \oplus A_1^*$$
$$A_7 = h(A_2^*||T_1)$$
$$A_8 = r_u \cdot P$$
$$A_9 = A_8 \oplus A_2^*$$
$$A_{10} = A_6 \oplus A_9$$
$$= A_4 \oplus A_8$$

where T_1 is the current timestamp.

Step UL3. Smart card transmits the login message $M_1 = \langle A_7, A_9, A_{10}, T_1\rangle$ to the gateway node GW_j.

In this way the user can initiates the protocol and login into system for accessing the patient data from the sensor node.

3.6. Authentication phase

This phase is executed to authenticate the protocol entities and create a session key between the them for the future session. The detailed description of the authentication phase is given below.

Step AP1. Upon the receipt of the login request, gateway node GW_j verifies the time delay $\triangle T = T_2 - T_1$, with the current timestamp T_2 at gateway node. If $\triangle T$ is not an acceptable time delay, the GW_j rejects the request otherwise computes the following

$$A_4^* = S_{GW_j} \cdot P$$
$$A_8^* = A_{10} \oplus A_4$$
$$A_2^{**} = A_9 \oplus A_8^*$$
$$A_7^* = h(A_2^{**}||T_1)$$

and checks whether $A_7^* \stackrel{?}{=} A_7$. If the check is correct, GW_j picks a random number $r_g \in F_q$ and computes

$$A_{11} = r_g \cdot A_8^* = r_u \cdot r_g \cdot P$$
$$A_{12} = r_g \cdot P$$
$$A_{13} = h(S_{SN_k}) \cdot A_{12}$$
$$A_{14} = h(GW_{ID_j}||S_{SN_k}) \cdot P$$
$$A_{15} = h(A_{14}||T_2)$$
$$A_{16} = A_8^* \oplus A_{13}$$

The gateway sends the message $M_2 = \langle A_{12}, A_{11}, A_{15}, A_{16}, T_2\rangle$ to SN_k.

Step AP2. After receive the message M_2 from GW_j, the sensor node SN_k verifies the time delay $\triangle T = T_3 - T_2$, with the current

timestamp T_3 at the sensor node. If $\triangle T$ is not an allowable time delay, then SN_k rejects the request otherwise computes $A_{14}^* = h(GW_{ID_j}||S_{SN_k}) \cdot P$, $A_{15}^* = h(A_{14}^*||T_2)$ and checks $A_{15}^* \stackrel{?}{=} A_{15}$. If it is true then chooses a random number $r_s \in F_q$ and computes the following

$$A_{17} = r_s \cdot A_{12}$$
$$A_{18} = h(A_{17}\|S_{SN_k}\|T_3)$$
$$A_{13}^* = h(S_{SN_k}) \cdot A_{12}$$
$$A_8^{**} = A_{16} \oplus A_{13}^*$$
$$A_{19} = r_s \cdot A_8^{**}$$
$$A_{20} = r_s \cdot P$$

Finally SN_k computes the session key $sk = r_s \cdot A_{11}$ and sends the message $M_3 = \langle A_{19}, A_{18}, A_{20}, T_3\rangle$.

Step AP3. After getting the message M_3 from SN_k, the gateway node GW_j checks the time delay $\triangle T = T_4 - T_3$, with the current timestamp T_4 at the gateway node. If $\triangle T$ is not an acceptable time delay, the GW_j rejects the request otherwise computes $A_{17}^* = r_g \cdot A_{20}$ and checks for the correctness of $A_{18}^* = h(A_{17}^*\|S_{SN_k}\|T_3) \stackrel{?}{=} A_{18}$. If it is true then the gateway node computes $A_{21} = h(A_2^{**}\|A_8^*\|A_4^*)$ and sends the message $M_4 = \langle A_{17}, A_{21}\rangle$. In addition, GW_j computes the session key $sk = r_g \cdot A_{19}$.

Step AP4. After getting the message M_4 from GW_j, the user U_i computes $A_4^* = A_6 \oplus A_2^*$, $A_{21}^{**} = h(A_2^*\|A_8^*\|A_4^*)$ and checks $A_{21}^* \stackrel{?}{=} A_{21}$. If it is true then the user computes the session key $sk = r_u \cdot A_{17}$. The login and authentication mechanism is depicted in Fig. 2

3.7. Password renewal phase

Suppose the existing user wish to renew the password for retaining the security, there is a need for a procedure. The following are the steps to describe this phase.

Step PP1. The user U_i inputs SC into the terminal (card reader) and enters ID_i, PW_i with the biometric B_i.

Step PP2. SC computes $b_i = H(B_i)$, $HID_i = h(ID_i||b_i)$ and $HPID = h(HID_i||PW_i)$. SC also computes $A_5^* = h(HID_i||HPID_i) \cdot P$ and checks whether $A_5^* \stackrel{?}{=} A_5$. If it is not satisfied then SC aborts the session, otherwise SC permits U_i to enter the new password.

Step PP3. User enters his new password PW_i^{new} into SC.

Step PP4. Then, SC computes the following

$$HPID^{new} = h(HID_i||PW_i^{new})$$
$$A_1^{new} = h(HID_i||HPW_i^{new}) \cdot P$$
$$A_3^{new} = (A_3 \oplus A_1) \oplus A_1^{new}$$
$$A_5^{new} = h(HID_i||HPID_i^{new}) \cdot P$$

Smart card replaces old A_3 and A_5 with new A_3^{new} and A_5^{new}. This process also depicted in the Algorithm 3.

3.8. Sensor node addition phase

The sensor node lapses its functionality when it is hacked by an attacker or it lost the capacity of its battery. And hence, a new sensor node SN_k^{new} needs to be installed in the existing MWSN. In this phase, we present a procedure for install a new sensor node into the system. The procedure is described as below.

SA selects a new identity $SN_{ID_k}^{new}$ for the sensor node SN_k^{new}, computes a secret value $S_{SN_k} = h(S_{SA}||SN_{ID_k}^{new})$ and stores $\langle SN_{ID_k}, S_{SN_k}\rangle$ into the memory of the gateway GW_j and SN_k.

Algorithm 3 Password renewal process

1: The user U_i inputs SC and enters ID_i, PW_i and B_i
2: Smart card SC computes $b_i = H(B_i)$, $HID_i = h(ID_i||b_i)$ and $HPID = h(HID_i||PW_i)$
3: SC also computes $A_5^* = h(HID_i||HPID_i) \cdot P$
4: **if** $(A_5^* == A_5)$ **then**
5: SC permits U_i to enter the new password.
6: User enters his new password PW_i^{new} into SC
7: SC computes $HPID^{new} = h(HID_i||PW_i^{new})$, $A_1^{new} = h(HID_i||HPW_i^{new}) \cdot P$, $A_3^{new} = (A_3 \oplus A_1) \oplus A_1^{new}$, $A_5^{new} = h(HID_i||HPID_i^{new}) \cdot P$
8: SC replaces old A_3 and A_5 with new A_3^{new} and A_5^{new}
9: **else**
10: SC aborts the session
11: **end if**

4. Security analysis

In this section the correctness of the proposed protocol is presented using the formal method BAN logic for authentication and the informal arguments for several security attacks.

4.1. Formal proof using BAN logic

The notion of BAN logic was first introduced by Burrows, Abadi and Needham in 1989. The BAN logic is a logical methodology for providing the formal proof of correctness authentication property [36]. The notion of a 'fresh message', shared key and all public parameters can be modelled using the BAN logic. The statements in the challenge–response protocols are usually idealized and the truth of a statement is based on the belief of an entity for the BAN logic. A valid proof of correctness can be stated using the proofs in BAN logic, with respect to the assumptions [25,37]. However, it is doubtful that with the analysis of the logic and that it will prohibit all possible attacks. BAN logic is usually applied in the scheme of an authentication protocol as a part of the formal method in the design process which can prevent the flaws [34,35,38].

4.1.1. Notations

Common notations with their syntax of the BAN logic used in the literature are presented in this section. Not all symbols are detailed here, only the symbols used for the analysis. Remaining are found in the base paper [36].

- A **believes** X: $A \mid\equiv X$. In the sense that A trusts that the formula X has the truth value true in the current run of the protocol.
- A **sees** X: $A \triangleleft X$. In the sense that, if somebody sends the message containing the formula X, then A sees the formula X, perhaps after doing some operation.
- A **once said** X: $A \mid\sim X$. The principal A sent a message at some time which consist of the statement X. It is unknown that X has been send in the current run of the protocol or long ago. The principal believed that A once said X.
- A has **control** over X: $A \mid\Rightarrow X$. The principal A has control over the formula X and should have believed the statement formula.
- A and B **share** a secret key K: $A \overset{K}{\longleftrightarrow} B$. It is believed that the two principals share the secret key K for their secret communication and none other than the two knows K.
- X is **fresh**: $\sharp(X)$. The statement X is created recently. The statement X is not used earlier and it can be a nonce.
- A and B **share** a secret Y : $A \overset{Y}{\rightleftharpoons} B$. The statement Y is a shared secret between the two principals A and B. They can use it to prove them self later to each other.

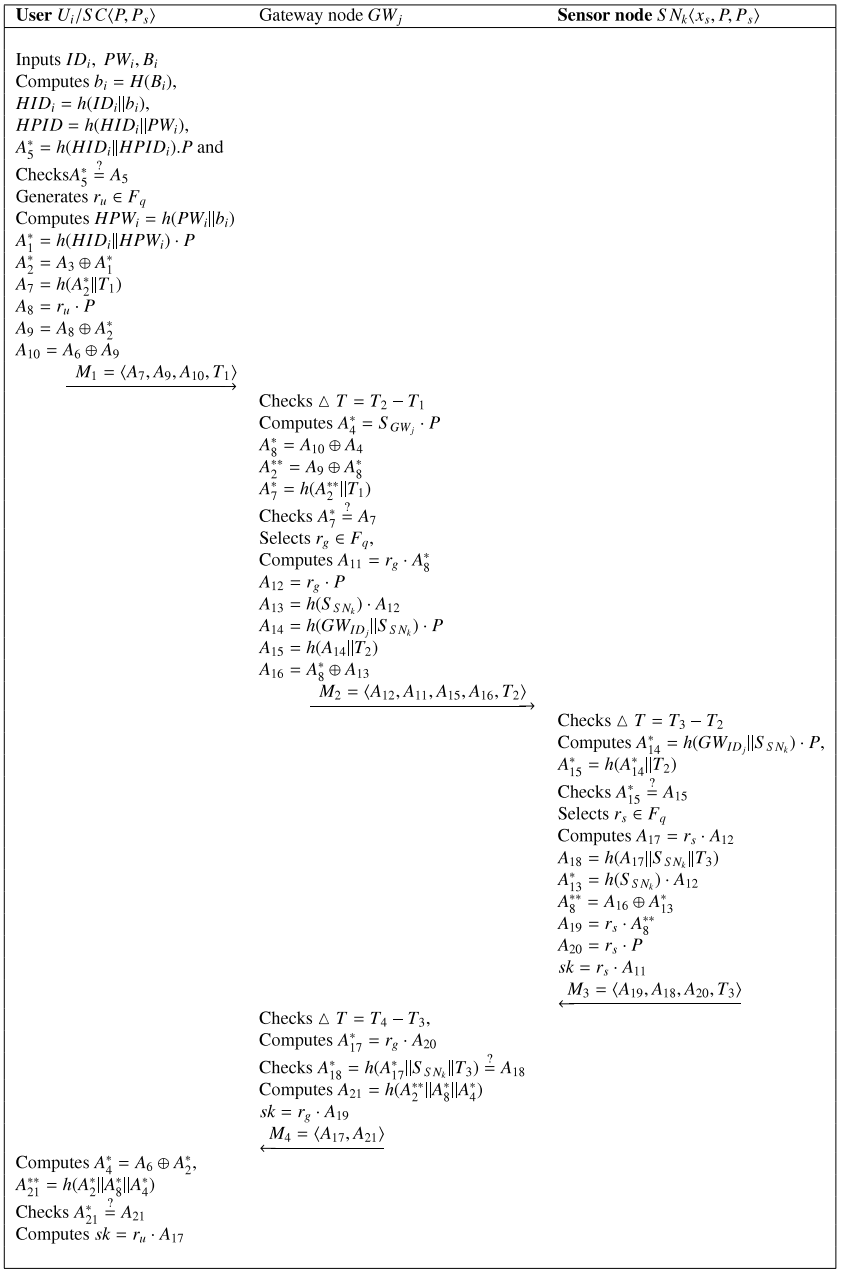


Fig. 2. Login-authentication phase.

4.1.2. Rules of inference

The most common used rules and their usage are given in this subsection. The overview not provides the entire, but is enough to carry out the analysis.

Message-meaning rule: When A trusts that the statement Y is shared with B and A sees X combined with Y, then A trusts that B once said X.

$$R_1 : \frac{A \mid\equiv B \overset{Y}{\rightleftharpoons} A,\ A \triangleleft \langle X\rangle_Y}{A \mid\equiv B \mid\sim X}$$

For random values

$$R_2 : \frac{A \text{ Chooses random } X}{A \mid\equiv \sharp X}$$

Jurisdiction rule: If A trusts that B has control over the statement X and A trusts B trusts X then A trusts that X has the truth.

$$R_4 : \frac{A \mid\equiv B \mid\Rightarrow X,\ A \mid\equiv B \mid\equiv X}{A \mid\equiv X}$$

Nonce-verification rule: If P trusts that X is fresh and that B once said X, then A believes that B believes X.

$$R_3 : \frac{A \mid\equiv \sharp X,\ A \mid\equiv B \mid\sim X}{A \mid\equiv B \mid\equiv X}$$

Freshness rule: If one component of a statement is recent, then the complete statement is also recent:

$$R_5 : \frac{A \mid\equiv \sharp X}{A \mid\equiv \sharp (X,\ Y)}$$

Session key rule: If A trusts that the statement formula X is fresh and A trusts B trust X, that is an essential component of the session key, then A trust that he or she shares the session key K

with B.

$$R_6 : \frac{A \mid\equiv \sharp X, A \mid\equiv B \mid\equiv X}{A \mid\equiv A \overset{K}{\rightleftharpoons} B}$$

The following can also be generalized to more than two statements. A compound statement can be built if a principal has trust in all the atomic statements.

$$R_7 : \frac{A \mid\equiv X,\ \ A \mid\equiv Y}{A \mid\equiv (X,\ Y)}$$

Some more rules on sub-component messages.

$$R_8 : \frac{A \mid\equiv B \mid\sim (X,\ Y)}{A \mid\equiv B \mid\sim X}$$

$$R_9 : \frac{A \mid\equiv B \mid\equiv (X,\ Y)}{A \mid\equiv B \mid\equiv X}$$

$$R_{10} : \frac{A \mid\equiv (X,\ Y)}{B \mid\equiv X}$$

$$R_{11} : \frac{A \lhd (X,\ Y)}{A \lhd X}$$

4.1.3. Idealized form of our protocol

Before the proper analysis, the proposed protocol requires to be idealized in the BAN logic.

$$U \rightarrow GW_j : M_1 = \{\langle P||T_1\rangle_{h(HID||S_{GW_j})},\ \langle P||h(HID||S_{GW_j})\rangle_{(r_u||P)},\ \langle r_u||P\rangle_{(\ GW_j||P)},\ T_1\}$$

$$GW_j \rightarrow SN_k : M_2 = \{(r_g \cdot P), (r_u \cdot r_g \cdot P), \langle h(GW_j||P||T_2)\rangle_{S_{SN_k}}, \langle (r_u \cdot P), (r_g \cdot P)\rangle_{(S_{SN_k})}, T_2\}$$

$$SN_k \rightarrow GW_j : M_3 = \{(r_s \cdot r_u \cdot P), \langle (r_s \cdot P||T_3)\rangle_{(r_g \cdot P||S_{SN_k})}, T_3\}$$

$$GW_j \rightarrow U : M_4 = \{\langle r_s \cdot r_g \cdot P||S_{GW_j} \cdot P||r_u \cdot P\rangle_{h(HID||S_{GW_j})\cdot P}\}$$

4.1.4. Security goals

The following are the list of security goals needed to be achieve.

$$G1 : GW_j \mid\equiv GW_j \overset{h(HID||S_{GW_j})}{\rightleftharpoons} U$$

$$G2 : SN_k \mid\equiv h(GW_j||P||T_2)$$

$$G3 : SN_k \mid\equiv GW_j \overset{sk}{\rightleftharpoons} SN_k$$

$$G4 : GW_j \mid\equiv GW_j \overset{sk}{\rightleftharpoons} SN_k$$

$$G5 : U_i \mid\equiv GW_j \overset{sk}{\rightleftharpoons} U_i$$

4.1.5. Initial assumptions

With respect to the security goals mentioned, some initial assumptions are listed below.

$$AS1 : GW_j \mid\equiv GW_j \overset{P||S_{GW_j}}{\rightleftharpoons} U$$

$$AS2 : GW_j \mid\equiv \sharp r_u$$

$$AS3 : GW_j \mid\equiv U \mid\Rightarrow r_u$$

$$AS4 : GW_j \mid\equiv \sharp T_1$$

$$AS5 : SN_k \mid\equiv GW_j \overset{S_{SN_k}}{\rightleftharpoons} SN_k$$

$$AS6 : SN_k \mid\equiv \sharp T_2$$

$$AS7 : SN_k \mid\equiv GW_j \mid\Rightarrow (GW_j||P)$$

$$AS8 : SN_k \mid\equiv GW_j \mid\Rightarrow (r_g)$$

$$AS9 : SN_k \mid\equiv \sharp(r_g)$$

$$AS10 : GW_j \mid\equiv GW_j \overset{(r_g \cdot P||S_{SN_k})}{\rightleftharpoons} SN_k$$

$$AS11 : GW_j \mid\equiv \sharp T_3$$

$$AS12 : GW_j \mid\equiv \sharp r_s$$

$$AS13 : U_i \mid\equiv \sharp r_s$$

$$AS14 : U_i \mid\equiv GW_j \mid\Rightarrow (S_{GW_j} \cdot P)$$

$$AS15 : U_i \mid\equiv \sharp r_g$$

4.1.6. Proof of correctness

Set of logical rules are applied on the idealized protocol together with the initial assumptions to obtain the required security goals.

According to the message M_1 and using seeing rule, we get

$$ST_1 = GW_j \lhd \{\langle P||T_1\rangle_{h(HID||S_{GW_j})},\ \langle P||h(HID||S_{GW_j})\rangle_{r_u||P},\ \langle r_u||P\rangle_{S_{GW_j}||P},\ T_1\}.$$

Using seeing rule for components we get
$ST_2 = GW_j \lhd \langle P||T_1\rangle_{h(HID||S_{GW_j})}$
$ST_3 = GW_j \lhd \langle P||h(HID||S_{GW_j})\rangle_{r_u||P}$
$ST_4 = GW_j \lhd \langle r_u||P||T_1\rangle_{S_{GW_j}||P}$
Using message meaning rule for ST_4 with the assumption $AS1$, we get
$ST_5 = GW_j \mid\equiv U \mid\sim (r_u||P||T_1)$.
Applying nonce verification rule on ST_5 and using the assumption $AS2$, we get
$ST_6 = GW_j \mid\equiv U \mid\equiv (r_u||P||T_1)$.
Applying this for each component, we get
$ST_7 = GW_j \mid\equiv U \mid\equiv (r_u||P)$.
Using jurisdiction rule with assumption $AS3$, we get
$ST_8 = GW \mid\equiv (r_u||P)$.
Using assumption $AS2$ and ST_7 with session key rule, we get
$ST_9 = GW_j \mid\equiv GW_j \overset{(r_u||P)}{\rightleftharpoons} U$.
Applying message meaning followed that nonce verification and jurisdiction rules successively on ST_9 with the assumptions $AS4$ and $AS3$, we get
$ST_{10} = GW_j \mid\equiv U \mid\equiv h(HID||S_{GW_j})$ and $ST_{11} = GW_j \mid\equiv h(HID||S_{GW_j})$.
At last, using the session key rule for ST_{10} with the assumption $AS4$, we get
$G1 = GW_j \mid\equiv GW_j \overset{h(HID||S_{GW_j})}{\rightleftharpoons} U$, which is our **goal** $G1$.

According M_2 and using seeing rule, we get
$ST_{12} = SN_k \lhd \{(r_g \cdot P), (r_u \cdot r_g \cdot P), \langle h(GW_j||P||T_2)\rangle_{(S_{SN_k})}, \langle (r_u \cdot P), (r_g \cdot P)\rangle_{(S_{SN_k})}, T_2\}$.
Applying same for the components, we get
$ST_{13} = SN_k \lhd \{\langle h(GW_j||P||T_2)\rangle_{S_{SN_k}}\}$ and $ST_{14} = SN_k \lhd \{\langle (r_u \cdot P), (r_g \cdot P)\rangle_{(S_{SN_k})}, T_2\}$.

Using message meaning rule on S_{13} with the assumption $AS5$, we get
$ST_{15} = SN_k \mid\equiv GW_k \mid\sim h(GW_j||P||T_2)$.
Using nonce verification rule and assumption $AS6$ in ST_{15}, we get
$ST_{16} = SN_k \mid\equiv GW_j \mid\equiv h(GW_j||P||T_2)$.
Applying jurisdiction rule on ST_{17} with assumption $AS7$, we get
$G2 = SN_k \mid\equiv h(GW_j||P||T_2)$ and which is our **goal** $G2$.

Successively applying message meaning followed by nonce verification and jurisdiction rules on ST_{14} with the assumptions $AS5$, $AS6$ and $AS8$, we get
$ST_{18} = GW_j \mid\equiv U \mid\equiv r_g \cdot P$ and $ST_{19} = GW_j \mid\equiv r_g \cdot P$.
Using session key rule and the assumption $AS9$ on ST_{18}, we get

$ST_{20} = SN_k \mid\equiv GW_j \overset{r_g \cdot P}{\rightleftharpoons} SN_k$ and hence obtain our **goal three** $G3 = SN_k \mid\equiv GW_j \overset{sk}{\rightleftharpoons} SN_k$ because, $r_g \cdot P$ is an essential parameter of the session key sk.

Using seeing rule on M_3, we get
$ST_{21} = GW_j \triangleleft \{(r_s \cdot r_u \cdot P), \langle (r_s \cdot P || T_3) \rangle_{(r_g \cdot P)}, T_3\}$.
Applying seeing rule for components we get
$ST_{22} = GW_j \triangleleft \langle (r_s \cdot P || | T_3) \rangle_{(r_g \cdot P)}$.
Using message meaning rule for ST_{22} together with $AS10$, we get
$ST_{23} = GW_j \mid\equiv SN_k \mid\sim (r_s \cdot P || T_3)$.
Applying nonce verification rule on ST_{23} and using the assumption $AS11$, we get
$ST_{24} = GW_j \mid\equiv SN_k \mid\equiv r_s \cdot P$.
Using jurisdiction rule with assumption $AS12$, we get
$ST_{25} = GW \mid\equiv (r_s \cdot P)$.
Using assumption $AS12$ and ST_{24} with session key rule, we get
$G4 = GW_j \mid\equiv GW_j \overset{sk}{\rightleftharpoons} SN_k$, which is our **goal** $G4$.

Using seeing rule on M_4, we get

$ST_{26} = U_i \triangleleft \{\langle (r_s \cdot r_g \cdot P) || (S_{GW_j} \cdot P) || (r_u \cdot P) \rangle_{h(HID || S_{GW_j}) \cdot P}\}$.
Applying message meaning rule and nonce verification rule on ST_{26} with the assumptions $AS13$ and $AS15$, we get
$ST_{27} = U_i \mid\equiv GW_j \mid\equiv (r_s \cdot r_g \cdot P) || (S_{GW_j} \cdot P)$.
Using jurisdiction rule and the assumption $AS14$ in S_{27}, we get
$S_{28} = U_i \mid\equiv (r_s \cdot r_g \cdot P) || (S_{GW_j} \cdot P)$.
Also applying the rule for the components, we get
$S_{29} = U_i \mid\equiv GW_j \mid\equiv (r_s \cdot r_g \cdot P)$ from S_{27}. As $(r_s \cdot r_g \cdot P)$ is an essential component in the construction of the key sk for U_i, using session key rule and the assumption $AS13$ in ST_{29}, we get our **final goal** $G5 = U_i \mid\equiv GW_j \overset{sk}{\rightleftharpoons} U_i$.

The obtained proofs for the mentioned security goals in BAN logic confirms the correctness of the proposed protocol against mutual authentication property.

4.2. Informal security analysis

The analysis of the proposed protocol for various security threats is carried out in this section with informal argument.

Proposition 1. *The proposed protocol provides user anonymity.*

Proof. All the message communications M_1, M_2, M_3 and M_4 of the proposed protocol, the user identity ID_i is secured by using cryptographic one-way hash function. In addition, the user submits his ID_i to SA after masked with his/her biometric b_i using hash function in the registration phase and hence insider also cannot get the user's identity. If an adversary tries to guess the user ID_i from the intermediate messages HID_i, A_3 and A_5. As they are masked using hash function with additional unknown secrets b_i, S_{GW_j} and $HPID_i$ respectively, checking the correctness of the guessed ID_i is computationally infeasible. Thus, the attacker has no way to get or guess the user's identity ID_i. Thus, the proposed protocol provides user anonymity. □

Proposition 2. *The proposed protocol provides strong protection against the off-line password guessing attack.*

Proof. The user's password PW_i is secured using one way hash function in all the communicated messages. The insider cannot get the user's identity since the user submits his PW_i to SA after masked with his/her biometric by using hash function in the registration phase. If an attacker tries to guess the user's password PW_i from the intermediated message HID_i, A_3 and A_5. Checking the correctness of the guessed PW_i is computationally infeasible since the masking of PW_i requires additional secrets b_i, S_{GW_j} and $HPID_i$ respectively while using hash function. Thus attacker has no options to get or guess the password PW_i and making the proposed protocol strong protection against the off-line password guessing attack. □

Proposition 3. *The proposed protocol is resilient against privileged insider attack.*

Proof. A privileged insider (A) can have access to the information about the user U_i at SA side. Even though the attacker has all the registration details such as $\langle HID_i, HPW_i, GW_{ID_j} \rangle$, he cannot guess the user identity ID_i. Because it is protected with the user's password PW_i and the biometric b_i, which cannot be calculated from HID_i, HPW_i and GW_{ID_j}. □

Proposition 4. *The proposed protocol is resilient against stolen smart card attack.*

Proof. If an attacker A steels all the data stored in the smart card SC of U_i after registration. Even though the attacker has all the smart card details such as $\langle A_3, A_5 A_6, h(\cdot), P \rangle$, he cannot guess the user identity ID_i. Because it is protected with the gateway's master secret S_{GW_j}, which cannot be calculated from A_3, A_5, A_6 and P □

Proposition 5. *The proposed protocol resists user impersonation attack.*

Proof. Suppose A be a honest user possesses the smart card $SC_A = \langle A_3^d, A_5^d, A_6^d, h(\cdot), P \rangle$ and tries to impersonate another legal user U_i. (A) constructs the login message $M_1^d = \langle A_7^d, A_9^d, A_{10}^d, T_1 \rangle$ where

$$
\begin{aligned}
HPW_i^d &= h(PW_i^d || b_i^d) \\
A_1^d &= h(HID_i^d || HPW_i^d) \cdot P \\
A_2^d &= A_3^d \oplus A_1^d \\
A_7^d &= h(A_2^d || T_1) \\
A_8 &= r_u \cdot P \\
A_9^d &= A_8 \oplus A_2^d \\
A_{10}^d &= A_6^d \oplus A_9^d
\end{aligned}
$$

and sends M_1^d to the gateway node GW_j.

After receive the login request, the gateway node GW_j checks the time delay $\triangle T = T_2 - T_1$, where T_2 is the current timestamp at GW_j node. As T_1 is valid time, $\triangle T$ will be an acceptable time delay, hence the GW_j starts to compute the following

$$
\begin{aligned}
A_4^* &= S_{GW_j} \cdot P \\
A_8^* &= A_{10}^d \oplus A_4^* \\
A_2^{**} &= A_9^d \oplus A_8^* \\
A_7^* &= h(A_2^{**} || T_1)
\end{aligned}
$$

and checks whether $A_7^* \overset{?}{=} A_7^d$. This will not be satisfied, because $A_8^* \neq A_8$, which implies $A^{**} \neq A_2^d$. Hence, proposed protocol withstands user impersonation attack. □

Proposition 6. *The proposed protocol is robust against gateway node impersonation attack.*

Proof. As the message $M_2 = \langle A_{12}, A_{11}, A_{15}, A_{16}, T_2 \rangle$ from gateway node GW_j to the sensor node SN_k contains $A_{15}^* = h(A_{14}^* || T_2)$, in which $A_{14}^* = h(GW_{ID_j} || S_{SN_k}) \cdot P$ is made up of the two secret parameters GW_{ID_j} and S_{SN_k}. But, guessing both the secret parameters simultaneously is computationally infeasible. Also, the message $M_4 = \langle A_{17}, A_{21} \rangle$ from GW_j to the user U_i contains

$A_{21} = h(A_2^{**} \| A_8^* \| A_4^*)$, in which $A_2 =$ and $A_4 =$ are made up of the secret parameters HID_i and S_{GW_j} respectively. It is computationally difficult to guess both the secret components simultaneously. Thus, the proposed protocol is secure from gateway node impersonation attack. □

Proposition 7. *The proposed protocol withstands the sensor node impersonation attack.*

Proof. Suppose the attacker intercept the authentication message $M_2 = \langle A_{12}, A_{11}, A_{15}, A_{16}, T_2 \rangle$ from the node GW_j and attempts to impersonate the node SN_k. Therefore, the attacker needs to compute the forged message $M_3 = \langle A_{19}^d, A_{18}^d, A_{20}^d, T_3 \rangle$, where

$A_{17}^d = r_s^d \cdot A_{12}$

$A_{18} = h(A_{17}^d || S_{SN_k} || T_3)$

$A_{13}^* = h(S_{SN_k}) \cdot A_{12}$

$A_8^{**} = A_{16} \oplus A_{13}^*$

$A_{19}^d = r_s^d \cdot A_8^{**}$

$A_{20} = r_s^d \cdot P$

But, these computations require the secret parameter S_{SN_k} which is mysterious to the attacker. Therefore, the attacker cannot impersonate the sensor node SN_k. □

Proposition 8. *The proposed protocol is robust against replay attack.*

Proof. Adversaries commonly use replay attacks to imitate a legitimate user. We suppose that the adversary captures the old messages and transmits the captured messages to the receiver without any modification in the current session. The protocol uses a system's timestamp to verify communication delay and hence rejects the messages sent by an adversary, as the communication delay calculated from old timestamps would exceed the allowable delay. Our proposed scheme thus withstands replay attacks. □

Proposition 9. *The proposed protocol is secure from untraceability attack.*

Proof. To execute this attack, the adversary usually collects minimum of two different sessions login authentication messages and attempts to find a relation between the messages. The attacker infers that the messages belong to a single user, if they happen to the same. Nevertheless, in the proposed scheme the attacker cannot track any single user by collecting one or more public messages from distinct sessions. The timestamp and random number used in each session are different and hence the login messages of each session differ from one another. Suppose the attacker collects the login message $M_1 = \langle A_7, A_9, A_{10}, T_1 \rangle$, which involves the random number r_u and the timestamp T_1. As the timestamp and random number are freshly generated session by session, the login messages of each session are also different. Also, If the attacker further catches response message of a legitimate sensor node and attempts to track the sensor node, it becomes difficult due to the freshness of random numbers and timestamps. □

Proposition 10. *The proposed protocol resist the off-line sensor-node-identity guessing attack.*

Proof. If an attacker tries to guess the sensor node S_k identity SN_{ID_k} in off-line mode, during the execution of the protocol he captures all the public messages. Note that ID_k is not inbuilt in the smart card; thus, attacker cannot get SN_{ID_k} from a stolen-smart card. Nevertheless, the attacker can neither extract nor guess SN_{ID_k} from public messages, because none of the messages M_1, M_2, M_3 and M_4 contains the identity of the sensor node. □

Proposition 11. *The proposed protocol is resilient against session key computation attack.*

Proof. In general, the encryption of the messages communicated over public channels, between entities uses the session key computed in the protocol. The freshness is the core characteristic of a session key, implying that the session key must be different for each session. The entities U_i, $GWN_j and SN_k$ in the proposed protocol agree upon the session key $sk = r_u r_g r_s \cdot P$, that depends on the secret random numbers r_u, r_g and r_s. Therefore, the session key sk is generated freshly. Also, it is not possible to construct the session key sk as the attacker does not know the secret values r_u, r_g and r_s. Thus, proposed protocol withstands session key computation attack. □

Proposition 12. *The proposed protocol is robust against denial of service attack.*

Proof. The denial-of-services (DoS) attacks are highly probable because wireless sensor networks are resource constrained. DoS attacks are usually executed in multiple network layers such as Transport, Routing, Link and Physical layers. As the proposed protocol is designed based on the request–response communication principle, DoS attack is not probable. We have mitigated the risk of flooding that used to affect the proposed authentication protocol and the user. The user ever gets a rejection or confirmation message from the sensor node so that the obtained response message is an authentic one and not a DoS attack. Also, the involvement of timestamps into the protocol mitigates any consequential request. Hence, our protocol is robust against DoS attacks. □

Proposition 13. *The proposed protocol achieves perfect forward secrecy.*

Proof. Suppose an attacker gets all the old used session key, still using the known information it is not probable for an attacker to find the current session key and all future session keys. Because $sk = h(r_u\ r_g\ r_s \cdot P)$ used three distinct random numbers r_u, r_g and r_s. The adversary cannot correctly guess these random numbers simultaneously. Thus, our protocol achieves perfect forward secrecy. □

Proposition 14. *The proposed protocol establishes a session key after three party mutual authentication.*

Proof. The objective of the user authentication protocol is to construct a session key such that every of the entities can get through securely with others. The our protocol constructs a session key sk between the sensor node, gateway node and user followed by the mutual authentication. Thus, the proposed protocol possesses benefit of session key negotiation. □

5. Efficiency evaluation and comparison

In this section we show the efficiency of our protocol by comparing it with the related other protocols in the aspect of securities, functionality requirements, computational cost, communication cost and storage cost. Our protocol efficiency is measured and compared and the results are depicted in different tables and charts.

Table 1
Comparison of functionality requirements and security threats.

Protocol	Ro_1	Ro_2	Ro_3	Ro_4	Ro_5	Ro_6	Ro_7	Ro_8	Ro_9	Ro_{10}	Ro_{11}	Ro_{12}	Ro_{13}
Li et al. [26]	○	○	×	○	×	○	○	○	×	○	×	○	×
Wu et al. [27]	○	×	○	×	○	○	×	×	○	×	○	○	×
Yeh et al. [39]	×	○	×	×	○	○	×	○	×	×	×	○	×
He et al. [25]	○	○	○	○	×	○	×	○	○	○	○	×	×
Shi et al. [40]	○	×	×	×	○	×	○	○	○	○	×	○	×
Khan and Kumari [24]	○	×	×	×	○	○	×	○	○	×	○	○	×
Kumar et al. [23]	○	×	×	×	×	○	×	○	○	○	○	×	×
Proposed	○	○	○	○	○	○	○	○	○	○	○	○	○

Ro_1 : Overcomes the problem of untraceability, Ro_2 : Withstands the password guessing attack, Ro_3 : Overcomes the identity guessing attack, Ro_4 : Overcomes the stolen smartcard attack, Ro_5 : Strong against privileged insider attack, Ro_6 : Overcomes the session key attack, Ro_7 : Withstands the impersonation attack, Ro_8 : Withstand replay attack, Ro_9 : Achieves the benefit of dynamic node addition, Ro_{10} : Achieves mutual authentication and includes its benefits, Ro_{11} : Achieves sensor node anonymity, Ro_{12} : Provides forward secrecy, Ro_{13} : Provides hardware implementation, ○ : Yes, × : No.

Table 2
Computational cost comparison.

Protocol	C_1	C_2	C_3	C_4	C_5
Li et al. [26]	$7T_h + 6T_s$	$5T_h + 2T_s$	$6T_h + 2T_s$	$18T_h + 10T_s$	96 ms
Wu et al. [27]	$6T_h + 5T_s$	$5T_h + T_s$	$10T_h$+$2T_s$	$21T_h + 8T_s$	80.1 ms
Yeh et al. [39]	$2T_h + 4T_p$	$3T_h + 2T_p$	$5T_h + 2T_p$	$10T_h + 8T_p$	8.376 ms
He et al. [25]	$3T_h + 5T_s$	$T_h + 2T_s$	$4T_h + 3T_s$	$8T_h + 10T_s$	91 ms
Shi et al. [40]	$4T_h + T_p$	$4T_h + 2T_p$	$6T_h + 3T_p$	$14T_h + 6T_p$	9.652 ms
Khan and Kumari [24]	$9T_h + 2T_s$	$7T_h$	$6T_h + T_s$	$22T_h + 3T_s$	37.1 ms
Kumar et al. [23]	$T_h + 3T_s$	$T_h + 2T_s$	$4T_h + 2T_s$	$6T_h + 7T_s$	63.9 ms
Proposed	$6T_h + 6T_p$	$4T_h + 5T_p$	$8T_h + 3T_p$	$18T_h + 14T_p$	15.188 ms

C_1 : Computation cost for Gateway node, C_2 : Sensor node's computation cost C_3 : User's computation cost, C_4 :Total cost, C_5 : Total running time.

Table 3
Communication cost comparison.

Protocol	Co_1	Co_2	Co_3	Co_4
Li et al. [26]	512	256	512	1280
Wu et al. [27]	1280	2048	1024	4352
Yeh et al. [39]	640	1792	1152	3584
He et al. [25]	256	256	512	1024
Shi et al. [40]	1024	4032	1344	6400
Khan and Kumari [24]	1536	1024	768	3328
Kumar et al. [23]	256	256	256	768
Proposed protocol	2304	960	1152	4416

Co_1 : Gateway node's communication cost, Co_2 : Communication cost of the sensor node, Co_3 : User's communication cost, Co_4 : Total cost.

5.1. Security threats and functionality requirements

Our protocol overcomes many security threats and possesses several functionality requirements, that make the protocol more strong. Table 1 shows a thorough comparison of our protocol with the existing protocols. The protocols in [23,24,27,40] are vulnerable to password guessing attack and stolen smart card attack. However, the protocols in [25,26,39] do not provide sensor node anonymity.

5.2. Computational cost comparison

In medical wireless sensor networks, user authentication schemes are developed as light-weight in the perspective of computation cost due to energy constraint [27,35,41]. The proposed scheme applies hash function and elliptic curve cryptosystem, which are light-weight compared to other operations, including public key cryptographic functions and symmetric key encryption/decryption. We have used the running time of the hash function and symmetric key encryption/decryption as are $T_h \approx 0.5$ ms and $T_{e/d} \approx 8.7$ ms, respectively based on the existing information. Running time for elliptic curve point multiplication is $T_p \approx 0.442$ ms. In Table 2, the computational cost for gateway, sensor node and the user of the proposed protocol and that of existing protocols is depicted. The computational capacity of sensor nodes is much less than that of the gateway node. To provide better efficiency, the computational cost of the sensor nodes must be reduced. Our protocol , as shown in Table 2 and Fig. 3 is efficient compared with the protocols in [23–27]

Table 4
Storage cost comparison.

Protocol	Storage cost (in bits)
Li et al. [26]	1792
Wu et al. [27]	1280
Shi et al. [40]	1536
He et al. [25]	1280
Yeh et al. [39]	1536
Khan and Kumari [24]	1792
Kumar et al. [23]	1280
Proposed protocol	1280

5.3. Communication cost comparison

The communication cost is regarded as the total number of bits required for transmitting messages in the login-authentication phase. Table 3 shows that the communication cost comparison of our protocol with that of the existing similar protocols. We suppose that the lengths of the password, identity, the hash function(SHA-512) output hash value and random number are each 512 bits. The length of the output of symmetric encryption (AES) and ECC point are is 256 bits and 320 bits respectively. In the proposed protocol, user sends two ECC points and one hash value to the gateway node which is of 640 + 512 = 1152 bits, the gateway node sends 3ECC points with 1 hash value (960 + 512 = 1472 bits) to the sensor node and 1ECC point with 1 hash value (320 + 512 = 832 bits) to the user and the sensor node transmits 3ECC points (960 bits). Therefore, the total communication cost is 4416 bits. The communication cost for different schemes are presented in Table 3. The Table shows that the communication cost for the protocol in [40] is more than other protocols and the proposed protocol requires the communication cost that nearly equal to the cost required by the other protocols in [24,27,39]. Although the protocols in [23,25,26] require less communication cost than ours' their protocol fails to satisfy the security functionalities such as identity guessing, privileged insider, impersonation attacks and so on.

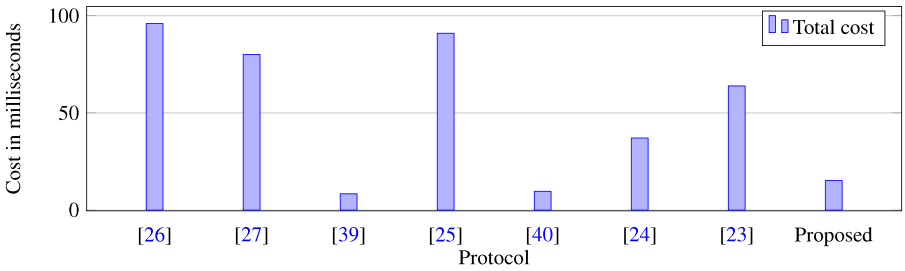


Fig. 3. Comparison of total cost for different protocols.

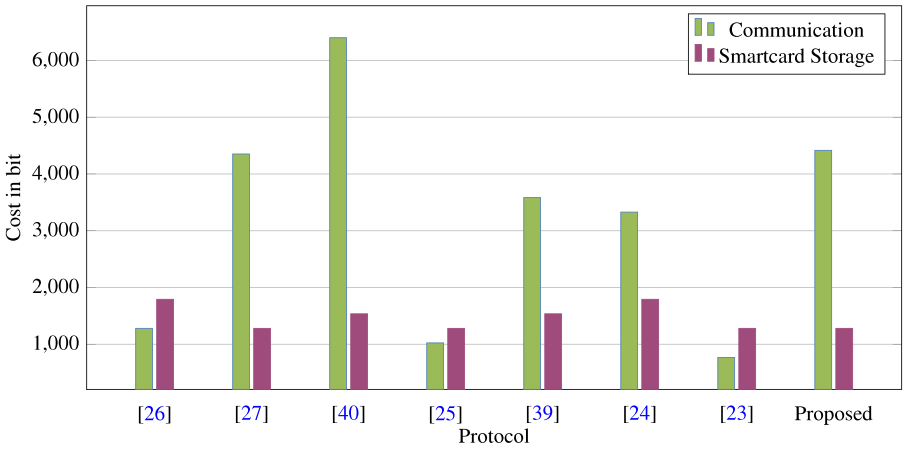


Fig. 4. Comparison of total communication and storage cost for different protocols.

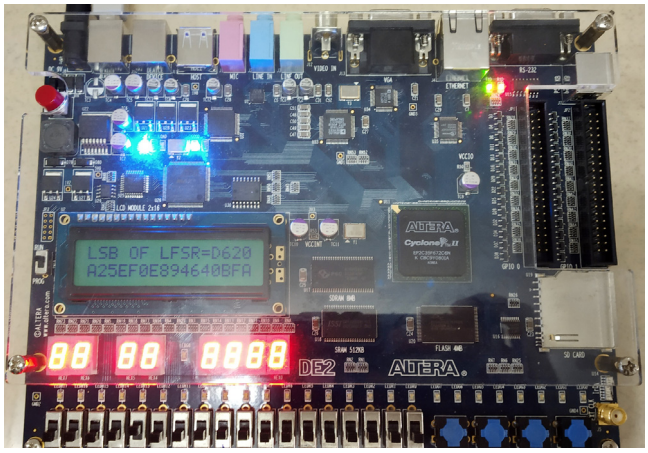


Fig. 5. LSB of the linear feedback shift register.

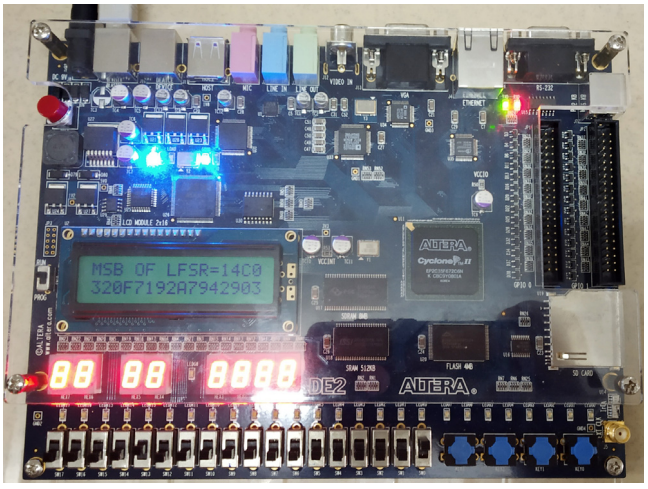


Fig. 6. MSB of the linear feedback shift register.

5.4. Storage cost comparison

Usually sensor nodes and smart card have relatively less storage capacity than the gateway node. It is essential that the storage cost of the sensor node and smart card are need to be reduced. We assume that the lengths of the random number, output of the hash function, password and identity are each 512 bits and length of the cipher text is 256 bits. The comparison of storage cost for several protocols is shown in Table 4 . It is noticed that the schemes in [24,26,39,40] need more storage cost than that of the other schemes. The smart card storage of the proposed protocol and that of the protocols in [23,25,27] are same. We have presented communication and smart card storage overhead in Fig. 4.

5.5. VLSI Hardware implementation results

Linear Feedback Shift Register (LFSR) plays a key role to generate the random numbers in the high end security applications. There are two different LFSR architectures are available namely Fibonacci and Galois type LFSR [42–44]. In that, Fibonacci LFSR is highly suitable for the hardware implementation of our scheme. Sutter et al. [45] proposes a high speed point multiplier for ECC using digit-serial binary field and took the analysis for various NIST recommended fields. Lopez et al. [46] describes a Montgomery multiplier method based algorithm for elliptic curve scalar multiplication without any pre-computations. In [47], Lai

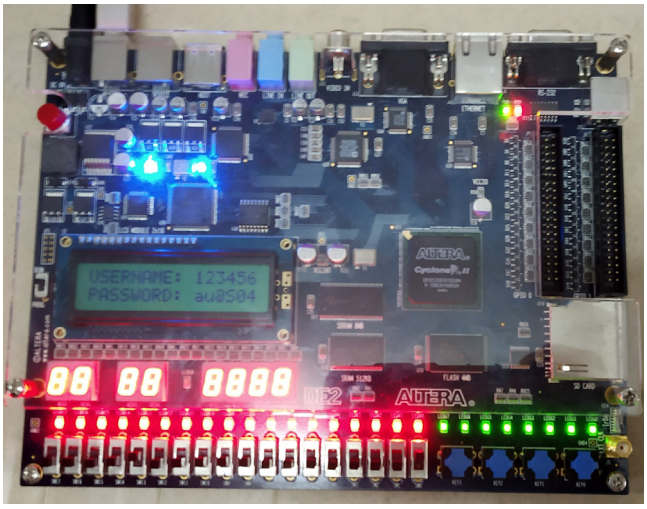


Fig. 7. Login and authentication for valid user.

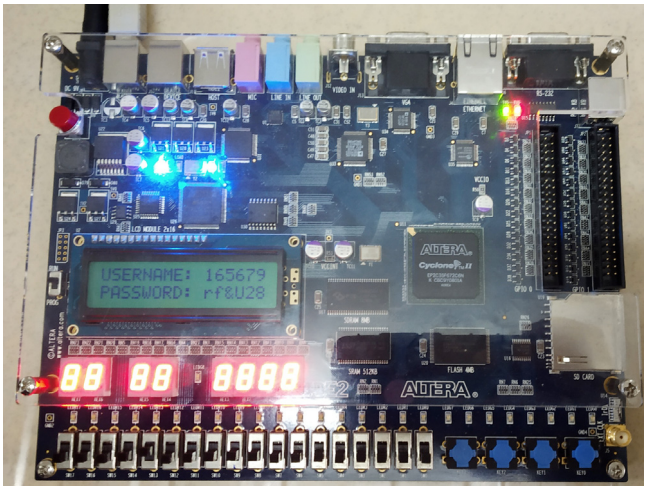


Fig. 8. Login and authentication for fake user.

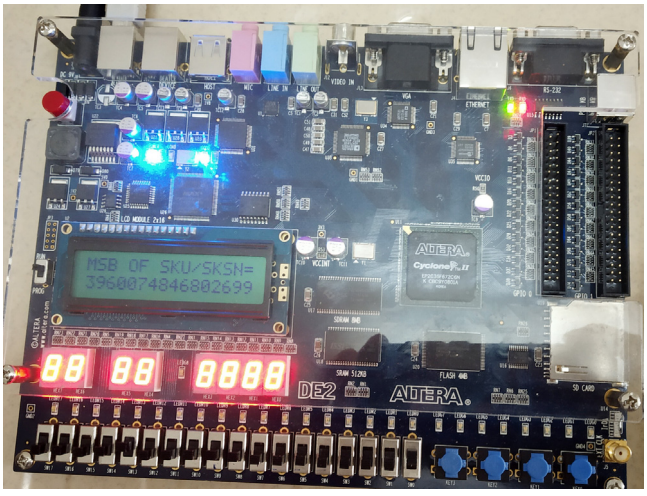


Fig. 9. Session key generation for valid user.

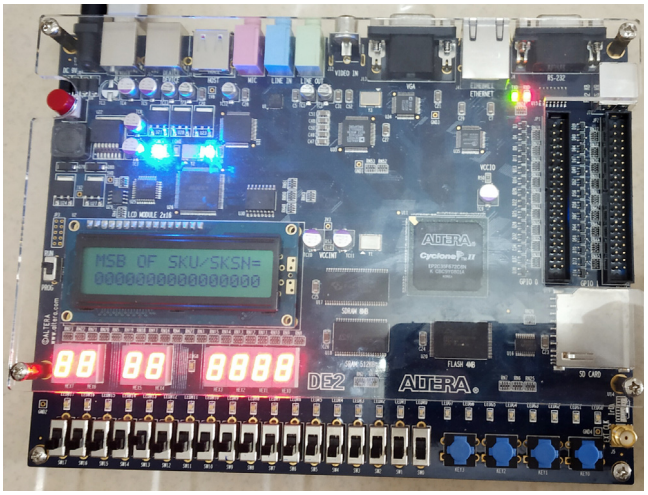


Fig. 10. Session key generation for fake user.

et al. proposed a efficient cipher processor for dual field elliptic curve cryptography that possesses all basic ECC operations in curve parameters and the programmable field. Kimmo Jarvinen [48] introduced a new FPGA based crypto processor for high speed elliptic curve cryptographical applications.

In security related applications, random number generation is one of the crucial parts to produce the numbers intermittently and those numbers are efficiently produced by Fibonacci LFSR in hardware. LFSR is a combination of D-Flip Flops and Ex-Or gates. The feedback input selection will be purely based on the primitive polynomial, whereas the n-bit LFSR can produce $2^n - 1$ values except zero. In LFSR design, an initial value is assigned and it should not be zero otherwise it remains in the zero itself. In our proposed protocol, 160 bit random number is generated using the polynomial $x^{160} + x^{158} + x^{157} + x^{155} + 1$ and it is shown in Fig. 11.

The hash algorithm and the scalar multiplication used in the proposed protocol implementation was taken as SHA-160 due to the resource constraints and the elliptic curve over the binary field $GF(2163)$ uses the polynomial $x^{163} + x^7 + x^6 + x^3 + 1$. The proposed protocol was described using Verilog Hardware Description Language (HDL) and simulated using Altera Quartus II for FPGA implementation. Finally, the entire protocol is implemented in Altera DE2 FPGA development board. For experimental purpose, the *id* and password of one legitimate user is assumed to be six characters i.e. $id = 123456$ and $password = au@s04$, then the appropriate terms in the protocol are verified and the same session key *sk* is produced in all the entities. The authenticity of the proposed protocol is verified by producing the value 1 at password check and otherwise it produces 0. The simulation results of the proposed protocol is shown in Fig. 12.

The complete hardware setup of the proposed protocol is shown in Fig. 13. The Figs. 5 and 6 shows the MSB and LSB of the 160 bit random number. In addition, the user id and password of the genuine or valid user is displayed in LCD screen of the development board along with glowing leds indicates that the entire protocol is authenticated and the same is shown in Figs. 7 and 8 otherwise the leds are in OFF mode. Finally, the session key generated by the user, gateway and sensor node for the valid user id and password for the authentic and the illegitimate users are given in Figs. 9 and 10.

6. Conclusion and future research

As always there is improvement for novel architecture of the system, in this article, we have proposed an architecture for

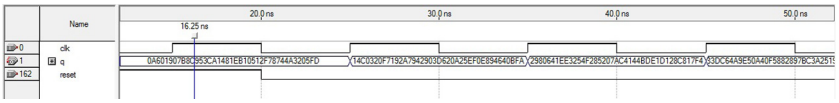


Fig. 11. Simulation result for 160 bit random number generator.

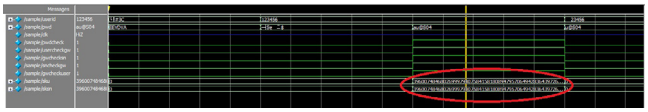


Fig. 12. Simulation result for the login and authentication phase of the proposed protocol.

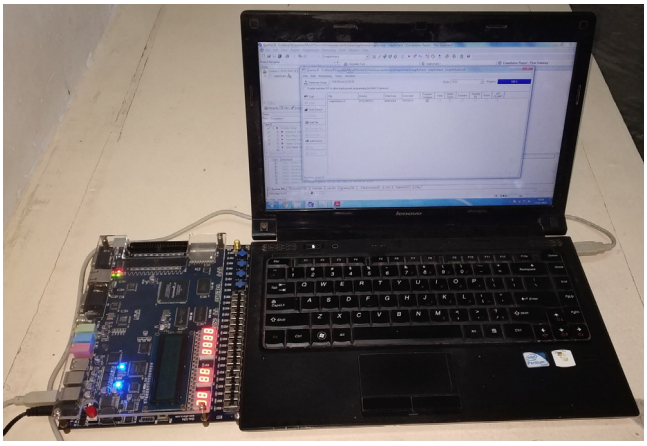


Fig. 13. Complete hardware setup of the proposed protocol.

MWSNs. Also, we have designed an ECC based robust mutual authentication protocol together with a key establishment technique useful in the IoT-enabled WSNs for medical environment to overcome the vulnerabilities in the existing protocols. The proposed protocol is analysed using the formal method BAN logic. Moreover, the informal analysis shows that our protocol is robust against many security threats. A comparative analysis of our scheme with existing similar schemes is carried out, the comparison shows proposed protocol outperforms the other protocols. We also have provided the FPGA implemented result for the proposed protocol. In recent times the advent of cloud computing applications, the secured data sharing protocol becomes a real challenge. For future work, an authenticated data sharing protocol between cloud server and doctor for accessing off-line data via any gateway can be designed with lower computational and communicational cost and achieves higher security.

Declaration of competing interest

The authors of this paper decalre that there is no conflict of interest.

References

[1] A. Ghoneim, G. Muhammad, S.U. Amin, B. Gupta, Medical image forgery detection for smart healthcare, IEEE Commun. Mag. 56 (4) (2018) 33–37.
[2] C. Stergiou, K.E. Psannis, B.-G. Kim, B. Gupta, Secure integration of IoT and cloud computing, Future Gener. Comput. Syst. 78 (2018) 964–975.
[3] Y. Zhou, Z. Sheng, C. Mahapatra, V.C. Leung, P. Servati, Topology design and cross-layer optimization for wireless body sensor networks, Ad Hoc Netw. 59 (2017) 48–62.
[4] K. Gai, K.-K.R. Choo, M. Qiu, L. Zhu, Privacy-preserving content-oriented wireless communication in internet-of-things, IEEE Internet Things J. 5 (4) (2018) 3059–3067.
[5] K. Gai, M. Qiu, Z. Xiong, M. Liu, Privacy-preserving multi-channel communication in edge-of-things, Future Gener. Comput. Syst. 85 (2018) 190–200.
[6] M. Qiu, K. Gai, Z. Xiong, Privacy-preserving wireless communications using bipartite matching in social big data, Future Gener. Comput. Syst. 87 (2018) 772–781.
[7] B. Abidi, A. Jilbab, M.E. Haziti, Wireless sensor networks in biomedical: Wireless body area networks, in: Europe and MENA Cooperation Advances in Information and Communication Technologies, Springer, 2017, pp. 321–329.
[8] N. Kaur, S. Singh, Optimized cost effective and energy efficient routing protocol for wireless body area networks, Ad Hoc Netw. 61 (2017) 65–84.
[9] K. Gai, M. Qiu, Blend arithmetic operations on tensor-based fully homomorphic encryption over real numbers, IEEE Trans. Ind. Inf. 14 (8) (2018) 3590–3598.
[10] B.B. Gupta, Computer And Cyber Security: Principles, Algorithm, Applications, and Perspectives, CRC Press, 2018.
[11] B. Gupta, D.P. Agrawal, S. Yamaguchi, Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security, IGI Global, 2016.
[12] A. Tewari, B. Gupta, Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using rfid tags, J. Supercomput. 73 (3) (2017) 1085–1102.
[13] V. Sureshkumar, R. Amin, R. Anitha, An enhanced bilinear pairing based authenticated key agreement protocol for multiserver environment, Int. J. Commun. Syst. 30 (17) (2017) e3358.
[14] M. Alhaidary, S.M.M. Rahman, M. Zakariah, M.S. Hossain, A. Alamri, M.S.M. Haque, B. Gupta, Vulnerability analysis for the authentication protocols in trusted computing platforms and a proposed enhancement of the offpad protocol, IEEE Access 6 (2018) 6071–6081.
[15] H. Zhao, M. Chen, M. Qiu, K. Gai, M. Liu, A novel pre-cache schema for high performance android system, Future Gener. Comput. Syst. 56 (2016) 766–772.

[16] K. Gai, M. Qiu, M. Liu, Z. Xiong, In-memory big data analytics under space constraints using dynamic programming, Future Gener. Comput. Syst. 83 (2018) 219–227.
[17] J. Nam, M. Kim, J. Paik, Y. Lee, D. Won, A provably-secure ecc-based authentication scheme for wireless sensor networks, Sensors 14 (11) (2014) 21023–21044.
[18] C.-H. Liu, Y.-F. Chung, Secure user authentication scheme for wireless healthcare sensor networks, Comput. Electr. Eng. 59 (2017) 250–261.
[19] S. Challa, A.K. Das, V. Odelu, N. Kumar, S. Kumari, M.K. Khan, A.V. Vasilakos, An efficient ecc-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks, Comput. Electr. Eng.
[20] M.L. Das, Two-factor user authentication in wireless sensor networks, IEEE Trans. Wirel. Commun. 8 (3) (2009) 1086–1090.
[21] D. He, Y. Gao, S. Chan, C. Chen, J. Bu, An enhanced two-factor user authentication scheme in wireless sensor networks., Ad Hoc Sens. Wirel. Netw. 10 (4) (2010) 361–371.
[22] P. Kumar, H.-J. Lee, Cryptanalysis on two user authentication protocols using smart card for wireless sensor networks, in: Wireless Advanced (WiAd), IEEE, 2011, pp. 241–245.
[23] P. Kumar, S.-G. Lee, H.-J. Lee, E-sap: Efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks, Sensors 12 (2) (2012) 1625–1647.
[24] M.K. Khan, S. Kumari, An improved user authentication protocol for healthcare services via wireless medical sensor networks, Int. J. Distrib. Sens. Netw. 10 (4) (2014) 347169.
[25] D. He, N. Kumar, J. Chen, C.-C. Lee, N. Chilamkurti, S.-S. Yeo, Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks, Multimedia Syst. 21 (1) (2015) 49–60.
[26] X. Li, J. Niu, S. Kumari, J. Liao, W. Liang, M.K. Khan, A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity, Secur. Commun. Netw. 9 (15) (2016) 2643–2655.
[27] F. Wu, L. Xu, S. Kumari, X. Li, An improved and anonymous two-factor authentication protocol for health-care applications with wireless medical sensor networks, Multimedia Syst. 23 (2) (2017) 195–205.
[28] M.S. Farash, M. Turkanović, S. Kumari, M. Hölbl, An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the internet of things environment, Ad Hoc Netw. 36 (2016) 152–176.
[29] R. Amin, G.P. Biswas, A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks, Ad Hoc Netw. 36 (2016) 58–80.
[30] R. Amin, S.H. Islam, G. Biswas, M.K. Khan, N. Kumar, A robust and anonymous patient monitoring system using wireless medical sensor networks, Future Gener. Comput. Syst. 80 (2018) 483–495.
[31] R. Ali, A.K. Pal, S. Kumari, A.K. Sangaiah, X. Li, F. Wu, An enhanced three factor based authentication protocol using wireless medical sensor networks for healthcare monitoring, J. Ambient Intell. Humaniz. Comput. (2018) 1–22.
[32] F. Wu, X. Li, A.K. Sangaiah, L. Xu, S. Kumari, L. Wu, J. Shen, A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks, Future Gener. Comput. Syst. 82 (2018) 727–737.
[33] W. Li, B. Li, Y. Zhao, P. Wang, F. Wei, Cryptanalysis and security enhancement of three authentication schemes in wireless sensor networks, Wirel. Commun. Mob. Comput. (2018).
[34] D. Mishra, P. Vijayakumar, V. Sureshkumar, R. Amin, S.H. Islam, P. Gope, Efficient authentication protocol for secure multimedia communications in IoT-enabled wireless sensor networks, Multimedia Tools Appl. 77 (14) (2018) 18295–18325.
[35] S. Suganthi, R. Anitha, V. Sureshkumar, S. Harish, S. Agalya, End to end light weight mutual authentication scheme in iot-based healthcare environment, J. Reliab. Intell. Environ. (2019) 1–11.
[36] M. Burrows, M. Abadi, R. Needham, A logic of authentication, ACM Trans. Comput. Syst. 8 (1) (1990) 18–36.
[37] D. He, N. Kumar, N. Chilamkurti, A secure temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks, in: Proceedings of the International Symposium on Wireless and Pervasive Computing (ISWPC'13), 2013, pp. 1–6.
[38] V. Sureshkumar, R. Amin, R. Anitha, A robust mutual authentication scheme for session initiation protocol with key establishment, Peer Peer Netw. Appl. (2018) 1–17.
[39] H.-L. Yeh, T.-H. Chen, P.-C. Liu, T.-H. Kim, H.-W. Wei, A secured authentication protocol for wireless sensor networks using elliptic curves cryptography, Sensors 11 (5) (2011) 4767–4779.
[40] W. Shi, P. Gong, A new user authentication protocol for wireless sensor networks using elliptic curves cryptography, Int. J. Distrib. Sens. Netw. (2013).
[41] S. Anandhi, R. Anitha, V. Sureshkumar, IoT enabled rfid authentication and secure object tracking system for smart logistics, Wirel. Pers. Commun. 104 (2) (2019) 543–560.
[42] M. Goresky, A.M. Klapper, Fibonacci and Galois representations of feedback-with-carry shift registers, IEEE Trans. Inform. Theory 48 (11) (2002) 2826–2836.
[43] P.K. Lala, Digital Circuit Testing and Testability, Academic Press, 1997.
[44] V. Vijaykumar, S.R. Sekar, S. Elango, S. Ramakrishnan, Implementation of $2^n - 2^k - 1$ modulo adder based rfid mutual authentication protocol, IEEE Trans. Ind. Electron. 65 (1) (2018) 626–635.
[45] G.D. Sutter, J.-P. Deschamps, J.L. Imaña, Efficient elliptic curve point multiplication using digit-serial binary field operations, IEEE Trans. Ind. Electron. 60 (1) (2013) 217–225.
[46] J. López, R. Dahab, Fast multiplication on elliptic curves over gf (2 m) without precomputation, in: International Workshop on Cryptographic Hardware and Embedded Systems, Springer, 1999, pp. 316–327.
[47] J.-Y. Lai, C.-T. Huang, A highly efficient cipher processor for dual-field elliptic curve cryptography, IEEE Trans. Circuits Syst. II: Express Br. 56 (5) (2009) 394–398.
[48] K. Järvinen, Optimized fpga-based elliptic curve cryptography processor for high-speed applications, Integr. VLSI J. 44 (4) (2011) 270–279.

Venkatasamy Sureshkumar received his M.Sc, M.Phil and Ph.D. degree in Mathematics from Bharathiyar University in 2004, Alagappa University in 2005 and Anna University in 2017 respectively. Currently, he is working as an Assistant Professor in the Department of Applied Mathematics and Computational Sciences, PSG College of Technology, Coimbatore, Tamilnadu, India. sand@amc.psgtech.ac.in. His research interests include Security protocols and Formal methods.

Ruhul Amin received Ph.D. in Computer Science and Engineering from the Indian Institute of Technology(ISM) Dhanbad, Jharkhand, India, in 2017. He also received B.Tech and M.Tech both in Computer Science and Engineering from Maulana Abul Kalam Azad University of Technology, West Bengal, India in 2009 and 2013, respectively. Presently, he is working as an Assistant Professor in the Department of Computer Science and Engineering, Dr. Shyama Prasad Mukherjee International Institute of Information Technology, Naya Raipur, India. His research interest includes authentication protocol and security in WSNs.

V.R. Vijaykumar received the Bachelor's degree in electronics and communication engineering from the Thanthai Periyar Government Institute of Technology, Vellore, India, and the Master's degree in communication systems from the Thiagarajar College of Engineering, Madurai, India, respectively. He received the Ph.D. degree in the area of non-linear filtering for image denoising from Anna University, Chennai, India. He is currently working as an Associate Professor in the Department of Electronics and Communication Engineering, Anna University Regional Campus, Coimbatore, India. He has 20 years of teaching experience, and his area of research include image processing, signal processing, and VLSI design. He has published more than 85 research papers in international journals and conferences.

S. Raja Sekar received the Bachelor's degree in electronics and communication engineering from Syed Ammal Engineering College, Ramanathapuram, India, and the Master's degree in VLSI design from Anna University Regional Campus, Coimbatore, India, in 2012 and 2015, respectively. He is currently working as an Assistant Professor in the Department of ECE, Bannari Amman Institute of Technology, Sathyamangalam. His research interests include cryptography and digital VLSI Design.

Implementation of $2^n – 2^k$ -1 Modulo Adder Based RFID Mutual Authentication Protocol

Vijaykumar V R, Member, IEEE, Raja Sekar S, Elango S and Ramakrishnan S

***Abstract*— In wireless communication, secure transmission and reception of data are the major concern today. In recent years, Radio Frequency Identification (RFID) plays a vital role in the security system for secured data communication. The main challenge in RFID based security system is to design a more secure, better area and power efficient encoder architecture for tag-reader mutual authentication protocol. This paper proposes new and efficient encoder architecture for RFID mutual authentication protocol which utilizes 2^n - 2^k - 1 modulo adder for achieving higher security. The proposed architecture is described in Verilog Hardware Description Language (HDL) and the functionalities are verified and synthesized using Altera Quartus II tool. The architecture is also synthesized using Cadence RTL compiler for 180 nm and 90 nm technology. Experimental results of the proposed scheme gives better performances in terms of area, power and delay when compared with existing mutual authentication schemes. In addition to that, the architecture is realized as hardware in Altera DE2 Cyclone II (EP2C35F672C6) Field Programmable Gate Array (FPGA) and real time verification has been carried out using Logic Analyzer 16851A. Finally, formal security analysis has been performed using the Burrows-Abadi-Needham (BAN) logic to show that the proposed protocol is secure.**

***Index Terms*— ASIC, BAN Logic, FPGA, RFID, Logic Analyzer and Mutual Authentication.**

I. INTRODUCTION

RFID is a recent wireless technology that utilizes radio signals to identify and track a variety of objects which has a unique serial identity [1]. This system consists of three major sections: transponder (tag), the interrogator (reader) and database [2]. It utilizes one of the three general frequency bands, (i.e.) 125 kHz to 134 kHz (low frequency), 13.56 MHz (high frequency), and 860 MHz to 930 MHz (Ultra High Frequency) [3]. Every RFID tag has owned unique identity code named as Electronic Product Code (EPC). There are two categories of tags namely passive and active based on the storage, specifications and applications. Passive tags do not need battery power because it acquires the power from the reader's electromagnetic request signals energy but the active tags need a battery back-up. Passive tags have lower storage capabilities less than 1KB and used for shorter range applications that range from 4 inches to 15 feet. It can be usually write-once-read-many (i.e. Read-only tags). Active tags have a storage ability of up to 512KB and are used for longer applications up to 300 feet [4]. RFID reader writes and reads the data available in tag. Database has an integrated circuit for storing the details of the tags associated with the reader, EPC and password of individual tags. Generally, there is a need for dynamic protocol for well-secured communication that takes place between the RFID reader and tag. For any security applications, Linear Feedback Shift Register (LFSR) plays a vital role to generate the random numbers at both the reader and tag. There are two types of LFSR architecture namely Fibonacci and Galois type LFSR [5] [6]. In that, Fibonacci LFSR is most commonly used for hardware implementation.

Initially, a very basic EPC Global Class-1 Gen-2 RFID standard has developed which provides a security purely based on the 16-bit pseudo random numbers only. Peris-Lopez [7]-[10] explains three different tag-reader mutual authentication protocols rely on the bit-wise operation. H. Y. Chien [11] describes the protocol with additional one rotation operation. Selwyn Piramuthu discusses as many numbers of RFID mutual authentication protocols in [12] [13]. Konidala et. al. [14] [15] proposes two different protocols that use PadGen which are computed using two passwords. The above-discussed protocols have its own advantages in terms of security however it has not been realized in hardware.

Recently, the hardware implementation of the authentication protocol with area, delay consideration concept has been emerged. Padgen function proposed by Konidala et. al. has been modified by Huang et. al. [16] and come up with two modified schemes for data confidentiality. It improves a bit security but not sufficiently large. The same author [17] further improved the security of the protocol by using XOR and Mod Div schemes. Even though, the above discussed hardware realized algorithms improve the security, it occupies large amount of area in the architecture. Hence, the above stated RFID protocols are not suitable for lightweight handheld applications. To overcome the area complexity, an

Manuscript received June 20, 2016; revised April 02, 2017; accepted May 07, 2017.

V. R Vijaykumar and S. Raja Sekar are with ECE Department, Anna University Regional Campus, Coimbatore, Coimbatore, Tamil Nadu, India. (E-mail: vr_vijay@yahoo.com and srajasekarbeece@gmail.com).

S. Elango is with ECE Department, Bannari Amman Institute of Technology, Sathyamangalam, Tamil Nadu, India. (E-mail: elangos@bitsathy.ac.in)

S. Ramakrishnan is with IT Department, Dr Mahalingam College of Engineering & Technology, Pollachi, Tamil Nadu, India. (E-mail: ram_f77@yahoo.com)

area efficient mutual authentication protocol based on truncated multiplier [18] is proposed with compromise in security. Liu et. al. [19] designs an ECC-based digital baseband controller for RFID tag chip and implemented in hardware. Schnorr protocol is used in the controller to perform the authentication between the reader and tag. In [20] [21], Niu et. al. proposes an EPC Gen2v2 mutual authentication protocol for ownership transfer, ownership delegation and ownership management. Mtitia et. al. [22] offers two different approaches for server less mutual authentication between the reader and multiple tags. In that, first one is for providing mass authentication to group of RFID tags whereas the other one is for tag search algorithm. Shang Ma et. al. [23] describes the designing methodology for (n-2) different modulo adder architectures which have been used for cryptographic applications also.

In [24], cho et. al. analyzes the security against the brute-force attack in the RFID mutual authentication protocols. Burrows et. al. [25] describes certain logics, rules and procedures to verify the authentication protocol for security analysis formally. Chatterjee et. al. proposes an authentication scheme in [26] and use BAN logic for proving their protocol's security. In [27], Liu et. al. proposes a Zero-knowledge mutual authentication protocol and analyzed its soundness in resisting various models. All the above-discussed hardware and software protocols are either improving the security or reducing the area complexity. Hence a new protocol is required to achieve better security with reduced area. This motivates to develop a new protocol which improves security and reduces area complexity.

The main contributions of the proposed work are as follows: 1) Development of a new Tag-Reader Mutual Authentication (TRMA) protocol which has lesser area, delay and power. 2) Hardware realization of the proposed protocol is done using ALTERA DE2 Cyclone II FPGA board. 3) The functionalities of the proposed protocol are verified using Logic Analyzer 16851A. 4) Performances of the proposed protocol are analyzed by implementing in both FPGA and ASIC platforms. 5) Formal security analysis is carried out using BAN logic.

The rest of the paper is organized as follows: Section 2, deals with detailed description of the well-known hardware implemented RFID mutual authentication protocols. The proposed authentication protocol is described in Section 3. The synthesized and implementation results are discussed in Section 4 quantitatively. Section 5 deals with the formal and informal security analysis of the proposed protocol. Finally, the conclusion of the paper is summarized in Section 6.

II. BACKGROUND AND RELATED WORK

In a RFID mutual authentication protocol, to establish the communication between the tag and the reader an encoded password is required. In general, the RFID communication starts with the request signal sent by the reader. The reader always emits the radio signal and whenever the tag enters into the range it responds to the reader's request. The protocols discussed below have their own procedure for encryption and decryption and has some advantages and disadvantages.

A. EPC Global Class-1 Generation-2 Standard

In this standard, a bitwise EX-OR is performed to generate a cover code string [4]. This scheme is not secure because it supports only reader authentication. This can help to create cloned fake tags using the unencrypted cover coded password which is generated by a simple bitwise operation.

B. PadGen Based Mutual Authentication Protocols

PadGen is a computation procedure for encrypting and decrypting the password. Konidala initially coined the word PadGen and has given the detailed procedure for mutual authentication scheme in [15]. This protocol uses two passwords and four random numbers for the two rounds of PadGen computation to compute cover coded password. The first round of PadGen uses access password while the second uses kill password. The drawback of the protocol is not realized in hardware. Huang et. al. [16] uses the same PadGen concept but the computation procedure is different. In that paper, two different computation procedures were described and it overcomes the drawbacks of the Konidala scheme. All the above discussed protocols need four different random numbers for PadGen computation. The same Huang et. al. [17] proposed two other well-secured protocols for mutual authentication namely XOR and Mod Div schemes. These two schemes are also based on the PadGen computation but it uses only two random numbers each. It improves the security than the previous protocols but needs a large amount of area. The above mentioned protocols [16] [17] are implemented in FPGA but it increases the hardware cost by increasing area, power and delay. Therefore there is a need for a better encoding architecture with less utilization of area and minimum delay is essential for lightweight cryptographic applications.

III. PROPOSED MUTUAL AUTHENTICATION PROTOCOL

A. Proposed Protocol

The proposed protocol architecture utilizes 32 bit password and two 32 bit random numbers (each one generated by the tag and the reader), for establishing the mutual authentication. The random numbers and the password are processed by the proposed encoder which uses 2^n-2^k-1 modulo adder for better security. Fig. 1 describes the overall flow of the proposed mutual authentication protocol and the generalized modulo adder based encoder architecture for achieving the mutual authentication is shown in Fig. 2.

The notations and symbols used in the proposed protocol are given in Table I. The assumptions and initial settings of the RFID system are as follows:

- The EPC code and Password (PWD) of the tag is known to both tag and server.
- Both the tag and server having the capability to generate random numbers.

- The value of k has been preset by the designer to develop the encoder architecture.

TABLE I
NOTATIONS AND SYMBOLS USED IN THE PROPOSED PROTOCOL

Notations/ Symbols	Abbreviations	Size
EPC	Electronic Product Code	-
Req_R	Request send from Reader to Tag	-
RT	Random Number generated at Tag	32
RM	Random Number generated at Reader	32
PWD	Tag's unique Password	32
PWDL	LSB of the Password (PWD)	16
PWDM	MSB of the Password (PWD)	16
CCPWDRT	Cover Coded Password generated at Reader to Tag	16
CCPWDR1	Intermediate Cover Coded Password generated at Reader in Reader Authentication phase	16
CCPWDT1	Intermediate Cover Coded Password generated at Tag in Reader Authentication phase	16
CCPWDTM	Cover Coded Password generated at Tag to Reader	16
CCPWDT2	Intermediate Cover Coded Password generated at Tag in Tag Authentication phase	16
CCPWDR2	Intermediate Cover Coded Password generated at Reader in Tag Authentication phase	16
LFSR	Linear Feedback Shift Register	16
SPWD	Session Password	32
MODADD	2^n-2^k-1 Modulo Adder	-
⊕	EX-OR Operation	-
‖	Concatenation Operation	-

The detailed description of the proposed protocol is as follows.

Step 1: A request message [Req_R] is send by the reader to the tag.

Step 2: A new random number, RT, is generated at the tag.

Step 3: The message [EPC, RT] is transmitted from tag to reader.

Step 4: The reader forwards the message [EPC, RT] received from the tag to the server.

Step 5: The server retrieves the password (PWD) associated with the EPC from database and also generates a new random number, RM.

Step 6: The server generates the Cover-Coded Password (CCPWDRT) by Ex-oring the stored password with the intermediate Cover-Coded Password (CCPWDR1) generated by the proposed modulo encoder.

$$CCPWDRT = CCPWDR1 \oplus PWD\ [15:0] \quad (1)$$

The procedure for the generation of the CCPWDR1 is as follows

$$M1\ [15:0] = \{RT\ [15:0] \oplus PWD\ [15:0]\} \quad (2)$$
$$M2\ [15:0] = \{RT\ [31:16] \oplus PWD\ [31:16]\} \quad (3)$$
$$LSB\ [7:0] = \{MODADD\ (M1\ [15:8], M2\ [7:0])\} \quad (4)$$
$$MSB\ [7:0] = \{MODADD\ (M1\ [7:0], M2\ [15:8])\} \quad (5)$$
$$CCPWDR1 = MSB \parallel LSB \quad (6)$$

Where RT is the 32 bit random number generated at the tag and MODADD is the Modulo Adder architecture.

Step 7: The message [EPC, CCPWDRT, RM] is transmitted to reader the from server.

Step 8: The tag receives the message [CCPWDRT, RM] from the reader.

Step 9: The tag generates the intermediate Cover-Coded Password (CCPWDT1) using the procedure identical to that of generation of CCPWDR1, as described in equation (2)-(6).

Step 10: The tag verifies the LSB part of the password by

$$PWDL = CCPWDRT \oplus CCPWDT1 \quad (7)$$

If PWDL = PWD [15:0], reader gets authenticated by the tag, otherwise authentication fails.

Step 11: The tag generates the Cover-Coded Password (CCPWDTM) by EX-ORing the stored password with the intermediate Cover-Coded Password (CCPWDT2) generated from the proposed modulo encoder.

$$CCPWDTM = CCPWDT2 \oplus PWD\ [31:16] \quad (8)$$

The procedure for the generation of the CCPWDT2 is same that of generation of CCPWDR1, except the random number RM is used in the encoder instead of the random number RT.

Step 12: The message [EPC, CCPWDTM] is transmitted to reader from tag.

Step 13: The reader forwards the message [EPC, CCPWDTM] received from the tag to the server.

Step 14: The server generates the intermediate Cover-Coded Password (CCPWDR2) using the procedure identical to that of generation of CCPWDR1, except the random number RM is used in the encoder instead of the random number RT.

Step 15: Server verifies the MSB part of the password by

$$PWDM = CCPWDTM \oplus CCPWDR2 \quad (9)$$

If PWDM = PWD [31:16], tag gets authenticated by the server, otherwise authentication fails.

Step 16: If both tag and reader gets authenticated to each other, the communication establishes between the tag and reader with a new Session password (SPWD)

$$SPWD = PWD \oplus CCPWD \quad (10)$$
$$\text{where } CCPWD = CCPWDT1 \parallel CCPWDT2 \text{ at Tag} \quad (11)$$
$$\text{and } CCPWD = CCPWDR1 \parallel CCPWDR2 \text{ at Reader} \quad (12)$$

B. Modulo $2^n – 2^k$ -1 Adder Architecture [23]

Generally, highly secured cryptographic applications consume a large amount of area due to the increase in the computation complexity for efficient encryption and decryption in wireless communication. In lightweight cryptographic applications, area delay and security are the major concerns. Basically, the security-based portable cryptographical applications need to work at high speed with less consumption of area whereas the available protocols are in contrast. Therefore, most of the researchers revolve around that and finally stay back with modulo adder structure because

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIE.2017.2711864, IEEE Transactions on Industrial Electronics

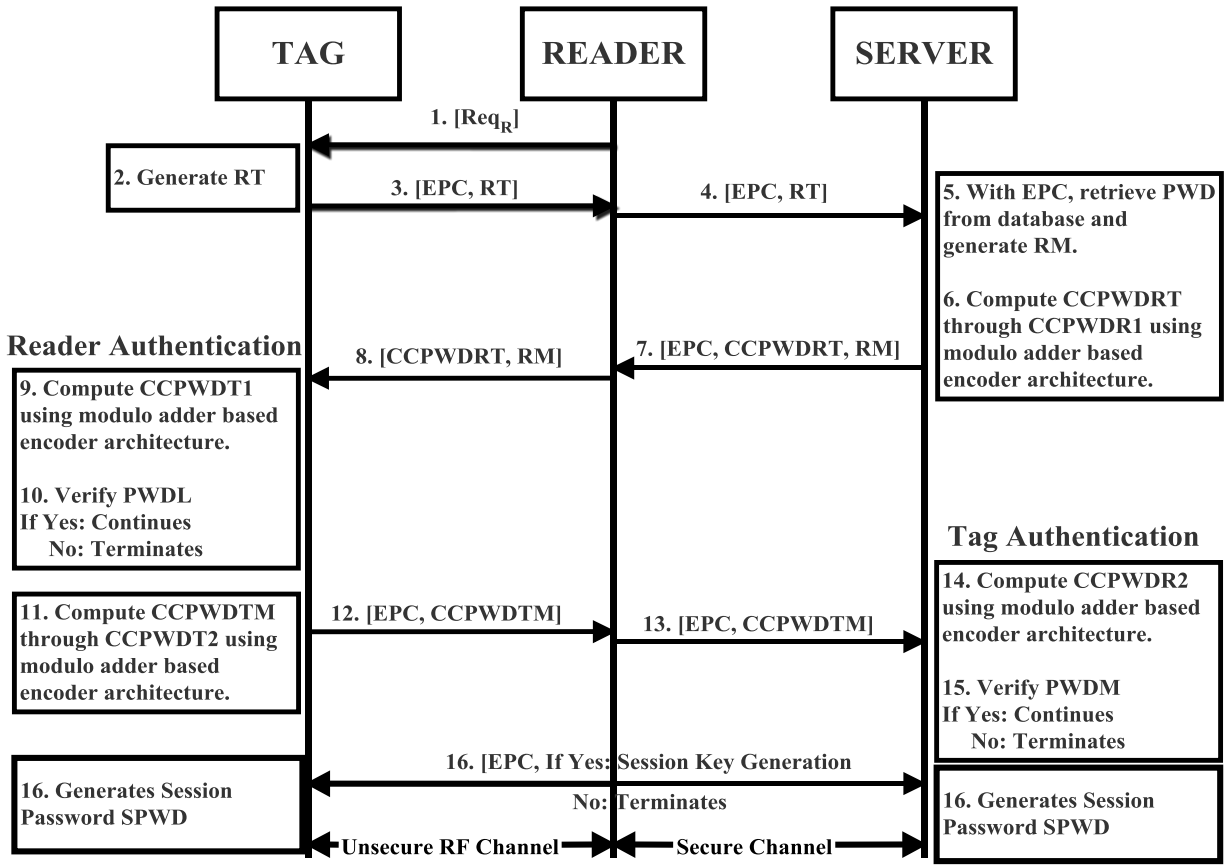


Fig. 1. Proposed Tag-Reader Mutual Authentication (TRMA) protocol

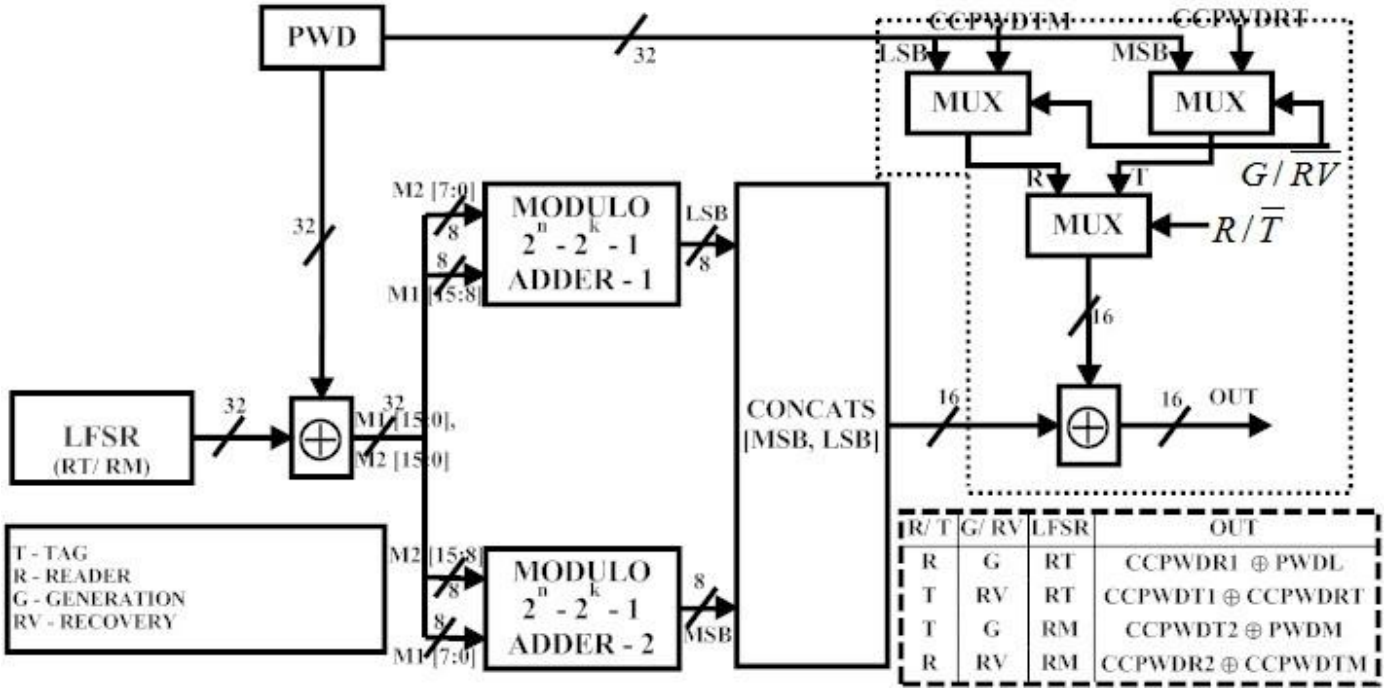


Fig. 2. Proposed TRMA protocol encoder architecture

it consumes less area than any other known architecture. Usually, modulo adder architecture depends on bit length (n) of the adder and takes the modulus of a result obtained from the normal adder. The operation of the modular adder needs two n bit numbers and a modulus value. Initially it adds those two n-bit numbers and subtracts the modulus value from the result. There are numerous amount of known modulo adder architectures which are available among the $2^n - 2^k$ -1 Modulo

adder [23] is used for proposed mutual authentication protocol architecture. The main reason behind choosing the above modulo adder in the proposed protocol is that it produces different architectures with less delay and minimum utilization of area.

The modulo adder architecture depends on two different values such as n and k. The value of n is the bit length used in the adder and the k value ranges from 1 to n-2 which is assumed by the designer. Therefore, there are n-2 different architectures [23] which are possible to construct. Then to overcome the delay encountered in the circuit, parallel prefix technique is used for obtaining the final result as modulus output. Hence the architecture will able to produce the results quicker with less utilization of area. In the proposed protocol architecture, the processed inputs are taken as 8 bit length. Therefore the n value is 8 and k value ranges from 1 to 6. For example, assume the values of inputs as a=215, b=177 and the modulus value k=4 {239 ($2^8 - 2^4 - 1$)} then it results in an output as $|392|_{239} = 153$. By using two different k values in protocol architecture, the security can be further improved i.e. $(n-2)*(n-2) = n^2-4n+4$ different architectures are possible.

C. Modified Linear Feedback Shift Register (MLFSR)

Whenever one goes for a security application, random number generation is a very crucial part and those numbers are efficiently generated by Linear Feedback Shift Register (LFSR) at both the reader and tag. Fibonacci type LFSR [5] [6] is used in the proposed protocol because it is more suitable for hardware. In general, LFSR consists of simple D-Flip Flops and EX-OR gates only. The selection of feedback inputs and entire architecture is purely based on the primitive polynomial $x^{32} + x^{30} + x^{29} + x^{25} + 1$. The important thing in design of LFSR is to assign the initial value. It must be except zero and can produce $2^n - 1$ values (otherwise it will remain zero for all time). Normally one of the critical problems which arise in passive tags is initial value assignment. Generally, it can initialize the same initial value every time it gets energized from the reader. To overcome this problem, a modified LFSR with 32-bit additional register is proposed and used in the mutual authentication protocol. The register can be used to store the currently produced random value and taken as initial value for the next time it gets energized. By using this concept, randomness in the passive tags has increased drastically.

IV. Results and Discussion

In this section, the proposed protocol is implemented in FPGA and ASIC platforms and its performances have been compared with the existing state of art software and hardware implemented mutual authentication protocols namely M^2AP [9], LMAP [8], EMAP [7], TRMA [14], konidala [15], SASI [11], M^3AP [10], three schemes in Y. J. Huang [16], XOR and MOD scheme [17]. The above mentioned protocols are described using Verilog HDL to simulate, and synthesize to produce gate level netlist using Altera Quartus II and Cadence RTL compiler for FPGA and ASIC implementation respectively.

A. FPGA Implementation

The 32-bit password (PWD) of the particular tag is encoded into a 16-bit cover coded passwords by the tag and reader using proposed architecture and verified. After the cover coded passwords are verified at either end means there is communication between the reader and tag begins otherwise it ends. For example, if password of the tag is taken as PWD = 32'H ABCDEF01 and the random numbers produced by the tag and reader are RT = 32'H 00A200A2, RM = 32'H 00D200D2 respectively. Then the proposed mutual authentication protocol produces its corresponding cover coded passwords CCPWDRT = 16'H B06E and CCPWDTM = 16'H 24D2 and verifies. The reader-authentic and tag-authentic signals produce the value '1' when it passes the verification successfully otherwise it produces '0'. The clock frequency used for simulation is 100 MHz. The simulation results of the proposed mutual authentication protocol at varies stages are shown in Fig. 3(a) – 3 (d).

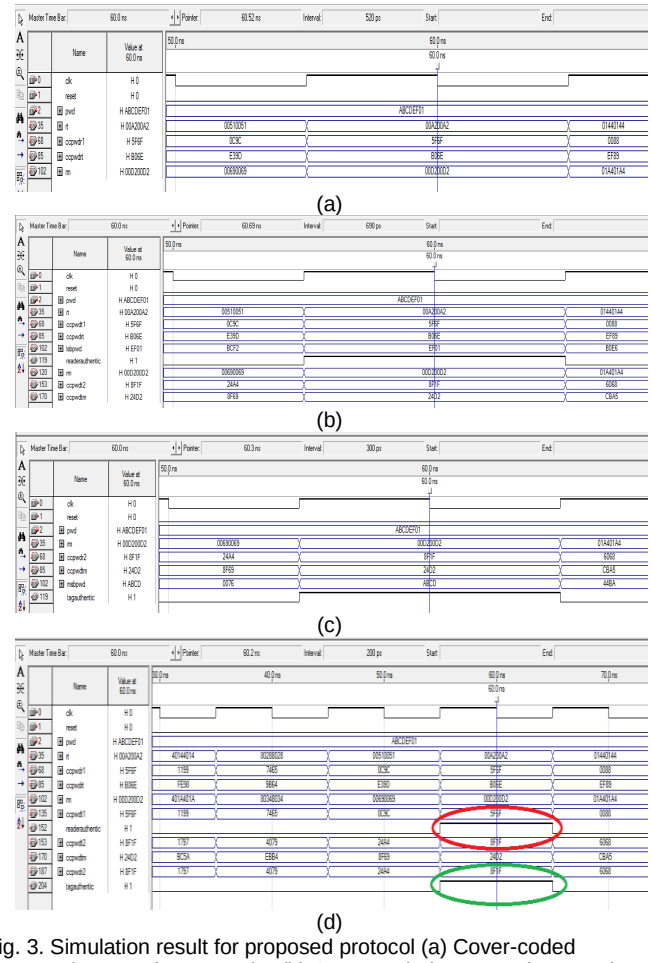


Fig. 3. Simulation result for proposed protocol (a) Cover-coded password generation at reader (b) Cover-coded password generation and reader authentication at tag (c) Tag authentication at reader (d) Overall simulation output

The modified LFSR architecture has the ability to store the processed 32 bit output with the help of 32 bit additional register. For example, if the initial value of the LFSR is assumed as 32'H A00AA00A and after n-1, n clock pulses the random numbers are 32'H 02A80289 and 32'H 05500512

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIE.2017.2711864, IEEE Transactions on Industrial Electronics

respectively. If the tag re-enters into the range of reader, the existing LFSR architecture starts from the initial value (i.e.) 32'H A00AA00A whereas the modified LFSR starts from the $(n-1)^{th}$ value 32'H 02A80289 and the same is shown in Fig. 4 and Fig. 5 respectively.

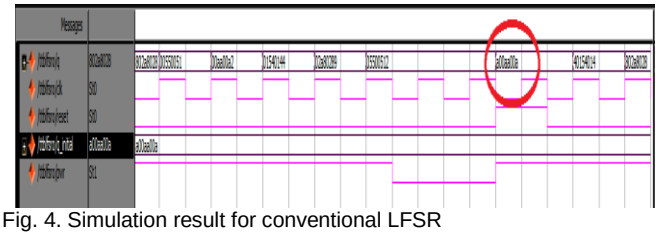


Fig. 4. Simulation result for conventional LFSR

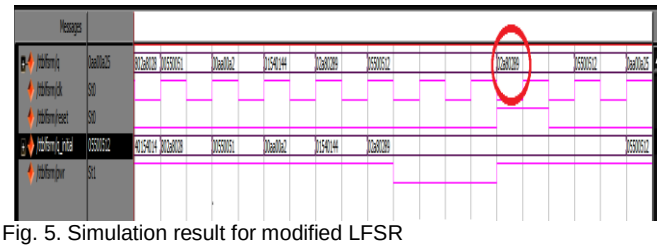


Fig. 5. Simulation result for modified LFSR

FPGA synthesis results obtained for the proposed scheme is compared with the existing M^2AP [9], LMAP [8], EMAP [7], TRMA [14], konidala [15], SASI [11], M^3AP [10], three schemes of Y. J. Huang [16], XOR and MOD schemes [17] using various quantitative parameters namely power, delay, number of logic elements and registers. The same are tabulated in Table II and Table III respectively.

TABLE II
POWER, DELAY AND PDP COMPARISON

Protocols	Dynamic Power (mW)	Propagation Delay (ns)	Clock to Output Delay (ns)	Critical path reg. to reg. delay (ns)	PDP (pJ)
M^2AP [9]	40.45	24.23	22.456	1.187	980.4
LMAP [8]	56.34	24.36	22.268	1.168	1373
EMAP [7]	34.85	23.98	22.168	1.178	835.9
TRMA [14]	29.67	23.59	21.167	1.188	700.0
Konidala [15]	30.92	23.68	21.238	1.185	732.2
SASI [11]	55.89	26.98	22.689	1.368	1508
M^3AP [10]	68.59	27.59	25.497	1.269	1892
Original Sch. at Y.J Haung [16]	36.45	24.23	21.785	1.034	882.3
Modified Sch.1 [16]	38.49	24.43	23.647	1.265	940.3
Modified Sch.2 [16]	48.34	24.86	24.765	1.185	1202.2
XOR Scheme [17]	32.98	24.75	23.650	1.189	816.1
MOD Scheme [17]	56.86	28.86	26.396	1.349	1641
Proposed	6.88	20.98	17.522	1.180	144.3

From Table II, the proposed protocol architecture is better in area, power and delay compared to all existing protocols. The proposed protocol saves nearly 70-90% of area than software related protocols and around 55-80% of area than the hardware implemented protocols. The power dissipation is 75-88% lesser than software protocol and 60-78% lesser than hardware protocols. Finally, the delay encountered in the proposed protocol is reduced around 17-31% compared to software protocol and 18-34% than the hardware implemented protocols. In Table III, the total number of registers specified as ROM is especially used for storing the Unique identification number (i.e. specific for each and every tag) of the tags and the total number of registers specified as RAM is for encryption and decryption process performed in the protocol architecture.

TABLE III
LOGICAL ELEMENTS AND REGISTER COMPARISON

Protocols	Total Logical Elements	Total No. of Registers (RAM)	Total No. of Registers (ROM)
M^2AP [9]	2021	1152	96
LMAP [8]	1724	1056	96
EMAP [7]	1536	1152	96
TRMA [14]	720	128	32
Konidala [15]	1449	128	64
SASI [11]	2234	1056	96
M^3AP [10]	4990	192	32
Original Sch. at Y.J Haung [16]	854	128	64
Modified Sch.1 [16]	958	128	64
Modified Sch.2 [16]	1230	128	64
XOR Scheme [17]	1440	64	64
MOD Scheme [17]	1642	64	64
Proposed	229	64	32

B. Hardware Realization and Real Time Verification

The proposed mutual authentication protocol is realized in Altera Cyclone II FPGA EP2C35F672C6 device [28]. A 16 bit CCPWDRT = 16'H B06E and CCPWDTM = 16'H 24D2 are displayed in Liquid Crystal Display (LCD), MSB of RT and RM are displayed in seven segment display. By glowing Green (tag-authentic) and red (reader-authentic) LEDs, the mutual authentication is achieved which is shown in Fig. 6.

The hardware implementation of the proposed protocol is also tested for real time verification using Logic Analyzer (16851A) and the setup is shown in the Fig. 7. And the results are given in Fig. 8.

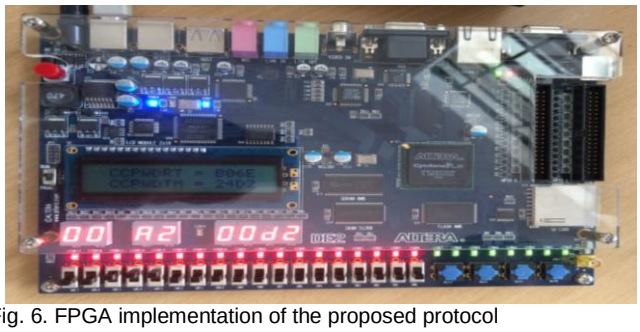


Fig. 6. FPGA implementation of the proposed protocol

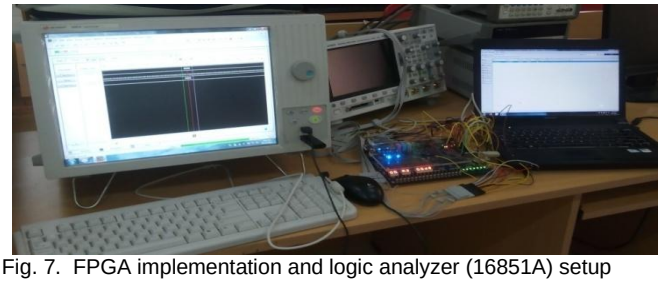


Fig. 7. FPGA implementation and logic analyzer (16851A) setup

TABLE IV
AREA, POWER AND DELAY COMPARISON

Protocols	Area (μm^2)		Leakage Power (μW)		Dynamic Power (μW)		Delay (ps)	
	180nm	90nm	180nm	90nm	180nm	90nm	180nm	90nm
M^2AP [9]	433594	142090	9.16	385.12	10668.2	2359.7	4499	3376
LMAP [8]	453604	148647	9.06	385.76	118888.8	2674.4	4492	3370
EMAP [7]	259896	85168	8.68	311.96	7461.8	1385.3	4481	3363
TRMA [14]	75523	24749	2.06	67.10	2748.8	2147.0	2942	2279
Konidala [15]	120257	39409	3.35	98.87	2924.0	637.8	2984	2371
SASI [11]	1122845	367956	12.96	556.24	64572.6	28464.7	3459	2749
M^3AP [10]	2324313	761683	22.81	1288.66	177745.7	49339.3	53741	37992
Original Sch. at Y.J Haung [16]	122865	40263	3.50	102.88	3851.4	809.2	3038	2403
Modified Sch.1 [16]	122818	40248	3.50	102.85	3783.5	796.5	3022	2393
Modified Sch.2 [16]	370305	121350	7.86	25.27	10708.4	2405.0	3994	3093
XOR Scheme [17]	141222	46279	3.97	112.65	4660.7	993.0	3324	2590
MOD Scheme [17]	2358058	772742	24.60	1245.46	21873.1	5604.9	26570	8959
Proposed	16943	5598	0.608	21.485	1287.32	274.2	2829	2251

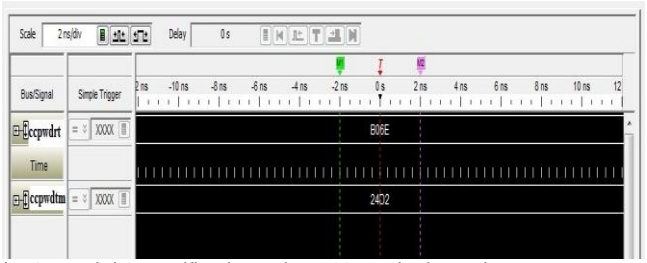


Fig. 8. Real-time verification using 16851A logic analyzer

C. ASIC Implementation

The existing and proposed protocols were synthesized using Cadence RTL Compiler for ASIC implementation. The performance metrics such as area, leakage power, dynamic power and delay where compared for both the 180 nm and 90 nm technologies and the same are given in Table IV. From the Table IV, the proposed scheme consumes only 5-24% for 180nm technology and 1-59% for 90 nm technology over existing software and hardware implemented protocols respectively. The power dissipation ratio for the proposed scheme is reduced over 63-98% for software and 44-95% for hardware implemented protocols. Finally, the delay encountered in the scheme is minimized up to 6-45% over the software protocols and 6-60% for hardware protocols. Physical design of proposed protocol is shown in Fig. 9.

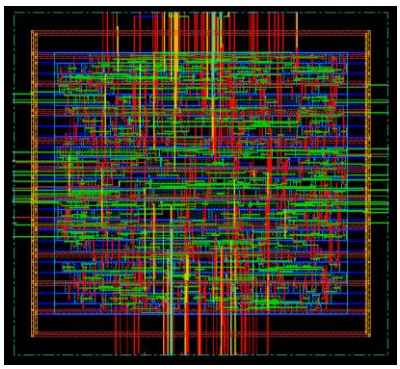


Fig. 9. Layout of the proposed protocol architecture

V. Security Analysis of the Proposed Protocol

Once the proposed mutual authentication protocol is implemented, it is further analyzed in terms of security. The security analysis of the proposed mutual authentication protocol is formally and informally verified in terms of various parameters such as Forward Secrecy, Brute Force Attack, Replay attack, Man in the Middle attack and Mutual Authentication.

A. Formal Security Analysis using BAN Logic

BAN logic [25] has been applied for the formal security analysis of the proposed mutual authentication protocol. The detailed explanations of the BAN Logic can be found in [25]. Notations and descriptions of the BAN logic used in this paper are given in Table V.

TABLE V
NOTATIONS AND DESCRIPTIONS IN BAN LOGIC

Notations	Descriptions
$P \mid\equiv X$	Principal P believes statement X
$P \lhd X$	P sees the statement X
$\#(X)$	The formula X is fresh
$P \mid\sim X$	Principal P once said statement X
(X, Y)	Formula X or formula Y is one part of the formula (X, Y)
$P \Rightarrow X$	P has jurisdiction over statement X
$\langle X \rangle_Y$	This represents X combined with the formula Y
$P \overset{K}{\longleftrightarrow} Q$	P and Q may use the shared key K to communicate. K is good in that it will be known only by P and Q
$SPWD$	Session Password used in the current session

The five rules of the BAN logic [26] are provided in Table VI and those five rules are applied to our proposed protocol and are presented in Table VII.

The assumptions are

A1: $T \Rightarrow RT$ **A2:** $T \mid\equiv \#(RT)$

A3: $R \Rightarrow RM$ **A4:** $R \mid\equiv \#(RM)$

A.5: $T \mid\equiv \left(T \overset{PWD}{\longleftrightarrow} R\right)$ **A.6:** $R \mid\equiv \left(T \overset{PWD}{\longleftrightarrow} R\right)$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIE.2017.2711864, IEEE Transactions on Industrial Electronics

TABLE VI
FIVE RULES OF BAN LOGIC

Inference Rules	
Rule Name	**Rule**
Rule 1: (Message Meaning Rule)	$\dfrac{P \mid\equiv Q \overset{K}{\longleftrightarrow} P, P \lhd \{X\}_K}{P \mid\equiv Q \mid\sim X}$
Rule 2: (Nonce – Verification Rule)	$\dfrac{P \mid\equiv \#(X), P \mid\equiv Q \mid\sim X}{P \mid\equiv Q \mid\equiv X}$
Rule 3: (Jurisdiction Rule)	$\dfrac{P \mid\equiv Q \Rightarrow X, P \mid\equiv Q \mid\equiv X}{P \mid\equiv X}$
Rule 4: (Freshness-Conjuncatenation Rule)	$\dfrac{P \mid\equiv \#(X)}{P \mid\equiv (X, Y)}$
Rule 5: (Other Inference Rules)	$\dfrac{P \lhd (X, Y)}{P \lhd X}$

TABLE VII
BAN LOGIC RULES FOR THE PROPOSED PROTOCOL

Rule	Inference rules of the Proposed Protocol
R. 1	(A) $\dfrac{T \mid\equiv \mathrm{R} \overset{PWD}{\longleftrightarrow} T, T \lhd \{CCPWDRT\}_{PWD}}{T \mid\equiv R \mid\sim CCPWDRT}$ (B) $\dfrac{\mathrm{R} \mid\equiv T \overset{PWD}{\longleftrightarrow} \mathrm{R}, \mathrm{R} \lhd \{CCPWDTM\}_{PWD}}{\mathrm{R} \mid\equiv T \mid\sim CCPWDTM}$
R. 2	(A) $\dfrac{T \mid\equiv \#(CCPWDRT), \mathrm{T} \mid\equiv \mathrm{R} \mid\sim CCPWDRT}{T \mid\equiv R \mid\equiv CCPWDRT}$ (B) $\dfrac{\mathrm{R} \mid\equiv \#(CCPWDTM), \mathrm{R} \mid\equiv T \mid\sim CCPWDTM}{\mathrm{R} \mid\equiv T \mid\equiv CCPWDTM}$
R. 3	(A) $\dfrac{T \mid\equiv R \Rightarrow CCPWDRT, \mathrm{T} \mid\equiv \mathrm{R} \mid\equiv CCPWDRT}{T \mid\equiv CCPWDRT}$ (B) $\dfrac{\mathrm{R} \mid\equiv T \Rightarrow CCPWDTM, \mathrm{R} \mid\equiv T \mid\equiv CCPWDTM}{\mathrm{R} \mid\equiv CCPWDTM}$
R. 4	(A) $\dfrac{T \mid\equiv \#(RT)}{T \mid\equiv \#(CCPWDRT, RT)}$ (B) $\dfrac{\mathrm{R} \mid\equiv \#(RM)}{\mathrm{R} \mid\equiv \#(CCPWDTM, RM)}$
R. 5	(A) $\dfrac{T \lhd (CCPWDRT, RM)}{T \lhd (CCPWDRT)}$ (B) $\dfrac{R \lhd (CCPWDTM, EPC)}{R \lhd (CCPWDTM)}$

For the purpose of analysis, we consider only two messages, which transmit cover coded passwords. Messages between reader and server are happened at the back-end which is a secure channel and hence we consider the messages between tag and reader (Unsecure RF channel).

Message 1: $R \rightarrow T : \left(\{CCPWDRT\}_{PWD,RT}, RM\right)$

Message 2: $T \rightarrow R : \left(EPC, \{CCPWDTM\}_{PWD,RM}\right)$

According to the BAN Logic [25], the mutual authentication of the protocol should satisfy the following goals

G1: $R \mid\equiv T \mid\equiv \left(T \overset{SPWD}{\longleftrightarrow} R\right)$ **G2:** $T \mid\equiv R \mid\equiv \left(T \overset{SPWD}{\longleftrightarrow} R\right)$

Based on the above said assumptions and BAN logic rules, we provide the proof of the idealized protocol as follows.

According to message 1 and R5 (A)

S1: $T \lhd \{CCPWDRT\}_{PWD,RT}$

According to the assumptions A1, A2 and R4 (A)

S2: $T \mid\equiv \#\{CCPWDRT\}_{PWD,RT}$

According to the assumptions A1, A5, S1 and R1 (A)

S3: $T \mid\equiv R \mid\sim \{CCPWDRT\}_{PWD,RT}$, $T \mid\equiv R \Rightarrow \{CCPWDRT\}_{PWD,RT}$

According to the S2, S3 and R2 (A)

S4: $T \mid\equiv R \mid\equiv \{CCPWDRT\}_{PWD,RT}$

According to the S3, S4 and R3 (A)

S5: $T \mid\equiv \{CCPWDRT\}_{PWD,RT}$

According to the S4 and S5, we obtain

S6: $T \mid\equiv R \mid\equiv \left(T \overset{PWD}{\longleftrightarrow} R\right)$

S7: According to the proposed protocol, $\langle SPWD\rangle_{PWD,CCPWDT1,CCPWDT2}$

According to the results of above statement S1-S7, we obtain

$T \mid\equiv R \mid\equiv \left(T \overset{SPWD}{\longleftrightarrow} R\right)$ **(Goal 2)**

According to message 2 and the rule R5 (B)

S8: $R \lhd \{CCPWDTM\}_{PWD,RM}$

According to the assumptions A3, A4 and R4 (B)

S9: $R \mid\equiv \#\{CCPWDTM\}_{PWD,RM}$

According to the assumptions A3, A6, S8 and R1 (B)

S10: $R \mid\equiv T \mid\sim \{CCPWDTM\}_{PWD,RM}$, $R \mid\equiv T \Rightarrow \{CCPWDTM\}_{PWD,RM}$

According to the S9, S10 and R2 (B)

S11: $R \mid\equiv T \mid\equiv \{CCPWDTM\}_{PWD,RM}$

According to the S10, S11 and R3 (B)

S12: $R \mid\equiv \{CCPWDTM\}_{PWD,RM}$

According to the S11 and S12, we obtain

S13: $R \mid\equiv T \mid\equiv \left(T \overset{PWD}{\longleftrightarrow} R\right)$

S14: According to the proposed protocol, $\langle SPWD\rangle_{PWD,CCPWDR1,CCPWDR2}$

According to the results of above statement S8-S14, we obtain

$R \mid\equiv T \mid\equiv \left(T \overset{SPWD}{\longleftrightarrow} R\right)$ **(Goal 1)**

From the Goal 1 and Goal 2, the formal security proof of the proposed mutual authentication protocol has been established.

B. Informal Security Analysis

1) Replay Attack: An attacker can store the old messages and replay by impersonating tag or reader. The attacker can use either old CCPWDRT or CCPWDTM to impersonate. In both the cases, the authentication fails because the tag and reader use two fresh random numbers (nonce) namely RT and RM.

Proof:

An attacker 'A' recorded all the exchanged messages of previous sessions between the tag and reader, then the attacker 'A' impersonate a tag T_a to cheat the reader R and can also impersonate a reader R_a to cheat a tag [27].

Consider the following cases where the attacker replay old message by cheating both sides as a legal entity. The message elements with single quotes denote the replayed ones (i.e.) RM' replayed nonce, RM is fresh nonce.

Case 1: Attacker impersonates Tag [Denoted by $A(T_a)$]

$$R \rightarrow A(T_a) \nrightarrow T : \mathrm{Re}\, q_R$$

$$A(T_a) \rightarrow \mathrm{R} \rightarrow \mathrm{S} : \mathrm{EPC'}, \mathrm{RT'}$$

$$S \rightarrow R : EPC', CCPWDRT', RM$$

$$R \rightarrow A(T_a) \nrightarrow T : CCPWDRT', RM$$

$$A(T_a) \rightarrow \mathrm{R} : \mathrm{EPC'}, \mathrm{CCPWDTM'}$$

$$R \rightarrow S : \mathrm{CCPWDTM'}$$

$$PWDM \neq CCPWDTM' \oplus CCPWDR2$$

Because CCPWDR2 is computed using the fresh nonce RM by the server whereas the replayed cover-coded password CCPWDTM' was computed using old nonce RM'. Hence authentication fails.

Case 2: Attacker impersonates as Reader A(R)

$$A(R_a) \rightarrow T : \mathrm{Re}\, q_R'$$

$$T \rightarrow A(R_a) \nrightarrow R : EPC, RT$$

$A(R_a)$ cannot forward the message to the server, because the path between Reader and Server is secure channel. However, $A(R_a)$ can replay the old message as follows:

$$A(R_a) \rightarrow T : CCPWDRT', RM'$$

$$PWDL \neq CCPWDRT' \oplus CCPWDT1$$

CCPWDT1 is computed using fresh nonce RT by Tag whereas the replayed CCPWDRT' was computed using old nonce RT'. Hence the authentication fails.

2) Forward Secrecy: The proposed protocol prevents the forward secrecy attack as both CCPWDRT and CCPWDTM use two fresh random numbers (nonce) namely RT and RM, every time for establishing the mutual authentication. Therefore, the messages transmitted in successive sessions are different from the previous ones. For further communication after mutual authentication, a session password (SPWD) is generated at tag and reader using the PWD and the intermediate CCPWD. The freshness of the cover coded passwords and session password guarantees the forward security of the proposed protocol.

3) Brute Force Attack: If the brute force attack is performed by the attacker to recover the password, the attacker can get only 16 bits out of the 32 bits of the password (Refer equations (1) and (8)). 2^{32} times brute force attack can help the attacker to succeed. Since the password size of RFID tag is 32 bits and brute force attack of order 2^{32} on the proposed protocol achieve the required strength.

4) Man In The Middle Attack: Proposed protocol achieves mutual authentication between the tag and reader by generating the cover coded password at one end and verified at the other end. In the protocol, the cover coded passwords CCPWDRT and CCPWDTM are generated using fresh nonces (RT and RM) and the secret password PWD. Thus, the proposed protocol avoids the man in the middle attack.

5) Mutual Authentication: Reader Authentication is performed by verifying cover coded password generated at the reader by tag (i.e.) PWDL = CCPWDRT $\oplus$ CCPWDT1. Similarly the tag authentication is performed by verifying the cover coded password generated at the tag by the reader (i.e.) PWDM = CCPWDTM $\oplus$ CCPWDR2. Hence the proposed protocol achieves mutual authentication.

C. Security Comparison of the Proposed Protocol

Security comparison of the proposed protocol with other related works are provided in Table VIII. It can be seen from the table, the proposed mutual authentication protocol prevents the attacks namely forward secrecy, brute-force attack, replay attack and Man-in-the Middle attack. In addition to that, the proposed protocol consumes less area compared to other related works which are implemented in hardware.

TABLE VIII
SECURITY COMPARISON OF THE PROPOSED PROTOCOL

	[15]	[16]	[17]	[18]	Proposed
Replay Attack	Yes	Yes	Yes	No	Yes
Forward Secrecy	No	No	No	No	Yes
Brute Force Attack	Yes	Yes	Yes	No	Yes
Man-in-the Middle Attack	Yes	Yes	Yes	Yes	Yes
Hardware/ Area Overhead	High	High	High	Low	Low

VI. Conclusion

In this work, novel encoder architecture for RFID mutual authentication protocol between the reader-tag with less area, less power and minimum delay with better security is proposed. The functionality of the proposed protocol is coded in Verilog HDL and implemented in both FPGA and ASIC environments. In addition to that, the protocol is also tested in Altera DE2 Cyclone II (EP2C35F672C6) FPGA board and its output has been verified by Logic Analyzer 16851A. The security analysis of the proposed mutual authentication protocol is also demonstrated formally using BAN logic. The proposed protocol consumes low power and occupies less area hence it can be highly suitable for lightweight RFID applications.

Acknowledgment

The authors thank the anonymous reviewers and the Associate Editor for their valuable comments on the paper which helped us to improve the quality of the work.

References

[1] Dennis. E. Brown, *RFID Implementations*, McGraw Hill Communications, Oct. 2006.

[2] Dirk Henrici, *RFID Security and Privacy-Concepts, Protocols and Architecture*, Lecture Notes in Electrical Engineering, Springer International Edition. 2008, vol. 17.

[3] Frank Thornton, Brad Haines, Anand M. Das, et. al., *RFID Security*, Syngress Publishing, Inc, 2006.

[4] Ver. 1.0.9 EPC global Ratifed Standard, EPC Radio-Frequency Identity Protocols Class- 1 Generation-2 UHF RFID Protocol for Communications at 860 MHz–960 MHz [Online]. Available: http://www.epcglobalinc.org/standards.

[5] Mark Goresky and Andrew M. Klapper, Fibonacci and Galois representations of Feedback-with-Carry Shift Registers, *IEEE Transactions on Information Theory*, vol. 48, no. 11, pp. 2826-2836, Nov. 2002.

[6] P. K. Lala, *Digital Circuit Testing and Testability*, Academic Press, 2002.

[7] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda, "EMAP: An Efficient Mutual Authentication Protocol for Low- Cost RFID Tags," in *Proceedings OTM Federated Conference and Workshop*, vol. 4277 of the series lecture notes in computer science, Nov. 2006, pp. 352 – 361.

[8] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda, "LMAP: A real lightweight mutual authentication protocol for low-cost RFID tags," in *Proc. 2nd Workshop RFID Security*, Jul. 2006, pp. 1–12. [Online]. Available: http://events.iaik.tugraz.at/RFIDSec06/Program/index.htm.

[9] P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador, and A. Ribagorda, "M2AP: A Minimalist Mutual-Authentication Protocol for Low-Cost RFID Tags," Proc. Int'l Conf. Ubiquitous Intelligence and Computing (UIC '06), pp. 912-923, 2006.

[10] P. Peris-Lopez, T.-L. Lim, and T. Li, "Providing stronger authentication at a low cost to RFID tags operating under the EPC global framework," in *Proc. IEEE/IFIP Int. Conf. EUC*, Dec. 17–20, 2008, vol. 2, pp. 159–166.

[11] H.-Y. Chien, "SASI: A new ultra lightweight RFID authentication protocol providing strong authentication and strong integrity," *IEEE Trans. Dependable Secure Comput.*, vol. 4, no. 4, pp. 337–340, Oct.–Dec. 2007.

[12] S. Piramuthu, "Protocols for RFID tag/reader authentication," *Decis. Support Sys,.*, vol. 43, no. 3, pp. 897–914, Apr. 2007.

[13] S. Piramuthu, "RFID Mutual Authentication Protocols", *Decis. Support Sys,.*, vol. 50, no.2, pp. 387-393, Jan. 2011.

[14] D. M. Konidala and K. Kim, "RFID Tag-Reader Mutual Authentication Scheme Utilizing Tag's Access Password", Auto-ID Labs White Paper WP-HARDWARE-033, Jan 2007.

[15] D. M. Konidala, Z. Kim, and K. Kim, "A simple and cost effective RFID tag–reader mutual authentication scheme," in *Proc. Int. Conf. RFID Sec*, Jul. 2007, pp. 141–152.

[16] Y. J. Huang, C. C. Yuan, M. K. Chen, W. C. Lin, and H. C. Teng, "Hardware implementation of RFID mutual authentication protocol," *IEEE Trans. Ind. Electron.*, vol. 57, no. 5, pp. 1573–1582, May 2010.

[17] Y. J. Huang, Wei-Cheng Lin, and Hung-Lin Li, "Efficient Implementation of RFID Mutual Authentication Protocol", *IEEE Trans. Ind. Electron.*, vol. 59, no. 12, pp. 4784–4791, Dec. 2012.

[18] V. R. Vijaykumar and S. Elango, "Hardware implementation of tag-reader mutual authentication protocol for RFID systems", *Integration, the VLSI Journal*, vol.47, no. 1, pp.123-129, Mar. 2014.

[19] D. Liu, Z. Liu, Z. Yong, X. Zou and J. Cheng, "Design and Implementation of an ECC-Based Digital Baseband Controller for RFID Tag Chip," *IEEE Trans. Ind. Electron.*, vol. 62, no. 7, pp. 4365–4373, July 2015.

[20] H. Niu, S. Jagannathan and E. S. Taqieddin, "A Gen2v2 Complaint RFID Authentication and Ownership Management Protocol," in *39th Annu. IEEE Conf. Local Comput. Networks*, Edmonton, Canada, 2014, pp. 331-336.

[21] H. Niu, E. Taqieddin and S. Jagannathan, "EPC Gen2v2 RFID Standard Authentication and Ownership Management Protocol," *IEEE Trans. Mobile Comput.* vol. 15, no. 1, pp. 137-149, Jan. 2016.

[22] C. Mtita, M. Laurent and J. Delort, "Efficient Serverless radio-freqeuncy identification mutual authentication and secure tag search protocols with untrusted readers," *IET Inform. Security*, vol. 10, no. 5, pp.262-271, Aug. 2016.

[23] Shang Ma, Jaian-Hao Hu, and Chen-HaoWang, "A Novel Modulo $2^n - 2^k - 1$ Adder for Residue Number System", *IEEE Transactions on Circuits and Systems – I: Regular Papers*, vol. 60, no. 11, pp.2962-2972, Nov.2013.

[24] Jung-sik Cho, Sang-Soo Yeo, and Sung Kwon Kim, "Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value", *Computer Communications*, vol. 34, no. 3, pp. 391-397, Mar. 2011.

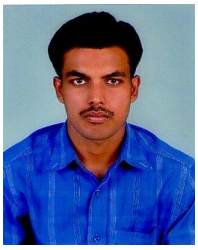
[25] M. Burrows, M. Abadi and R. Needham, "A Logic of Authentication," *ACM Trans. Computer Systems*, vol. 8, no. 1, pp. 18-36, Feb. 1990.

[26] S. Chatterjee et. al., "Secure Biometric-Based Authentication Scheme using Chebyshev Chaotic Map for Multi-Server Environment," *IEEE Trans. Depend. Sec. Comput.* vol. PP, no. 99, pp. 1-1, Oct. 2016. [Online] **DOI:** 10.1109/TDSC.2016.2616876.

[27] Hong Liu and Huansheng Ning, "Zero-Knowledge Authentication Protocol Based on Alternative Mode in RFID Systems," *IEEE Sensors J.*, vol. 11, no. 12, pp.3235-3245, Dec. 2011.

[28] [Online].Available:http://www.altera.com/products/devices/cyclone2/cy2-in.dex.jsp.

V. R. Vijaykumar is currently working as Associate Professor in the Department of Electronics and Communication Engineering, Anna University Regional Campus, Coimbatore. He received his Ph.D. degree from Anna University Chennai in the area of nonlinear filtering and Masters and Bachelors from Thiayarajar College of Engineering, Madurai and Thanthai Periyar Govt. College of Technology, Vellore respectively. He has 20 years of teaching experience and his area of research includes Image Processing, Signal Processing and VLSI Design. He has published more than 85 research papers in International Journals and Conferences.



S. Raja Sekar completed his Bachelor's degree in Electronics and Communication Engineering at Syed Ammal Engineering College, Ramanathapuram and Master's degree in VLSI Design at Anna University Regional Centre, Coimbatore in the year 2012 and 2015 respectively. His research interest includes Cryptography and Digital VLSI Design.

S. Elango received his Bachelor's Degree in ECE and Master's Degree in VLSI Design from Anna University Chennai, Tamil Nadu, India in 2010 and 2012 respectively. Currently, he is working as an Assistant Professor, Department of ECE, Bannari Amman Institute of Technology, Sathyamangalam, Tamil Nadu, India and pursuing Ph.D. Degree under Anna University Chennai. His research interest includes Digital IC Design, Computer Arithmetic, VLSI System Design, VLSI Signal Processing, Reconfigurable Computing and Residue Number System (RNS).

S. Ramakrishnan received the B.E. (ECE) in 1998, a M.E. (CS) in 2000 and PhD degree in Information and Communication Engineering from Anna University, Chennai in 2007. He is a Professor and the Head of IT Department, Dr. Mahalingam College of Engineering and Technology, Pollachi. He has 17 years of teaching experience and 1 year industry experience. He has published 139 papers and 6 books. His areas of research include digital image processing, information security and soft computing.

Measurement 47 (2014) 880–892

Contents lists available at ScienceDirect

Measurement

journal homepage: www.elsevier.com/locate/measurement

Straightening of highly curved human chromosome for cytogenetic analysis

Devaraj Somasundaram *, V.R. Vijay Kumar

Department of Electronics and Communication Engineering, Anna University Chennai, Regional Centre, Coimbatore 641 047, Tamilnadu, India

ARTICLE INFO

Article history:
Received 29 August 2013
Received in revised form 19 September 2013
Accepted 4 October 2013
Available online 18 October 2013

Keywords:
Human chromosome
Karyotyping
Straightening curved chromosomes
Inverse mapping
Thinning algorithm

ABSTRACT

Analyzing the morphological characteristics of the human chromosomes is a general task of diagnosing many genetic disorders. For this purpose, 23 pairs of the chromosomes are placed on a table like format known as a karyotype. This is usually carried out manually by a skilled operator. Automation of this procedure is a difficult image processing task due to the non-rigid nature of the chromosomes making them to have unpredictable shapes and curvatures within the image. A novel Projective Straightening Algorithm (PSA) for straightening and length detection in any given (straight, curved or highly curved) chromosome is proposed. This conventional method starts with filtering the spikes in chromosome images using median filter. Kettler algorithm is used to convert the image into binary image and Stentiford Thinning Method (STM) provides the medial axis of chromosome image. Projective Straightening Algorithm is used to straighten the medial axis, with straighten medial axis as reference and midline, binary image is straightened. A row matrix is created with respect to the straightened binary image. Chromosome image is projected over the row matrix which gives the straightened chromosome image. The parameters such as straighten angle, length and area of human chromosomes are calculated.

1. Introduction

The human body is made up of cells. In the center of each cell is an area called the nucleus. Human chromosomes are located in the nucleus of the cell. A chromosome is a structure in the nucleus that contains genes. Genes determine the traits, such as eye color and blood type. Chromosomes are threadlike strands that are composed of DNA (Deoxyribo Nucleic Acid). The usual number of chromosomes in each cell of the human body is 46 total chromosomes, or 23 pairs. Half of the chromosomes are inherited (one member of each pair) from the biological mother, and the other half (the matching member of each pair) from the biological father.

Chromosomes can be numbered in pairs from 1 to 22, with the 23rd pair labeled as X's or Y's, depending on the structure. The first 22 pairs of chromosomes are called autosomes, the 23rd pair of chromosomes is known as the sex chromosomes, because they determine whether someone will be born male or female. Females have two X chromosomes, and males have one X and one Y chromosome [1]. A picture of all 46 chromosomes, in their pairs, is called a karyotype. A normal female karyotype is written 46, XX, and a normal male karyotype is written 46, XY.

Karyotyping, which is usually done manually by a human expert, is a difficult and time consuming task. In conventional Karyotyping [2,3], giesma banded cells are photographed under a light microscope during the metaphase stage (one of the four stages of the cell division namely: prophase, metaphase, anaphase and telophase). The appearance of chromosomes depends on the stage of the cell division cycle at which they are viewed.

Automatic Karyotyping is the process of ordering and classifying the chromosomes into their respective classes, 22 pairs of autosomes and a pair of allosomes. Ordered karyograms are created using karyotyping [4,5], which are used to study chromosomal morphology. By identifying

* Corresponding author. Tel.: +91 9791267062.
E-mail address: dsomasundaramcbe@gmail.com (D. Somasundaram).

0263-2241/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.measurement.2013.10.014

the aberration in chromosome features, such as, length of chromosome, area of the chromosome and band patterns clinicians are able to judge whether the samples contain signatures of a disease [6–8]. Many genetic disorders or possible abnormalities (translocation and deletion) that may occur in the future generations can be predicted through analyzing the shape and morphological characteristics of the chromosomes.

A basic human chromosome modeling program has recently been introduced as a tool for cytogenetics education [9,10]. In the early model, however, the changeable parts are limited to certain points along the [11] chromosome. In this paper, we describe an improved method for chromosomal skeletonization which serves as a basis for programming the inter-conversion of chromosome shapes from curved to straight and vice versa. The functionality of the chromosome shape alteration is to reconstruct original chromosome images into different shapes. Pixels on the original images are mapped to new positions on destination images using a transformation function.

The new algorithms are capable of changing chromosome shapes at any points along the entire length of the chromosome. The new function meets the following two requirements: First, the length and width of the original chromosome image remain unchanged when the altered chromosome is created, and second, the original information including the gray scale values and G-bands information are kept as close as possible to the newly generated model. Throughout our beta tests, there were no missing or adding G-bands on the altered chromosomes.

2. Materials and methods

2.1. Chromosome database

Chromosomes are the structures in cells that contain genetic information. When chromosomes are photographed during cell division, the images of these chromosomes contain much information about the health of an individual. In the past it was necessary for laboratory technicians to examine these images visually by lengthy and tedious manual processes of locating, classifying, and evaluating the chromosomes [12]. Since many images often have to be inspected, many attempts have been made to automate these processes; however, automated image chromosome analysis is still an open topic. Automatic Karyotyping consists of the two main stages of segmentation and classification of the human chromosomes within the photographic pictures obtained using a light microscope. Both of the automatic chromosome segmentation [13] and classification procedures have been a well-studied problem in the last 3 decades. Most of the classification methods, however, suffer from the natural complexity of the problem, which is caused by various unpredictable appearances of the chromosomes due to their non-rigid nature (see Fig. 1).

2.2. Automated scheme

In this study we developed and tested a new computerized scheme that includes multiple stages to search for

Fig. 1. Karyotyped chromosome image.

curved chromosome from each segmented chromosome. The flow diagram of the scheme is presented in Fig. 2. The details of each stage are explained as follows. This conventional method starts with filtering the spikes in chromosome images using median filter. Kettler algorithm is used to convert the image into binary image and Stentiford Thinning Method (STM) provides the medial axis of chromosome image. Projective Straightening Algorithm (PSA) is used to straighten the medial axis, with straighten medial axis as reference and midline, binary image is straightened. A row matrix is created with respect to the straightened binary image. Chromosome image is projected over the row matrix which gives the straightened chromosome image (see Figs. 3 and 4).

2.3. Binary chromosome image

Binary images are images whose pixels have only two possible intensity values. Smaller memory requirement, Faster execution time are the advantages of binary image. Binary is obtained by thresholding the grayscale image. Thresholding is a method to convert a gray scale image into a binary image, so that objects of interest are separated from the background.

2.3.1. i. Kittler's method

Kittler and Illingworth have proposed a thresholding algorithm whose cost function. To be optimized is based on the Bayesian classification rule. In this method, it is assumed that the components in the bi-modal histogram in a gray-level image $h(g)$ are normally distributed. Normal distributions are defined by their means μ_i, standard deviations σ_i, and a priori probability P_i. For a case of two different classes ($I = 1, 2$), the background and foreground, and given a threshold T, the parameters can be estimated from the following:

$$(T) = \sum_{g=a}^{b} h(g) \tag{4.1}$$

$$\mu_i(T) = \frac{1}{P_i(T)} \sum_{g=a}^{b} h(g)g \tag{4.2}$$

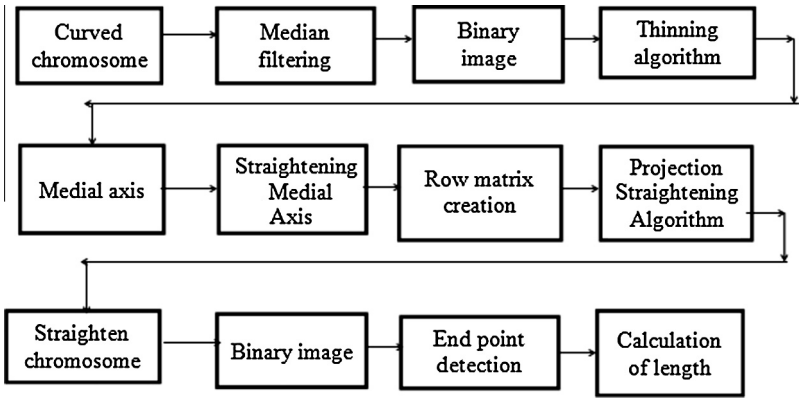


Fig. 2. The flow diagram for the straightening of chromosomes.

Fig. 3. Normal chromosome.

Fig. 4. curved chromosome.

$$\sigma_i^2(T) = \frac{1}{P_i(T)} \sum_{g=a}^{b} (g - \mu_i(T))^2 h(g) \tag{4.3}$$

where

$$a = \begin{cases} 0 & i = 1 \\ T+1 & i = 2 \end{cases} \quad \text{and} \quad a = \begin{cases} T & i = 1 \\ n & i = 2 \end{cases}$$

Now, the criterion function can be calculated as,

$$J(T) = 1 + 2[P_1(T)\log\sigma_1(T) + P_2(T)\log\sigma_2(T)] - 2[P_1(T)\log P_1(T) + P_2(T)\log(T)P_2(T)] \tag{4.4}$$

And the minimum error threshold is computed by minimizing the criterion $J(T)$.

2.4. D. Detection of the medial axis

Medial axis has to be extracted from the binary converted chromosome image, to obtain the skeleton [14] the chromosome image for this thinning algorithm is used. Three thinning algorithms are discussed of which efficient has to be considered. In parallel thinning algorithms, pixels are examined for deletion on the basis of results obtained only from the previous iteration. This algorithm has always received more considerable attention in the research area of parallel thinning as they have reduced the computation time in a number of iterations, and that is why they are sometimes called one-pass or fully parallel algorithms.

2.4.1. i. Zhang Suen Thinning algorithm

Zhang and Suen is a fast parallel thinning algorithm, which yields good results with respect to both connectivity and contour noise immunity. This method gives a better skeleton. Two sub-iterations are there. First sub-iteration removes south or east boundary pixels or north-west corner pixels. Second sub-iteration removes north or west boundary pixels or southeast corner pixels. If at the end of any sub-iteration there are no pixels to be deleted, the skeleton is completed. This method is fast and simple to implement; it counts with two sub iterations in which those pixels fulfilling the rules defined for iteration are removed. The Zhang-Suen algorithm consists of iteratively

deleting edge-points, while keeping endpoints, and also the shape connectedness should not be occurring. A pixel is a final point if it has a single black neighbor, being the rest all white. A pixel's connectivity is defined as the number of objects it could connect with the original image, and is computed turning round a pixel clockwise and counting how many color changes are produced. The number of changes will be the connectivity, i.e., The number of regions it connects.

This algorithm is made of two sub-iterations. In the fist one, a pixel $I\,(I, j)$ is deleted if the following condition is satisfied:

- *Step 1*. Its connectivity number is one.
- *Step 2*. It has at least two black neighbors and not more than six.
- *Step 3*. At least one of $I\,(I, j+1)$, $I\,(I-1, j)$, and $I\,(I, j-1)$ are white.
- *Step 4*. At least one of $I\,(i-1, j)$, $I\,(i+1, j)$, and $I\,(i, j-1)$ are white.

At the end, pixels satisfying these conditions will be deleted. If at the end of either sub-iteration there are no pixels to be deleted, then the algorithm stops.

2.4.2. ii. Stentiford thinning algorithm

Stentiford is a parallel thinning algorithm, which tends to produce lines that follow curves very well, resulting in vectors that more accurately reflect the original image. The objects are connected to a particular pixel. Zhang Suen Thinning algorithm, normal representation is used and objects connected point is not depending on particular pixel [15]. In our application Stentiford improves the Accuracy more than Zhang Suen. For this reason Stentiford is selected in our method.

The Stentiford algorithm can be stated as follows:

- *Step 1*. Find a pixel location (i, j) where the pixels in the image match those in template T1. With this template, all pixels along the top of the image are removed moving from left to right and from top to bottom.
- *Step 2*. If the central pixel is not an endpoint, and has connectivity number as 1, then mark this pixel for deletion. Endpoint pixel, is considered as endpoint if it is connected to just one other pixel. That is, if a black pixel has only one black neighbor out of the eight possible neighbors, then it is an endpoint pixel. Connectivity number, is a measure of how many objects are connected with a particular pixel.

$$C_n = \sum_{K \in S} N_K - (N_K \cdot N_{K+1} \cdot N_{K+2}) \tag{4.5}$$

where *N_K* is the color of the eight neighbors of the pixel analyzed. N0 is the center pixel. N1 is the color value of the pixel to the right of the central pixel and the rest are numbered in counterclockwise order around the center.

- *Step 3*. Repeat steps 1 and 2 for all pixel locations matching T1.
- *Step 4*. Repeat steps 1–3 for the rest of the templates: T2, T3, and T4. T2 will match pixels on the left side of the object, moving from bottom to top and from left to right. T3 will select pixels along the bottom of the image and move from right to left and from bottom to top. T4 locates pixels on the right side of the object.
- *Step 5*. Set white the pixels marked for deletion.

2.5. E. Straightening medial axis

Medial axis obtained from the Stentiford algorithm has to be straighten this is done so as to keep the straighten medial axis as reference for chromosome straightening method. Consider the number of thinned values in thinned image and mark those pixels in a single column. This gives straight line of medial axis which is the length of curved chromosome. Now with medial axis as reference further development can be proceed. Row matrix is created with reference to length of the straightened medial axis.

2.6. D. Projective Straightening Algorithm

The straighten medial axis is considered as reference and the chromosome image has to be projected on it as steps discussed.

- *Step 1*. Chromosome image which is curved is considered along with its medial axis, the first pixel in the medial axis is considered as template T1 and the neighbors are checked for white pixel to define the boundary. The pixels other than white are selected considering horizontally vertically and diagonal direction and are projected to the reference straightened medial axis.
- *Step 2*. Next pixel of medial axis considered and with first pixel as end point step 1 is repeated. It has at least two black neighbors and not more than six.
- *Step 3*. At least two of $I\,(I, j+1)$, $I\,(I-1, j)$, and $I\,(I, j-1)$ are white.
- *Step 4*. At least two of $I\,(i-1, j)$, $I\,(i+1, j)$, and $I\,(i, j-1)$ are white.
- *Step 3*. Steps 1, 2 are repeated until the last pixel of medial axis is achieved
- *Step 4*. The projected image gives the straighten image.
- *Step 5*. Calculate the length of the straightened chromosome.

Considering the end points of the medial axis distance between the end points is calculated using the following formulas which give the length of the chromosome.

Euclidean distance considers the coordinates

$$D = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2} \tag{4.6}$$

City Block Distance calculates Up–Down and Left–Right

$$D = |x_2 - x_1| + |y_2 - y_1| \tag{4.7}$$

Chessboard distance calculates at any direction (King Move)

$$D = \max(|x_2 - x_1| + |y_2 - y_1|) \tag{4.8}$$

3. Results and discussion

The Straightening of the curved chromosome using a Projective Straightening Algorithm is simulated using MATLAB 2011a. The G-band images are cytogenetic data obtained by staining the chromosomes with geisma, a fluorescent dye that concentrates in different regions of the chromosomes, giving rise to the characteristic banding patterns that identify the different chromosome types. The images appear as a white background onto which the chromosomes stand out with a bright and dark banding. The proposed method uses the image with the resolution of 768×576 and this method works well for calculating length, area and curve angle for the input image. Forty-six chromosomes of an individual are considered for straightening and processed.

3.1. Simulation results

3.1.1. Image acquisition

Chromosome images were acquired by microscopic imaging of metaphase or prophase cells on specimen slides and the images are provided as input for straightening and length calculation purpose. Table 5.1 gives the distribution of the bend angles of the chromosomes in the dataset. Three sample chromosomes 1, 2 and 6 are considered as Input image for straightening and it is shown in Fig. 5.1. The stored images from 1 to 46 are of various length each length has to be calculated after straightening the chromosomes.

Highly curved and moderately curved chromosomes are to be straightened with care to extract the genetic information and dimensions without any variation.

Table 5.1
Distribution of the bend angles of the chromosomes in the dataset.

	Highly curved (less than 150°)	Curved (range 150–170°)	Slightly curved (range 170–180°)
Chromosomes in dataset (%)	21.8	43.4	34.8

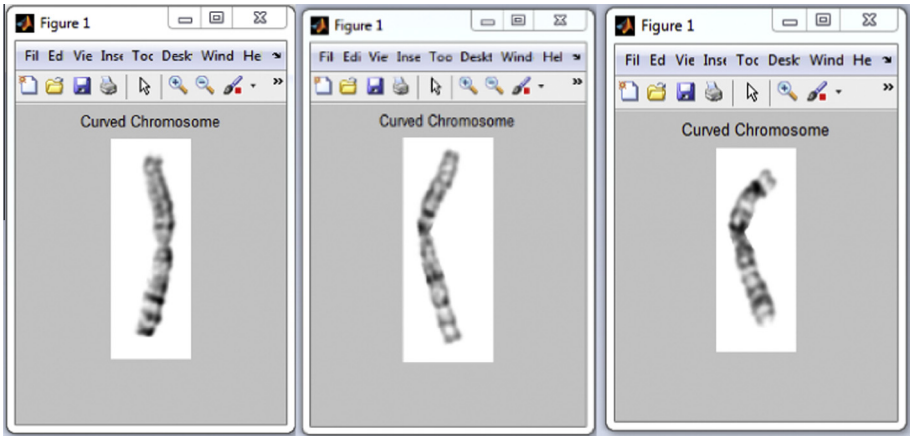


Fig. 5.1. Curved chromosomes.

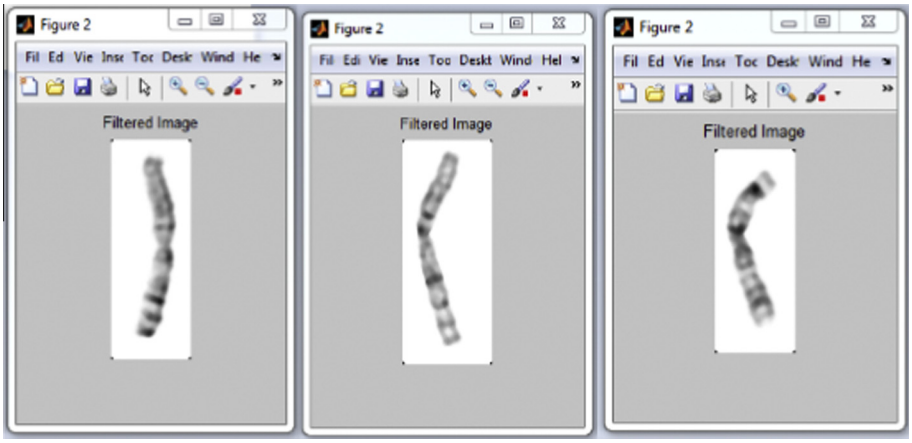


Fig. 5.2. Median filter applied chromosome image.

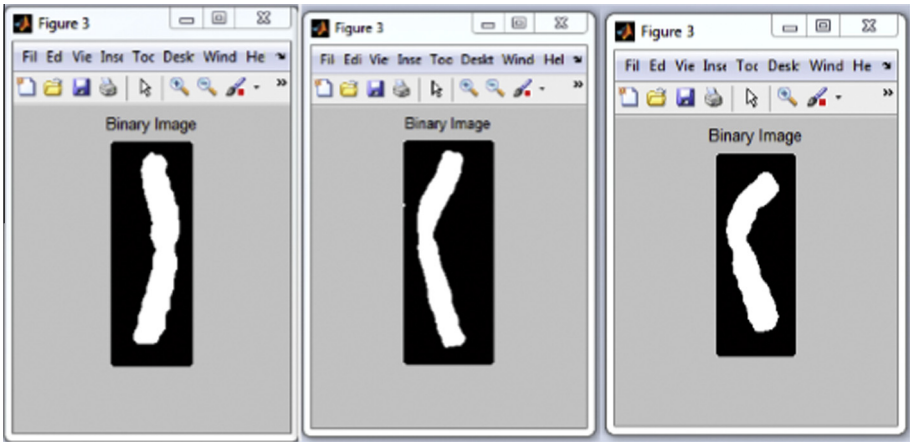


Fig. 5.3. Binary image.

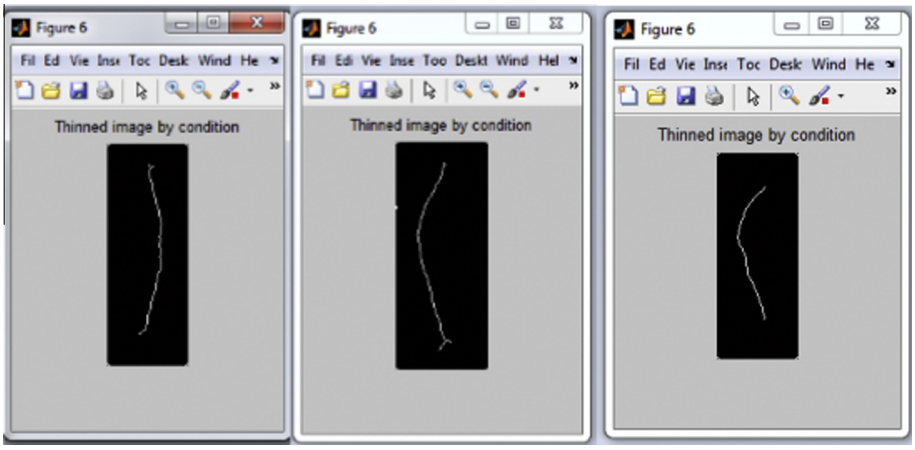


Fig. 5.4. Medial axis of chromosome.

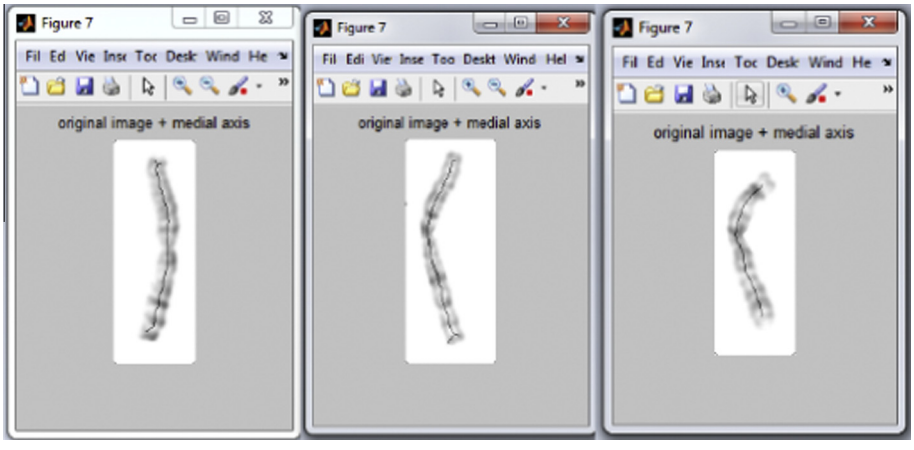


Fig. 5.5. Medial axis overlapped on original curved chromosome.

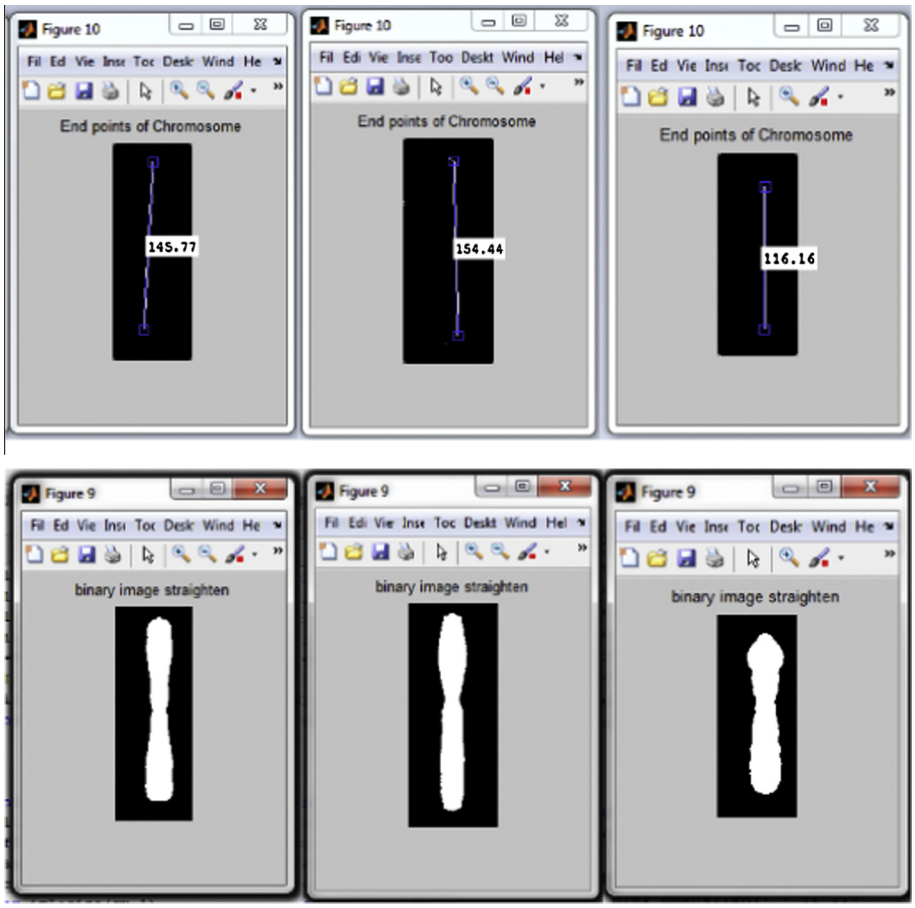


Fig. 5.6. Length of chromosome obtained from straighten medial axis.

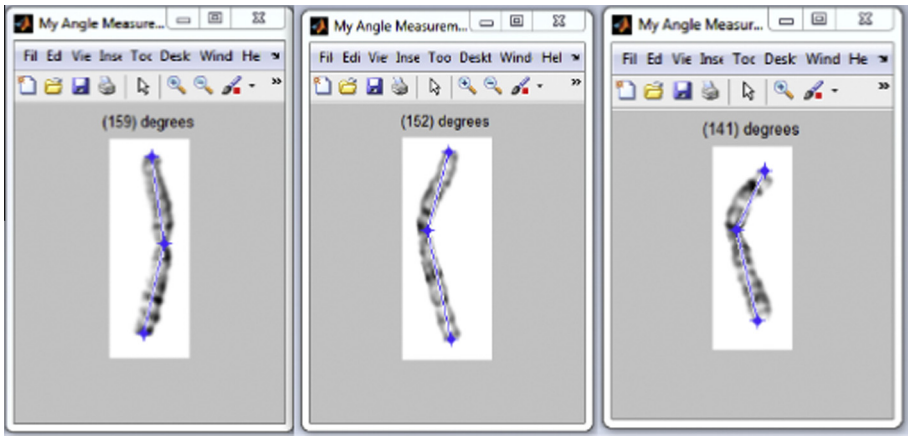


Fig. 5.7. Angle measurement for curved chromosomes.

3.1.2. Preprocessing

The curved chromosome image is applied 3 × 3 median filter and the spikes are removed. Fig. 5.2 shows the spikes removed image of curved chromosomes.

3.1.3. Binary image and medial axis

The filtered chromosome image is processed with kettler method thresholding and the binary image consisting of 1's and 0's are obtained. Fig. 5.3 shows the binary image

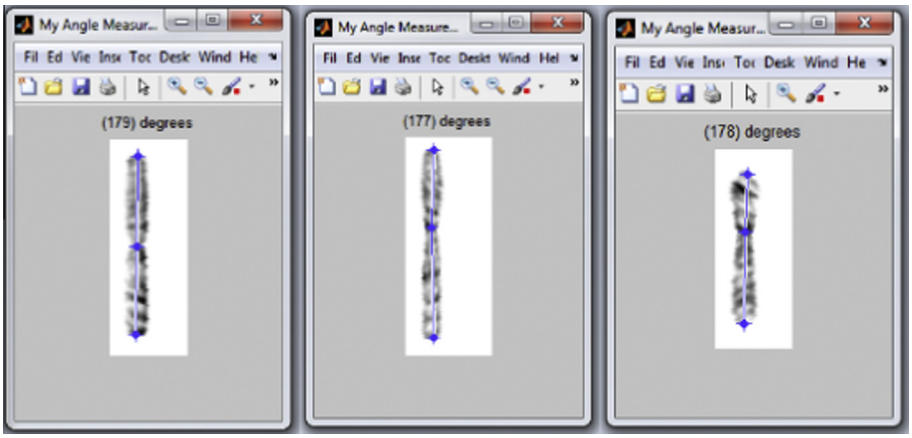


Fig. 5.8. Angle measurement for straighten chromosome.

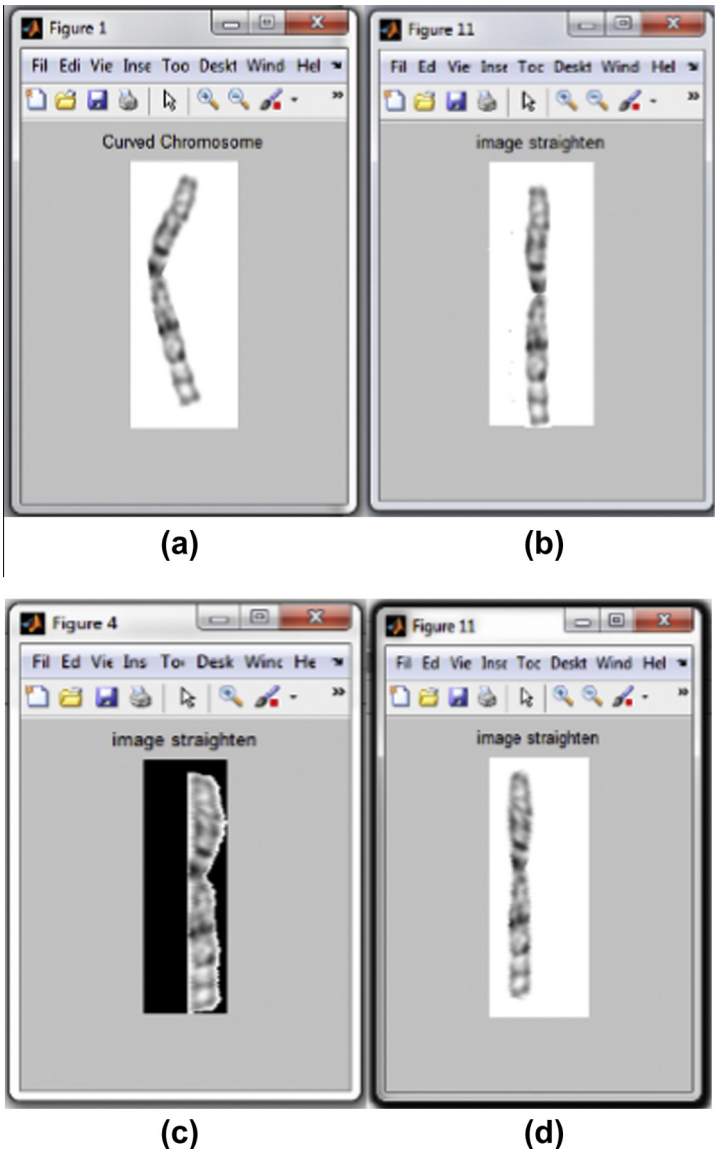


Fig. 5.9. Chromosome 1 straightened using (a) curved chromosome(152°), (b) varying rotation angles (172°), (c) forward mapping (173°) and (d) proposed algorithm (177°).

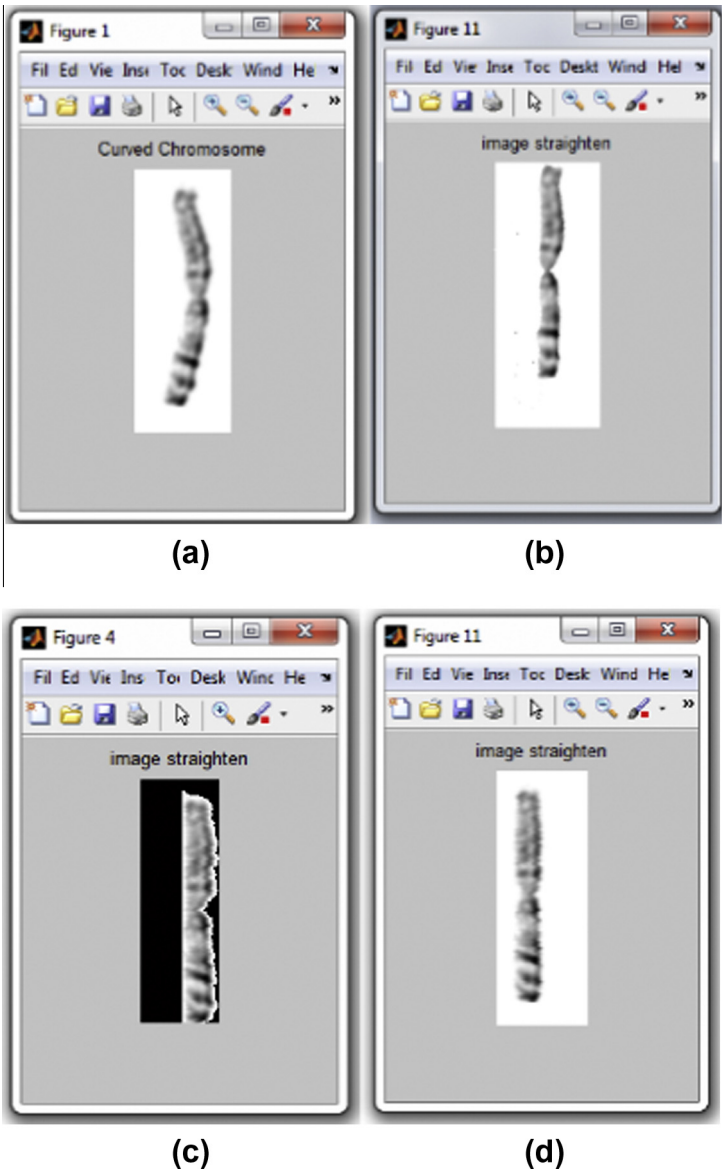


Fig. 5.10. Chromosome 2 straightened using (a) curve chromosome(141°), (b) varying rotation angles (169°), (c) forward mapping (173°) and (d) proposed algorithm (178°).

of filtered chromosome by application of kittler method. Binary image is obtained using ostu's method and kettler method of which later thresholding method provides better efficient.

The binary image of chromosome is applied to the Stentiford thinning algorithm, which gives the skeleton of the chromosome. Fig. 5.4 explains it in diagrammatic fashion. The skeleton image of the chromosome gives the structure to chromosome so by modifying the skeleton the shape of the chromosome can be varied.

The medial axis obtained is straightened and kept as reference, the medial axis is over lapped with the original image as shown in Fig. 5.5. The end pixel of the medial axis is considered and Projective Straightening Algorithm is applied to that endpoint pixel and the same is applied to the next pixels.

The endpoints are obtained from the medial axis straightened. The distance between the end points are obtained using Euclidean distance formula as shown in Fig. 5.6.

The length of each chromosome have standard size, starting from chromosome number 1–44 chromosome size are in ascending fashion. Three methods of distance calculation is adopted for chromosome length calculation. Euclidean, city block and checker board methods considered, of which Euclidean gives the close enough standard distance value.

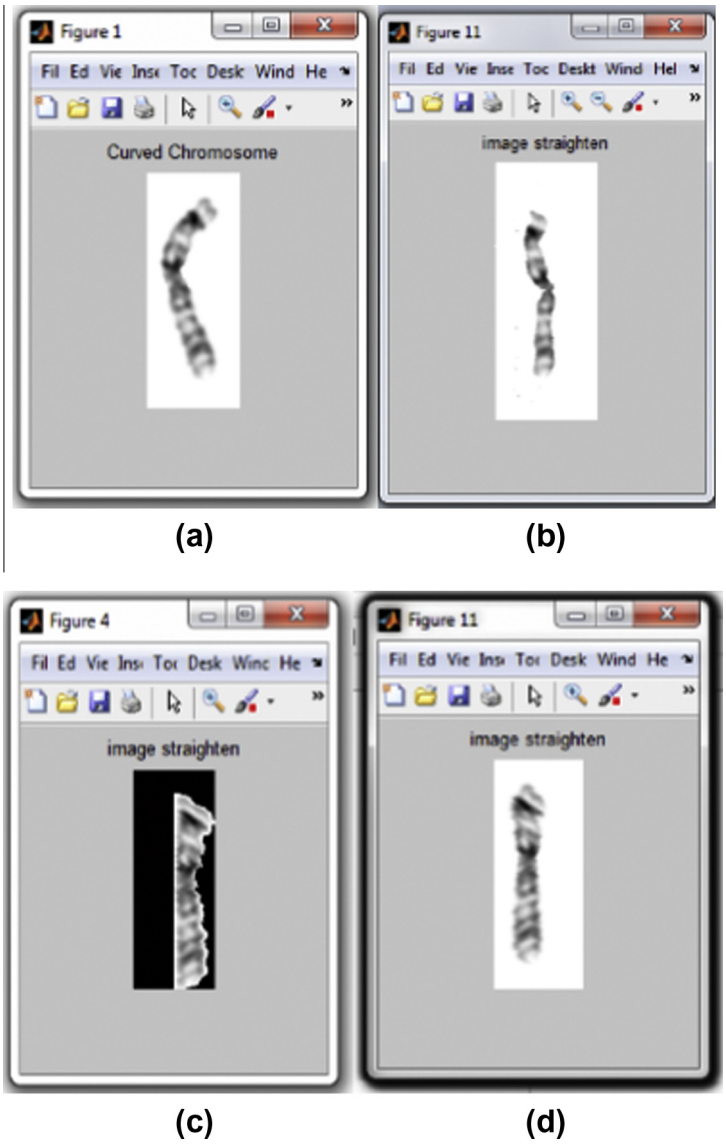


Fig. 5.11. Chromosome 6 straightened using (a) curved chromosome (159°), (b) varying rotation angles (172°), (c) forward mapping (176°) and (d) proposed algorithm (179°).

Angle measurement gives the proof for straightening of chromosome. Figs. 5.7 and 5.8 show the method of measuring angle for curved and straighten chromosome.

The dataset which consists of curved chromosomes are grouped into three based on the angle curved. Highly, slightly and moderately curved are the three groups. From proposed method algorithm all the three group chromosomes are straighten closely up to 178°.

Chromosome straightening methods are already available but those are not efficient. Figs. 5.9–5.11 give the comparison of straighten image by varying rotation angle, forward mapping and Projective Straightening Algorithm methods.

The comparison shows that the proposed projective straightening method is more efficient compared to the varying rotation angle and forward mapping method. The genetic information of chromosome is unchanged in our proposed method process.

The length of each chromosome is compared with the standard length, if the difference is found to be more than acceptable level, then we can conclude that there is some deletion in genetic material in that length differed chromosome. Processing steps in proposed algorithm is shown in Fig. 5.12.

Standard deviation is obtained by considering all the test result angle corrected and the deviation from desired angle. The maximum angle is examined by considering the angles which give maximum deviation from required result. The length area and angle corrected for the straightened chromosomes of 23 pairs are noted and are tabulated

Fig. 5.12. Processing steps in proposed algorithm.

Table 5.2
Comparison with existing method.

	Varying rotation angle method [7]	Forward mapping algorithm [16]	Proposed method
Mean°	7.3	6.5	4.6
Standard deviation°	4.6	3.9	2
Maximum°	11.4	9	7

Table 5.3
Length, area and angle after straightening 46 chromosome images.

Chromosome No.	Length (pixels)	Angle curved (°)	Angle corrected (°)	Area (pixels)
1	145.19	159	179	3549
2	154.05	152	177	3506.4
3	128.25	149	178	3439.9
4	138.15	131	179	3312
5	120.53	169	179	2850.6
6	116.45	141	178	2789.1
7	114.65	165	177	2874.3
8	104.85	171	176	2531.5
9	104.54	173	180	2606.8
10	97.89	134	176	2735.9
11	99.70	162	176	2542.3
12	94.87	149	178	2451.5
13	93.56	171	176	2309.5
14	91.88	169	179	2228.1
15	79.74	158	177	1921
16	75.01	105	173	1986.8
17	73.58	163	178	1889.3
18	70.04	166	176	1788.4
19	68.39	156	178	1974.9
20	70.66	176	179	1864.3
21	72.45	157	176	1918.5
22	70.85	159	177	1900.1
23	65.02	170	179	1932.3
24	78.55	163	178	2087
25	57.05	173	179	1587.3
26	63.08	174	177	1512.8
27	62.03	175	179	1451
28	59.92	135	176	1553.9
29	57.72	161	175	1396.8
30	52.02	166	177	1516
31	47.42	156	179	1338.4
32	42.96	171	178	1252.1
33	42.54	154	177	1200.8
34	41.87	102	173	1223.9
35	41.38	148	177	1191.8
36	37.45	176	179	1141.1
37	34.57	177	179	907.500
38	33.07	175	180	895.1250
39	29.07	176	178	937.1250
40	28.54	170	179	970.2500
41	27.8	172	178	637.3750
42	26.75	175	179	611.5000
43	25.87	165	178	717.1250
44	23.45	107	175	758.2500
x	81.45	158	178	2159.3
y	26.87	174	179	711.5000

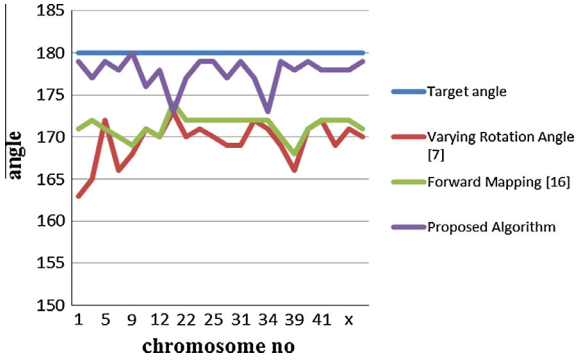


Fig. 5.13. Proposed vs. existing method on chromosome straightening.

in Table 5.2. The length of each chromosome is compared with the standard measure, from the findings deletion and dislocation in the genetic material of chromosome can be identified.

Forty-six chromosomes of an individual are considered for straightening purpose. The proposed method algorithm is applied to those chromosome images. Considering the end points of the medial axis distance between the end points is calculated using the Euclidean distance formula, which give the length of the chromosome. The length of each chromosome is compared with the standard length, if the difference is found to be more than acceptable level, then we can conclude that there is some deletion in genetic material in that length differed chromosome.

Angle measurement gives the proof for straightening of chromosome. The dataset which consists of curved chromosomes are grouped into three based on the angle curved. Highly, slightly and moderately curved are the three groups. From proposed method algorithm all the

three group chromosomes are straighten closely up to 178°, which is evident from Table 5.3.

The Area of each chromosome has standard value, the values are compared with the proposed method's value. High difference between the area values concludes that there is some deletion in genetic material. Area measured in the proposed method is based on number of pixels occupied by the chromosome image.

Varying rotation angle method, forward mapping method and Projective Straightening Algorithm methods straightened images are checked for straighten angle, it is shown in Fig. 5.12. The proposed algorithm gives the better straightening result compared to the existing methods. The proposed method straightens the curved chromosomes closely up to 178° compared to Varying rotation angles method's 175.4° and Forward mapping algorithm's 176.1°.

4. Conclusion

Projective Straightening Algorithm for chromosome straightening is executed using MATLAB. The proposed algorithm applied to the chromosome images in the database is effective to alter the curved images of the human chromosomes into straight one. The performance index of straightening human chromosomes i.e., length of each chromosome, is compared with the standard length, if the difference is found to be more than acceptable level, then we can conclude that there is some deletion in genetic material in that length differed chromosome (see Fig. 5.13).

The proposed method straightens the curved chromosomes closely up to 178° compared to Varying rotation angles method's 175.4° and Forward mapping algorithm's 176.1°. The proposed method is capable of changing chromosome shapes at any points along the entire length of the chromosome. This efficient technique meets the following two requirements: First, the length and width of the original chromosome image remains unchanged, when the altered chromosome is created. Second, the original information including the grayscale values and G-bands information is kept as close as possible to the newly generated model.

References

[1] S.D. Barrett, C.R. DeCarvalho, A software tool to straighten curved chromosome images, IEEE Engineering in Medicine and Biology 5 (11) (2003) 83–88.
[2] A. Carothers, J.H. Melnyk, J. Piper, Computer-aided classification of human chromosomes, IEEE Computer Graphics and Applications 3 (11) (1994) 161–171.
[3] A. Carothers, J. Piper, Classification of human chromosomes by banding patterns, IEEE Computer Graphics and Applications 5 (16) (1996) 145–151.
[4] K.R. Castleman, J.H. Melnyk, Automated System for Chromosome Analysis, Final Report, Jet Propulsion Laboratory, Pasadena, California, 1976.
[5] J.M. Cho, Chromosome classification using back propagation neural network, IEEE Engineering in Medicine and Biology 8 (18) (2000) 28–33.
[6] P.S. Heckbert, Survey of texture mapping, IEEE Computer Graphics and Applications 6 (11) (1986) 56–67.
[7] M. Javan Roshtkhari, S.K. Setarehdan, A novel algorithm for straightening highly curved images of human chromosome, Pattern Recognition Letters 29 (19) (2008) 1208–1217.
[8] R. Keys, Cubic convolution interpolation for digital image processing, IEEE Transactions on Acoustics, Speech and Signal Processing 29 (6) (1981) 1153–1160.
[9] Mehdi Moradia, S. Kamaledin Setarehdan, New features for automatic classification of human chromosomes: a feasibility study, Pattern Recognition Letters 27 (9) (2006) 19–28.
[10] M. Moradi, S.K. Setarehdan, S.R. Ghaffari, Automatic locating the centromere on human chromosome pictures, in: Proceedings of the 16th IEEE Symposium on Computer-based Medical Systems, vol. 9, No. 18, 2003, pp. 56–61.
[11] Qiang Wu, Zhongmin Liu, Tiehan Chen, Zixiang Xiong, Kenneth R. Castleman, Subspace-based prototyping and classification of chromosome images, IEEE Transactions on Image Processing 14 (9) (2005) 1277–1282.
[12] Ronald J. Stanley, James M. Keller, Data-driven homologue matching for chromosome identification, IEEE Transactions on Medical Imaging 17 (3) (1998) 451–462.
[13] Sahar Jahani, Seyed Kamaledin Setarehdan, Centromere and length detection in artificially straightened highly curved human chromosomes, International Journal of Biological Engineering 2 (5) (2012) 56–61.
[14] Shadab Khan, Alisha D Souza, Joao Sanches, Rodrigo Ventura, Geometric correction of deformed chromosomes for automatic karyotyping, IEEE Transactions on Medical Imaging 21 (5) (2012) 51–62.
[15] P. Subashini, S. Jansi, Optimal thinning algorithm for detection of FCD in MRI images, International Journal of Scientific and Engineering Research 2 (9) (2011) 125–133.
[16] Wei Wu, Xiaoli Yang, Charles C. Tseng, Effective algorithms for altering human chromosomes shapes, International Journal of Scientific and Engineering Research 3 (9) (2012) 124–131.

INTEGRATION, the VLSI journal 47 (2014) 123–129

Contents lists available at ScienceDirect

INTEGRATION, the VLSI journal

journal homepage: www.elsevier.com/locate/vlsi

Hardware implementation of tag-reader mutual authentication protocol for RFID systems

V.R. Vijaykumar [a,*], S. Elango [b]

[a] Department of Electronics and Communication Engineering, Anna University, Coimbatore, Coimbatore-641047, Tamil Nadu, India
[b] Department of Electronics and Communication Engineering, Bannari Amman Institute of Technology, Sathyamangalam, Erode-638401, Tamil Nadu, India

ARTICLE INFO

Article history:
Received 13 September 2012
Received in revised form
24 January 2013
Accepted 6 March 2013
Available online 21 March 2013

Keywords:
Authentication protocol
Field programmable gate array
RFID
Linear feedback shift register
Truncated multiplier

ABSTRACT

Radio-frequency identification (RFID) is a recent technology that utilizes radio frequencies to track the object by transmitting a signal with a unique serial identity. Generally, the drawbacks of RFID technology are high cost and authentication systems between a reader and a tag become weak. In this paper, we proposed a protocol for RFID tag–reader mutual authentication scheme which is hardware efficient and consumes less dynamic power. Truncated multipliers are implemented in RFID tag–reader mutual authentication protocol system due to reduction in hardware cost and dynamic power. Experimental evaluation reveals that the proposed protocol with truncated multipliers provides more security than the earlier schemes. The proposed protocol is described in VHDL and simulated using Altera Quartus II. The functional block is implemented as hardware using an Altera DE2 Cyclone II (EP2C35F672C6) Field-Programmable Gate Array (FPGA).

1. Introduction

An RFID tag stores the information electronically which can be read from several meters away without having contact between tag and reader. Tag consists of an integrated circuit for handling data and an antenna for receiving and transmitting a radio-frequency signal. The RFID system utilizes one of three general band's low frequency (LF) at 125 kHz to 134 kHz, high frequency (HF) at 13.56 MHz, and Ultra HF at 860 MHz to 930 MHz [1,2]. RFID tags contain a unique serial number namely electronic product code (EPC) that can individually identify every single tagged item [3,4]. Electronic product Code Class 1 generation 2 (EPC C1G2) provides only very basic security tools using a 16 bits pseudorandom number generator (PRNG) [5]. The LFSR can be created using the Galois or Fibonacci configuration of gates and registers. Fibonacci implementation, the output from some of the registers is EX-ORed with each other and fed back to the input of the shift register. Fibonacci LFSR is more suitable for hardware implementation than the Galios LFSR [6–8]. A light authentication protocols that use only efficient bitwise operations (such as EX-OR, AND, OR, addition etc.) on tags have been defined in [9]. In [10] Hernandez-Castro et al. proposed an efficient protocol for low cost RFID tags in which number of addition operation reduced compared to [9]. An additional rotation operation is used for authentication protocol in [11]. Konidala et al. [12] proposed a protocol that utilized tag's access and kill passwords for the tag–reader mutual authentication scheme based on EX-OR operation.

In Peris-Lopez et al. [13] uses a MixBits function that require many iterations to complete, which leads to increase the hardware cost. Huang et al. [14] modified the Padgen function proposed by Konidala et al. and implemented a protocol in FPGA. Li et al. [15] proposed a EX-OR scheme for an efficient implementation of protocol. Schulte et al. [16] states that the power dissipation of a truncated multiplier is less compared to a standard multiplier. Wang et al. [17] states that truncated multiplier is used for lossy applications. Ko and Hsiao proposed an efficient array based truncated multiplier, which consume less power and utilized fewer hardware resources [18]. Selwyn discussed a various RFID Mutual authentication protocol in [19,20] in order to identify the vulnerabilities in protocols. In another work Cho et al. [21] analyzed, securing against brute-force attack of a hash function based authentication protocols. All the above protocols are fails in any one of the following aspects such as cost, security, power consumption and possibility of backward processing of the operation or function. In this paper truncated multiplier is used to encode the information during a mutual authentication process, it reduces the hardware cost, strengthening security and consumes less power to perform this multiplication. In addition to that, number of bit processing is fewer which lead to reduction in the bit length and their no possibility of finding the information by performing backward processing. The rest of this paper is organized as follows. In Section 2, we present the background and its related work on the RFID reader-to-tag authentication protocol.

* Corresponding author. Tel.: +919442014139.
E-mail addresses: vr_vijay@hotmail.com (V.R. Vijaykumar), eceelango@gmail.com (S. Elango).

0167-9260/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.vlsi.2013.03.002

The Proposed mutual authentication protocol is discussed in Section 3. Section 4 shows the simulation and implementation results of the mutual authentication scheme. Finally, we conclude the paper in Section 5.

2. Background and related works

RFID systems work, whenever a reader antenna emits a radio frequency signal. Tag pick up that radio signal and respond to a reader. Reader reads the signal which is responded by tag. The reader is act as a transceiver (i.e., a combination of transmitter and receiver) because their usual role is to request a tag and receive information from tag. The antenna can be a separate device, or it can be an integrated within a reader [1].

2.1. EPC class-1generation-2 standard

The access password is a 32-bit value stored in the tag's reserved memory if this password is set, then data transfer will be established between tag and reader. Initially reader requests a random number from the tag. Tag generates a random number and sends to reader. The reader cover codes the password by performing a bitwise EX-OR between password and random number. The generated EX-OR output is transmits to the tag. The tag decodes the coded password by performing a bitwise EX-OR of the received cover-coded string with the original as shown in Fig. 1 [5].

In this scheme, both the random number sends un-encrypted form. Man in middle attack is possible to happen by carrying out EX-OR operation between the cover coded passwords with random number, which provides access password and their by malicious reader to illegally access the tag's data [12].

2.2. Konidala mutual authentication scheme

In Konidala et al. [12] proposed a scheme where the server, reader, and the tag follows a multi-step tag–reader mutual authentication procedure as shown in Fig. 2. It uses the tag's 32 bit access and kill passwords in order to perform tag–reader mutual authentication. This protocol uses two rounds of Pad generation function (Padgen) to compute a cover-coding pad. The first round of Padgen function performs over the access password, while the second round of Padgen function performs over the kill password. The Padgen function is used to generate a 16 bit pads for "cover coding" the access password. The main drawbacks of this scheme, it is not implemented as hardware. To perform a single Padgen function it requires much more logical operation also its leads to increase the hardware cost and consume much dynamic power due to increase in the number of transition. To overcome the drawbacks of the above scheme Huang et al. [14] implemented a protocol in FPGA with modified Padgen function, but it increases the hardware cost.

3. Proposed mutual authentication scheme

3.1. Proposed protocol

The protocol consists of three main component's tag, reader and server or database. In the proposed protocol, each tag has an individual EPC, Password (PWD) and a common architecture (truncated multiplier function) provided by manufacturer to encrypt PWD. The database has the information about EPC and PWD of all tags. It also has a common protocol architecture which is embedded in all tags.

Fig. 3. describes the proposed protocol communication step between a reader and a tag. The detailed description of the proposed protocol is as follows:

Step 1: Initially, reader sends a request message to a tag.
Step 2: The tag responds by generating a new random number RTI.
Step 3: The EPC, RT1 information is sent to the server through the reader.
Step 4: The server then computes a CCPWDRT (cover coded password computed by reader from RT1) from truncated multiplier function and generates a new random number RM1 and transmitted to the tag.
Step 5: The tag performs a truncated multiplier function with RT1 and PWD to compute CCPWDTT (cover coded password computed by tag from RT1).

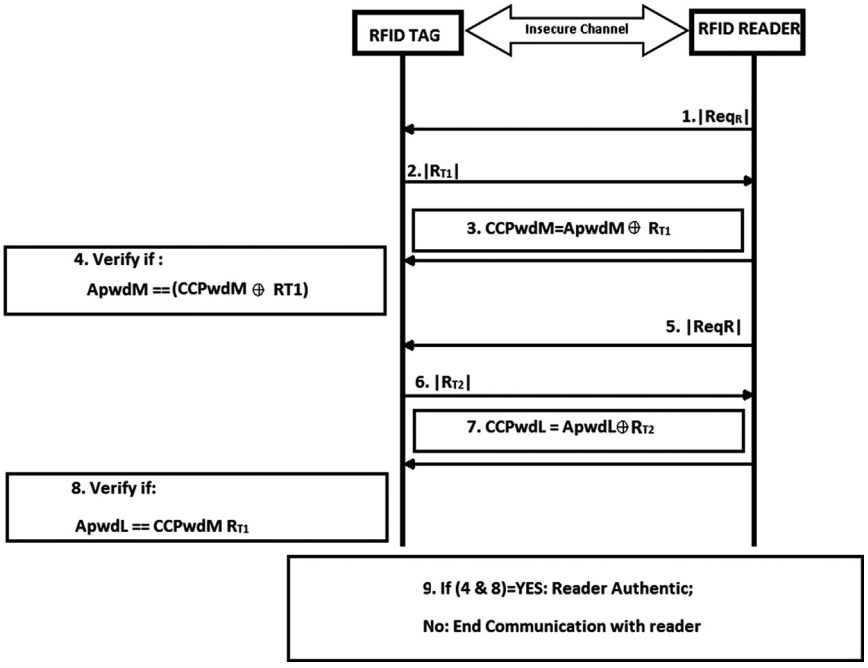


Fig. 1. Authentication scheme proposed by EPC global [5].

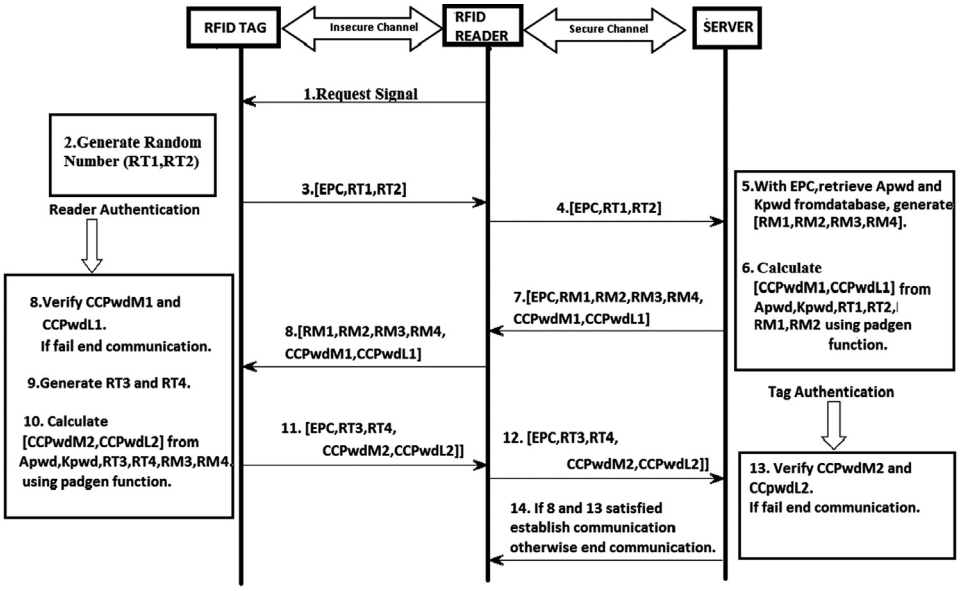


Fig. 2. Konidala tag–reader mutual authentication scheme [12].

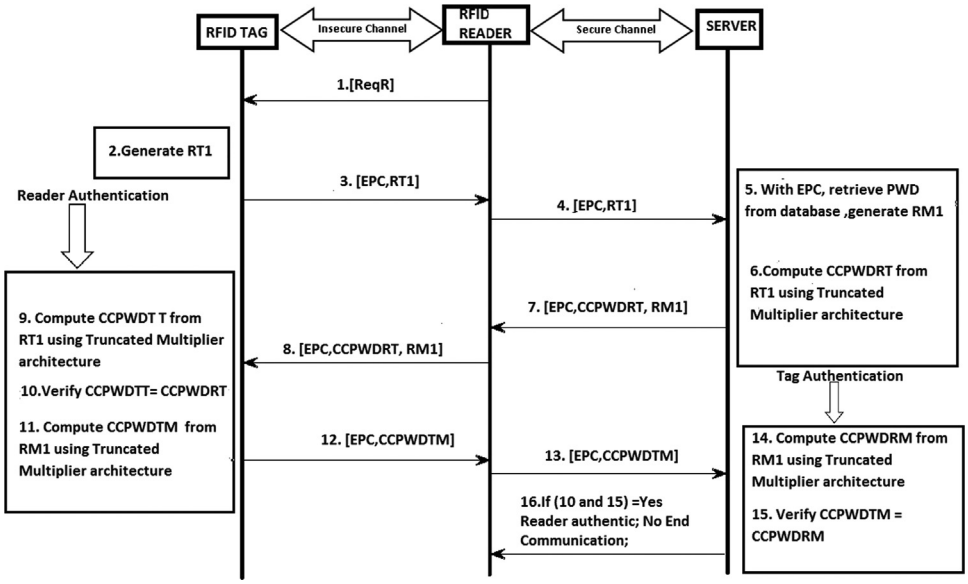


Fig. 3. Proposed RFID mutual authentication protocol.

Step 6: Verification of CCPWDRT=CCPWDTT is done. If it is satisfied, the process continues otherwise communication is ended.

Step 7: The tag computes a CCPWDTM (cover coded password computed by tag from RM1) from truncated multiplier function, and the same is transmitted to the server.

Step 8: The server performs a truncated multiplier function with RM1 and PWD to compute CCPWDRM (cover coded password computed by reader from RM1).

Step 9: Verification of CCPWDRM=CCPWDTM is done. If it is satisfied, the process continues otherwise communication is ended.

3.2. Truncated multiplier as encrypter

A standard digital n–x–n multiplier computes the $2n$ bit product, but truncated multipliers compute only n most significant bits (MSBs) of the $2n$ bit product. Many researchers have been made to design a truncated multiplier [18]. Hars [22] is the first author who describes the truncated multiplier can be used for cryptographic applications. Each author can design their own truncated multiplier architecture according to their requirements, but the final output results of the truncated multiplier vary with respect to the architecture. In the proposed scheme, truncated multiplier is used to encode function in the functional block shown in Figs. 3 and 5. The behavior of truncated multiplier converts a data of n bit into some other n bit data. Hence it is used to encrypt the data send from tag to reader and vice versa. To justify the above statement, let us consider the inputs a and b for truncated multiplier where a=00011011(27), b=00011011(27). When the input is processed in truncated multiplier, actual output of standard multiplier is 0000001011011001(729), but it produces an error output as 00000011~~00000000~~(768) according to the architecture. This result shows that the truncated multiplier converts the input value from one form to some other form. Hence

it can be used to encode the password. If anyone tapped the information they can able to get the encoded bits. These bits are not possible to retrieve the information until they know the architecture of truncated multiplier. The reasons behind for choosing truncated multiplier in this protocol is that it provides an efficient method for reducing the hardware cost compare to Padgen function, avoids growth in word-size and also used as an encoder. In our protocol the efficient truncated multiplier architecture which is recently proposed by Ko and Hsiao [18] is used for encrypt the password.

3.3. Linear feedback shift register (LFSR)

The LFSR is important in many areas of communications, computing and VLSI circuit testing, such as cryptography, spread-spectrum communications, signature analyzer, etc. It provides a fast and efficient method for generating a wide variety of random sequences [6]. In LFSR, the outputs of a selected number of stages are fed back to the input of the LFSR through an EX-OR module. An n bit LFSR requires n clock cycle to generate $2n-1$ nonzero binary patterns in sequence. This sequence is termed the maximal length sequence of the LFSR [8]. Feedback position of the LFSR controls the initial value of random number and also sequence of the pattern generated. Fig. 4a shows that the general representation of an n bit LFSR that generate a random number for each clock pulse. A 16 bit LFSR requires, a 16 flip flops with few EX-OR gates for a random number generation as shown in Fig. 4b [14].

3.4. Protocol architecture

The proposed protocol utilizes the tag's 32 bit password in achieving tag–reader mutual authentication as shown in Fig. 5. This scheme uses truncated multiplier function to compute a cover-coded password. The output of this functional block is used to create the 16 bit cover-coded password of tag or reader (CCPWDXX) by using Eqs. (1)–(5).

$$M1\,(15:0) = [R(15:0)]\text{XOR}[\text{PWDL}(15:0)] \tag{1}$$

$$M2(15:0) = \{[R\,(15:0)]\ \text{XOR}\ [\text{PWDM}\,(31:16)]\} \tag{2}$$

$$\text{LSB}\,(7:0) = \text{TMF}\,[M1\,(15:8), M2\,(7:0)] \tag{3}$$

$$\text{MSB}\,(15:8) = \text{TMF}\,[M1\,(7:0), M2\,(15:8)] \tag{4}$$

$$\text{CCPWDXX}\,[15:0] = \text{MSB} \,||\, \text{LSB} \tag{5}$$

where R (15:0) is 16 bit random number (LFSR) and TMF is truncated multiplier function.

4. Results and discussion

4.1. Simulation results

The proposed and other state of art RFID mutual authentication protocols are described using structural VHDL to produce gate level netlist and synthesized using Altera Quartus II tool. Here

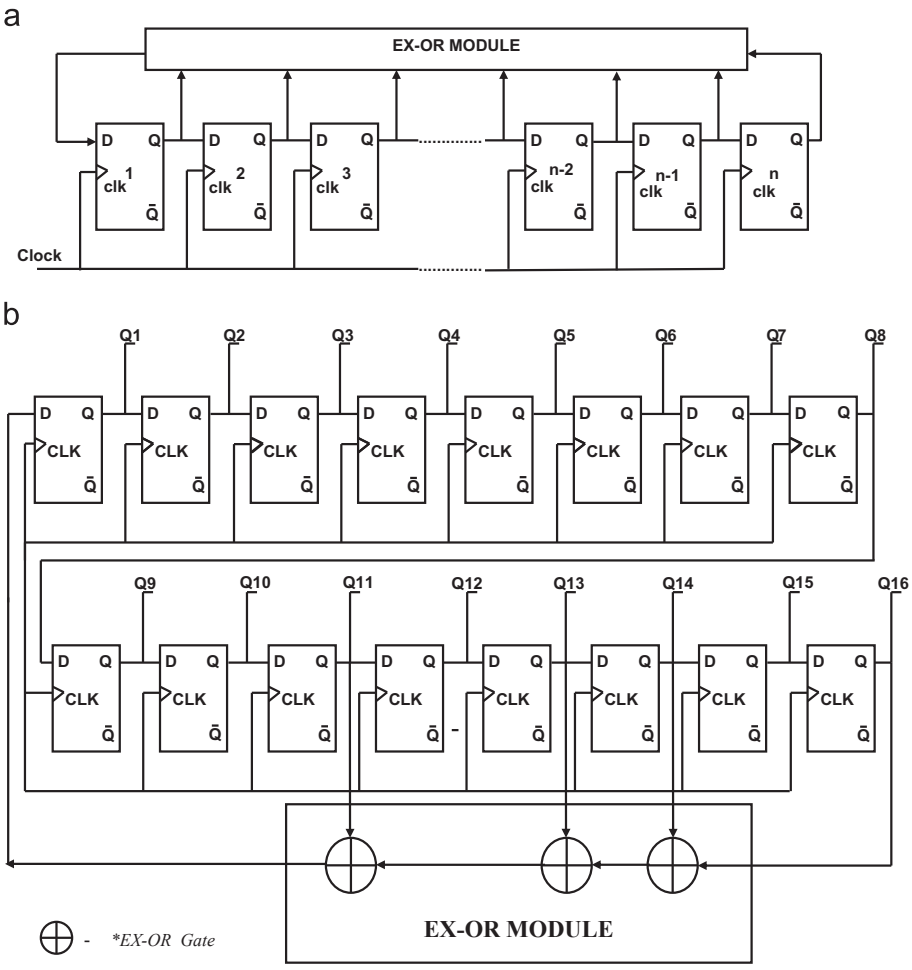
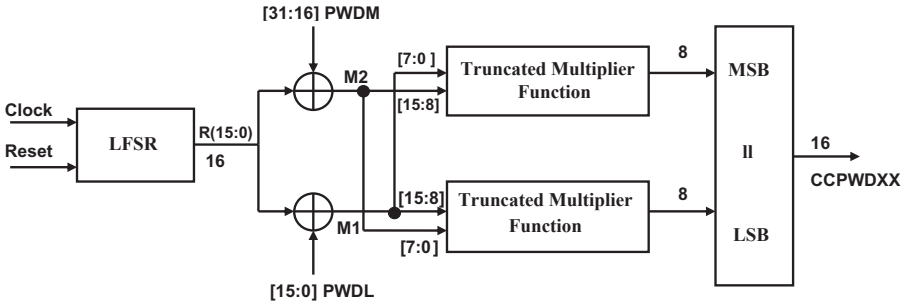


Fig. 4. (a) General representation of n bit LFSR [8]. (b) Sixteen bit LFSR.



*||concatenates its right operand to the end of its left operand.

Fig. 5. Functional block diagram in the mutual authentication scheme.

Table 1
Comparison of logic elements and register count of proposed protocol with earlier schemes.

Parameters	LMAP [9]	EMAP[10]	SASI [11]	Konidala [12]	M^{3}AP [13]	Huang [14]	Lin (XOR scheme) [15]	Proposed protocol
Logic elements	656	436	404	724	2484	692	932	**534**
Total number of registers	32	32	32	128	128	128	128	**32**

Table 2
Comparison of power, delay and PDP estimation of proposed protocol with earlier schemes.

Parameters	LMAP [9]	EMAP [10]	SASI [11]	Konidala [12]	M^{3}AP [13]	Huang [14]	Lin (XOR Scheme) [15]	Proposed protocol
Propagation delay (ns)	20.411	21.027	19.764	23.530	13.875	22.434	22.391	**24.921**
Clock to output delay (ns)	17.009	20.339	16.330	19.536	17.437	19.486	20.516	**22.194**
Critical path register to register delay (ns)	1.172	1.418	1.398	1.147	101.279	1.147	1.167	**1.147**
Dynamic power dissipation (mW)	91.14	89.9	55.06	51.56	56.98	33.88	37.48	**30.32**
PDP (pJ)	1860	1890	1088	1213	790	760	839	**755**

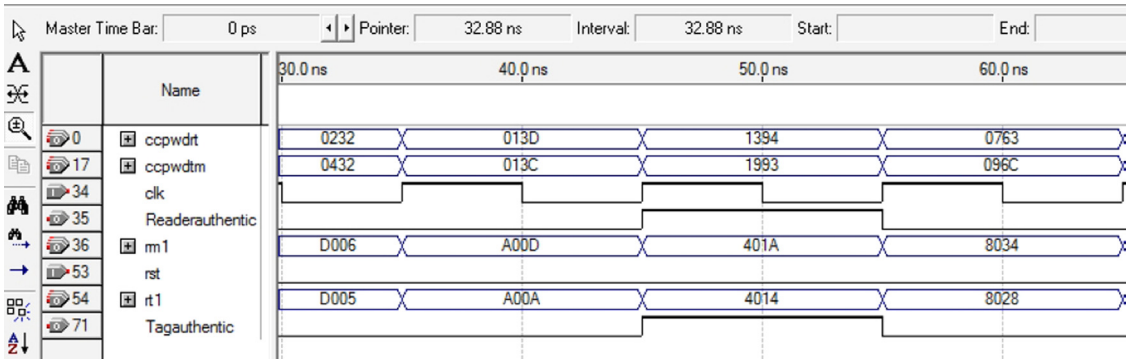


Fig. 6. Simulation results of proposed scheme.

seven different RFID tag–reader authentication protocol namely LMAP, EMAP, SASI, Konidala Scheme, M3AP, Huang et al. and Lin et al. are considered for comparison [9–15].

The logical element requirement to perform a single time MixBits, Padgen, truncated multiplier function is 2016, 160, 110, respectively. Each protocol may utilize the function eight times to complete a single authentication process. The logical elements of truncated multiplier and number of transition required to complete a truncated multiplier function is less compared to other functions like Padgen, MixBits etc., which is used in other protocols to cover code the password. From the synthesis results in Table 1, it is shown that the logical elements of the protocol [10,11] are low, but it consumes high power due to number of transition increases. The reason for increased number of transitions is that, it needs to be updating the value for each iteration by performing some logical operation after each authentication process. Protocol [12–14] use a Padgen function to encrypt the password since

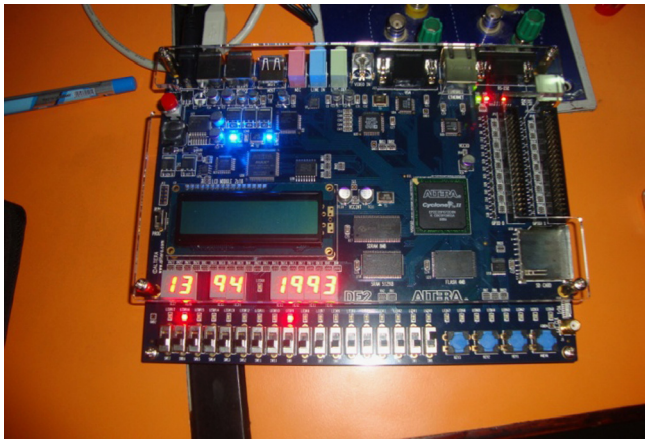


Fig. 7. Implementation of proposed protocol.

Table 3
Security analysis of proposed protocol with earlier schemes.

Parameters	LMAP [9]	EMAP [10]	SASI [11]	Konidala [12]	M^{3}AP [13]	Huang [14]	Lin (XOR scheme) [15]	Proposed protocol
Man-in-the-middle attack prevention	Average	Average	Average	Average	Average	Average	High	**High**
Mutual authentication	Low	Low	Low	High	Average	High	High	**High**
User data confidentiality	Low	Low	Average	Average	High	High	High	**High**
Operations used	^, v, +, XOR	^, v, +, XOR	^, v, +, Rot, XOR	Padgen, XOR	Mixbits	Padgen, XOR	Padgen, XOR, mod	**Truncated multiplier , XOR**
Hardware implementation	Yes	Yes	No	No	No	Yes	Yes	**Yes**
Area overhead	Average	Less	Less	High	High	High	High	**Average**

Padgen function consumes more logic elements which increases the hardware cost.

The dynamic power dissipation of our proposed protocol is less compared to all other existing protocols [9–15] for 100 MHz clock frequency. This is due to the reduced switching activities. In addition to that the cost is low for our proposed protocol scheme which is achieved at the expense of small increase in delay as shown in Table 2.

Fig. 6 shows that simulation output of the proposed protocol where RT1=4014 h RM1=401 A h PWD=A10BC549h and their corresponding CCPWDRT=1394 h CCPWDTM=1993 h. The clock frequency is used in this simulation is 100 MHz Whenever the CCPWDTT and CCPWDRM matches with the value of CCPWDRT and CCPWDTM, respectively, authentication signal becomes high.

4.2. Implementation

The proposed protocol is synthesized in Quartus II 9.0 tool and implemented as hardware in Altera Cyclone II FPGA EP2C35F672C6 device [23]. A 16 bit CCPWDRT=1394 h and CCPWDRM=1993 h which is indicated in seven segment display and glowing with LED indicates that mutual authentication is achieved between reader and tag as shown in Fig. 7.

4.3. Security analysis

Once the proposed mutual authentication protocol has been implemented, Proposed Mutual Authentication is further evaluated in terms of security using following metrics like Spoofing, Replay attack prevention, Forgery Resistance, Man in middle attack prevention and Mutual Authentication as Peris-Lopez analyzed in [9]. Table 3 shows the comparative analysis of proposed protocol with previous protocol in terms of subjective evaluation.

4.3.1. Spoofing

Spoofing attacks supply false information that looks valid and that the system accepts. Our protocol accepts the information but immediately verify whether it is valid data or not.

4.3.2. Replay attack prevention

In a replay attack, a valid RFID signal is intercepted and its data is recorded this data is later transmitted to a reader. Until they have architecture of the truncated multiplier they cannot able to find the password even though they send the message later.

4.3.3. Forgery resistance

The information stored in the tag is sent to truncated multiplier function over random numbers (RT1, RM1). Output of the truncated multiplier gives an encoded format of information. Therefore, the simple capture of information on the tag by eavesdropping is impossible.

4.3.4. Mutual authentication

Reader-to-tag authentication is done by verify CCPWDRT=CCPWDTT and tag-to-reader authentication is done by verifying CCPWDRM=CCPWDTM. If authentication fails, it terminates connection else connection has been established between tag and reader. Hence mutual authentication is existed in the proposed protocol.

4.3.5. Man-in-the-middle attack prevention

In the proposed protocol a man-in-the-middle attack is impossible because it is based on a mutual authentication, in which two random numbers (RT1, RM1) are updated at each iteration of the protocol, are used. This scheme is secure and capture of information on the tag by eavesdropping is impossible because they get only encrypted version of information.

5. Conclusion

In this paper, an efficient RFID mutual authentication protocol is proposed whose functionality is verified using the VHSIC hardware description language. Truncated multiplier functions were examined for the tag–reader mutual authentication protocol in the RFID system environment. The proposed scheme is feasible in improving the weakness of the EPC global C1G2 communication authentication scheme. The hardware implementation of proposed RFID tag–reader mutual authentication protocol has been done on the Altera DE2 Cyclone II FPGA board. In addition to that our proposed protocol outperforms than the earlier schemes in terms of area and dynamic power dissipation.

References

[1] Frank Thronton, Brad Haines, Anita Campbell, RFID security, Syngress Publishing, Inc, 2006.
[2] S. Han, H. Lim, J. Lee, An efficient localization scheme for a differential-driving mobile robot based on RFID system, IEEE Transactions on Industrial Electrons 53 (5) (2007) 3362–3369.
[3] Class 1 Generation 2 UHF Air Interface Protocol Standard, ⟨http://www.epcglobalinc.org/standards/⟩.
[4] Radio Frequency Identification for Item Management, 2nd ed., ISO/IEC 18000, (2008).
[5] Ver. 1.0.9 EPC global Ratified Standard, EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860–960 MHz, ⟨http://www.epcglobalinc.org/standards/⟩.
[6] Mark Goresky, Andrew M. Klapper, Fibonacci and galois representations of feedback-with-carry shift registers, IEEE Transactions on Information Theory 48 (11) (2002) 2826–2836.
[7] ⟨http://www.xilinx.com/support/documentation/data_shee ts/ds100.pdf⟩.
[8] P.K. Lala, Digital Circuit Testing and Testability, Academic Press, 2002.
[9] P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador, A. Ribagorda, LMAP: a real lightweight mutual authentication protocol for low-cost RFID tags, in: Proceedings Second Workshop RFID Security, (2006), pp. 1–12.
[10] P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador, A. Ribagorda, EMAP: an efficient mutual authentication protocol for low- cost RFID tags, in: Proceedings OTM Federated Conference and Workshop: IS Workshop, (2006).

[11] H.-Y. Chien, SASI: a new ultra lightweight RFID authentication protocol providing strong authentication and strong integrity 4 (4) (2007) 337–340.
[12] D.M. Konidala, Z. Kim, K. Kim, A simple and cost effective RFID tag–reader mutual authentication scheme, in: Proceedings International Conference on RFID Security, (2007), pp. 141–152.
[13] P. Peris-Lopez, T.-L. Lim, T. Li, Providing stronger authentication at a low cost to RFID tags operating under the EPCglobal framework, in: Proceedings IEEE/IFIP International Conference EUC, vol. 2, Dec. 17–20, (2008), pp. 159–166.
[14] Yu-Jung Huang, Ching-Chien Yuan, Ming-Kun Chen, Wei-Cheng Lin, Hsien-Chiao Teng, Hardware implementation of RFID mutual authentication protocol, IEEE Transactions on Industrial Electronics 57 (5) (2010) 1573–1582.
[15] Yu-Jung Huang, Wei-Cheng Lin, Hung-Lin Li, Efficient implementation of RFID mutual authentication protocol, IEEE Transactions on Industrial Electronics (2011), Issue 99.
[16] M.J. Schulte, J.G. Hansen, J.E. Stine, Reduced power dissipation through truncated multiplication, in: Proceedings IEEE Alessandro Volta Memorial International Workshop Low Power Design, (1999), pp. 61–69.
[17] J.-P. Wang, S.-R. Kuang, S.-C. Liang, High-accuracy fixed-width modified booth multipliers for lossy applications, IEEE Transactions on Very Large Scale Integration (VLSI) System 19 (1) (2011) 52–60.
[18] Hou-Jen Ko, Shen-Fu Hsiao, Design and application of faithfully rounded and truncated multipliers with combined deletion, reduction, truncation, and rounding, IEEE Transactions on Circuits and Systems II: Express Briefs 58 (5) (2011) 304–308.
[19] Selwyn Piramuthu, Protocols for RFID tag/reader authentication, Decision Support Systems 43 (2007) 897–914.
[20] Selwyn Piramuthu, RFID mutual authentication protocols, Decision Support Systems 50 (2011) 387–393.
[21] Jung-Sik Cho, Sang-Soo Yeo, Sung Kwon Kim, Securing against brute-force attack: a hash-based RFID mutual authentication protocol using a secret value, Computer Communications, 34, 391–397, Elsevier.
[22] L. Hars, Fast truncated multiplication for cryptographic applications, in Proceedings of the Seventh International Workshop on Cryptographic Hardware and Embedded Systems (CHES '05), of Lecture Notes in Computer Science, Edinburgh, UK, vol. 3659, (2005), pp. 211–225.
[23] [Online].Available:⟨http://www.altera.com/products/devices/cyclone2/cy2-index.jsp⟩.

V.R. Vijaykumar received his bachelor degree in Electronics and Communication Engineering in the year 1996 from Government College of Technology Vellore and subsequently he completed his M.E. degree in Communication Systems at Thiagarajar college of Engineering Madurai in the year 1997. He completed his Ph.D. in the area of Nonlinear Image Filtering from Anna University Chennai in the year 2008. He has 14 years of Teaching Experience. Currently he his working as Associate Professor in the Department of Electronics and Communication Engineering, Anna University, Coimbatore, Tamil Nadu, India. His area of interest includes Image Processing, Signal Processing, Digital Communication and Low Power VLSI.

S. Elango received the bachelor's degree in Electronics and Communication Engineering from Anna University Tamil Nadu, India, in 2010 and Master's degree in VLSI Design from Anna University, Tamil Nadu, India in 2012. At present he is working as Assistant Professor in the Department of ECE, Bannari Amman Institute of Technology, Sathyamangalam, Erode, Tamil Nadu, India. His main research interests includes design of VLSI Data path elements, VLSI signal processing and Low power VLSI Designs.

Int. J. Electron. Commun. (AEÜ) 68 (2014) 1145–1155

Contents lists available at ScienceDirect

International Journal of Electronics and Communications (AEÜ)

journal homepage: www.elsevier.com/locate/aeue

Fast switching based median–mean filter for high density salt and pepper noise removal

V.R. Vijaykumar[a,*], G. Santhana Mari[a], D. Ebenezer[b]

[a] Department of Electronics and Communication Engineering, Anna University, Coimbatore, Tamil Nadu, India
[b] Department of Electronics and Communication Engineering, Eswari Engineering College, Chennai, India

ARTICLE INFO

Article history:
Received 25 March 2013
Accepted 9 June 2014

Keywords:
Image restoration
Impulse detection
Mean filter
Median filter
Salt and pepper noise

ABSTRACT

This paper proposes a fast switching based median–mean filter for high density salt and pepper noise in images. The extreme minimum value and extreme maximum value of the noisy image are used to identify the noise pixels. In the filtering stage, the corrupted pixel is replaced either by median value or mean value based on the number of noise free pixels in the filtering window. The qualitative and quantitative results show that the proposed filter outperforms the other switching based filters namely ACWMF, PSMF, AMF, DBA and MDBUTMF in terms of noise removal and edge preservation for noise densities varying from 10% to 90%.

1. Introduction

Images are often corrupted by salt and pepper noise during transmission. Generally, linear filtering techniques fail when the noise is non-additive and are not effective in removing impulse noise [1]. This has lead to the use of nonlinear signal processing techniques. Most commonly used nonlinear filter is the median filter. The main drawback of a Standard Median Filter (SMF) is that every pixel in the image is replaced by the median value in its neighborhood as a result of which the desirable details in the image are removed [2]. At high noise densities, SMF often exhibits blurring for large window sizes and insufficient noise suppression for small window sizes. The Weighted Median Filter (WMF) [3] and the Center-Weighted Median Filter (CWMF) [4] were proposed as remedy to improve the median filter by giving more weight to some selected pixels in the filtering window. Although these two filters can preserve more details than the median filter, they are still implemented uniformly across the image without considering whether the current pixel is noise free or not.

Switching median filters [5–14] were proposed with the objective of discriminating between corrupted and uncorrupted pixels prior to non-linear filtering. Possible noisy pixels are identified and replaced by using median value or its variant while leaving uncorrupted pixels unchanged. An Adaptive Median Filter (AMF) proposed in [5] is good at low and medium noise density levels. At higher noise densities, the number of replacements of corrupted pixel increases considerably; increasing window size will provide better noise removal performance; however, the original pixel values and replaced median pixel values are less correlated. As a consequence, the edges are smeared significantly. The Adaptive Center Weighted Median Filter (ACWMF) proposed in [6] is used to remove high density impulse noise. It requires optimized thresholds for both salt and pepper and random valued impulse noise types. Though Progressive Switching Median Filter (PSMF) [7] performs efficiently, it is time consuming and computationally complex as a result of which its hardware implementation becomes difficult.

Recently, some novel decision based median filters such as a Boundary Discriminative Noise Detector (BDND) [8], Decision Based Algorithm (DBA) [9], Simple Adaptive Median Filter (SAMF) [10] and Modified Decision Based Unsymmetrical Trimmed Median Filter (MDBUTMF) [11] have been proposed in the literature to remove high density salt and pepper noise in digital images. The BDND uses a large window of size 21×21 to detect noise pixels. Therefore, it requires high computation time and details get blurred at higher noise densities. A fixed 3×3 window is used for filtering in DBA. In this algorithm, the corrupted pixels are replaced by the median value of the filtering mask. At higher noise densities, the median value may also be a noisy pixel in which case

* Corresponding author. Tel.: +91 9442014139.
E-mail address: vr_vijay@hotmail.com (V.R. Vijaykumar).

http://dx.doi.org/10.1016/j.aeue.2014.06.002
1434-8411/

$X_{i-1,j-1}$	$X_{i-1,j}$	$X_{i-1,j+1}$
$X_{i,j-1}$	$X_{i,j}$	$X_{i,j+1}$
$X_{i+1,j-1}$	$X_{i+1,j}$	$X_{i+1,j+1}$

Fig. 1. A 3×3 filtering window highlighting previously processed pixels.

the most recently processed pixel is used for replacement. Since previously processed pixel is used for replacement, streaking in the image becomes a problem at higher noise densities. The SAMF in [10] is used to remove high density salt and pepper noise. At higher noise ratios SAMF does not preserve edges satisfactorily and moreover an adaptive window of length 15×15 is used for filtering at high noise densities. The Modified Decision Based Unsymmetric Trimmed Median Filter (MDBUTMF) for high density salt and pepper noise removal assumes the minimum value (i.e. 0) and the maximum value (i.e. 255) in the dynamic range as pepper noise and salt noise respectively. The main drawback is that at higher noise densities, if all the pixels in the 3×3 filtering window are corrupted either by pepper noise value (i.e. 0) or by salt noise value (i.e. 255), then it uses mean value of all the elements in the filtering window to replace the noise pixel which is also a noisy value, i.e. 0 or 255.

In this paper, a fast switching based median–mean filter is proposed to remove high density salt and pepper noise with edge preservation and reduced streaking. The noise pixels are detected in the first stage. In the second stage, corrupted pixel is replaced either with median value in the filtering window or mean value

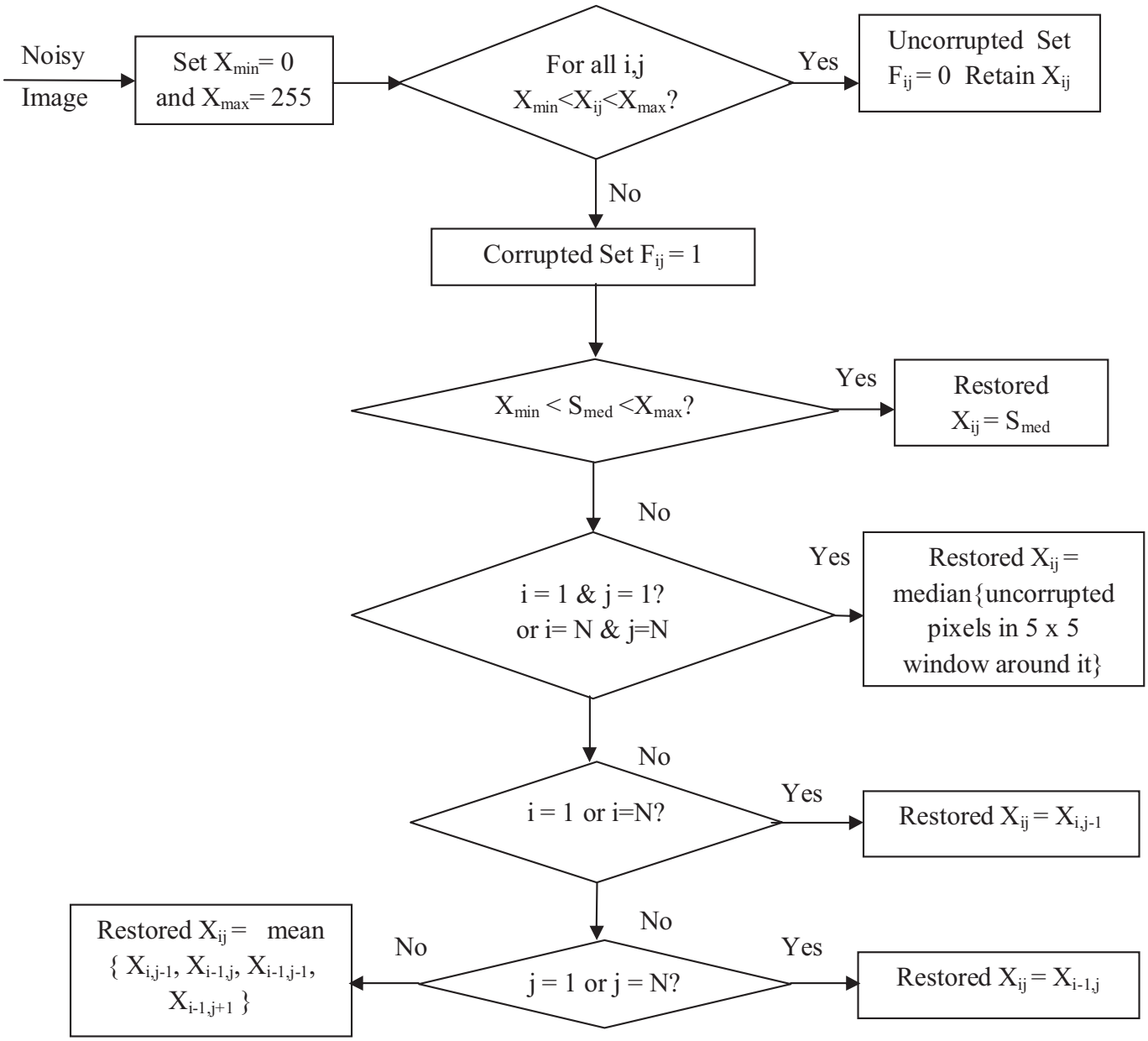


Fig. 2. Flowchart of the proposed algorithm.

of the four previously processed pixels. The proposed algorithm requires significantly lower processing time compared with the existing methods since it uses a 3×3 fixed window for detection and filtering. The rest of the paper is organized as follows; noise model is given in Section 2; Section 3 describes the proposed algorithm; illustrations are presented in Session 4; experimental results are discussed in Section 5; Section 6 concludes the paper.

2. Noise model

Noise is modeled as salt-and-pepper impulse noise where the image pixels are randomly corrupted by two fixed extreme values, 0 and 255 [12] (for 8-bit monochrome image), generated with the same probability of occurrence. That is, for each image pixel at location (i,j) $(1 \le i \le M, 1 \le j \le N$ for an $M \times N$ image) with intensity value O_{ij}, the corresponding pixel of the noisy image will be X_{ij}, in which the probability density function of X_{ij} is

$$f(x) = \begin{cases} \rho/2; & x = 0 \\ 1-\rho; & x = O_{ij} \\ \rho/2; & x = 255 \end{cases} \quad (1)$$

where, ρ is the noise probability.

3. Proposed switching based median–mean filter

The proposed algorithm consists of two stages namely detection stage and filtering stage. In the detection stage a 3×3 detection mask is applied to the current processing pixel. The maximum (X_{max}) and minimum intensity values (X_{min}) of the dynamic range of the noisy image are used to detect the noise pixels. After detection, we employ either median filter or mean filter to replace the noise candidate. The proposed algorithm is described as follows:

Let X_{ij} be the current pixel to be processed and Y_{ij} be its restored value. Let S_{ij} be the sliding window of size $W \times W$ centered at X_{ij}, where $W = (2L+1)$ with L being a positive integer value. For example, a 3×3 window has parameters $W = 3$ and $L = 1$. S_{ij} comprises of pixels defined by the set $\{X_{i-u,\, j-v}, -L \le u,v \le L\}$.

1. Get the noisy image X of size $M \times N$ as input.
2. Set the sliding window size $W = 3$.
3. For every pixel X_{ij} in the image,

a. If $X_{min} < X_{ij} < X_{max}$ then the corresponding pixel is considered uncorrupted and its flag status is set to '0' in the flag image F.

b. Else X_{ij} is corrupted and its flag status is set to '1' in the flag image F.

c. The flag image is given by

$$F_{ij} = \begin{cases} 0, & X_{min} < X_{ij} < X_{max} \\ 1, & \text{Otherwise} \end{cases} \quad (2)$$

4. For the replacement of those values in X whose flag value equals '1', compute S_{med}, the median value of all pixels in S_{ij}. If $X_{min} < S_{med} < X_{max}$, then replace X_{ij} with S_{med}. Else, carry out the following steps.

a. If X_{ij} is the very first pixel of the image (i.e. $i = j = 1$ and $i = j = N$), replace it with the median of uncorrupted pixels in the 5×5 window centered about it.

b. Else if X_{ij} is a pixel in the first or last row of the image (i.e. $i = 1$ or $i = N$), replace it with the processed pixel to its immediate left $(X_{i,j-1})$.

c. Else if X_{ij} is a pixel in the first or last column of the image (i.e. $j = 1$ or $j = N$), replace it with the processed pixel immediately above it $(X_{i-1,j})$.

d. Else replace X_{ij} with the mean of four previously processed pixels in S_{ij} as shown in Fig. 1.

5. The image X obtained after carrying out the above steps is the final restored image Y.

The flowchart for the algorithm is shown in Fig. 2

4. Illustration

The working of the proposed algorithm is demonstrated by using segments of test image and its efficiency in removing noise pixels is highlighted in this section.

4.1. Demonstration for a 5×5 noisy image segment

In order to demonstrate the working of the proposed algorithm a 5×5 image segment is chosen for illustration from "Lena.jpg", corrupted by salt and pepper noise of density 90%. The minimum and maximum pixel values in the noisy segment, i.e. X_{min} and X_{max} are found to be 0 and 255, respectively.

NOISY IMAGE SEGMENT

$$N_{SEG} = \begin{bmatrix} 255 & 255 & 118 & 0 & 0 \\ 255 & 0 & 255 & 0 & 119 \\ 0 & 120 & 255 & 255 & 118 \\ 255 & 255 & 255 & 0 & 0 \\ 255 & 0 & 0 & 0 & 255 \end{bmatrix}$$

FLAG IMAGE SEGMENT

$$F_{SEG} = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Step 1: Initially, the noisy image is zero padded and a 3×3 filtering mask is defined on the very first pixel, i.e. $X_{11} = 255$ (highlighted) as shown in NZP_{SEG}. Since the very first pixel is corrupted, as per our algorithm, the center pixel (i.e. 255) is replaced by the median of the uncorrupted pixel in the 5×5 mask, i.e. Median $\{120, 118\} = 119$. The filtered image segment FI_{SEG} is given below.

$$NZP_{SEG} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 255 & 255 & 118 & 0 & 0 & 0 & 0 \\ 0 & 0 & 255 & 0 & 255 & 0 & 119 & 0 & 0 \\ 0 & 0 & 0 & 120 & 255 & 255 & 118 & 0 & 0 \\ 0 & 0 & 255 & 255 & 255 & 0 & 0 & 0 & 0 \\ 0 & 0 & 255 & 0 & 0 & 0 & 255 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$FI_{SEG} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 119 & 255 & 118 & 0 & 0 & 0 & 0 \\ 0 & 0 & 255 & 0 & 255 & 0 & 119 & 0 & 0 \\ 0 & 0 & 0 & 120 & 255 & 255 & 118 & 0 & 0 \\ 0 & 0 & 255 & 255 & 255 & 0 & 0 & 0 & 0 \\ 0 & 0 & 255 & 0 & 0 & 0 & 255 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Step 2: Move the 3×3 filtering mask to the next pixel, i.e. $X_{1,2} = 255$. Since the center pixel is corrupted, as per our algorithm it is replaced by the median of the array, i.e. Median $\{0,0,0,0,118,255,255,255,255\} = 118$. The filtered image FI_{SEG} is given below.

$$NZP_{SEG} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 255 & 255 & 118 & 0 & 0 & 0 & 0 \\ 0 & 0 & 255 & 0 & 255 & 0 & 119 & 0 & 0 \\ 0 & 0 & 0 & 120 & 255 & 255 & 118 & 0 & 0 \\ 0 & 0 & 255 & 255 & 255 & 0 & 0 & 0 & 0 \\ 0 & 0 & 255 & 0 & 0 & 0 & 255 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$FI_{SEG} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 119 & 118 & 118 & 0 & 0 & 0 & 0 \\ 0 & 0 & 255 & 0 & 255 & 0 & 119 & 0 & 0 \\ 0 & 0 & 0 & 120 & 255 & 255 & 118 & 0 & 0 \\ 0 & 0 & 255 & 255 & 255 & 0 & 0 & 0 & 0 \\ 0 & 0 & 255 & 0 & 0 & 0 & 255 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Step 3: Move the filtering window to the next pixel, i.e. $X_{1,3} = 118$. Since the center pixel is uncorrupted and retained as such. The same is shown in the filtered image segment FI_{SEG} given below.

$$NZP_{SEG} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 255 & 255 & 118 & 0 & 0 & 0 & 0 \\ 0 & 0 & 255 & 0 & 255 & 0 & 119 & 0 & 0 \\ 0 & 0 & 0 & 120 & 255 & 255 & 118 & 0 & 0 \\ 0 & 0 & 255 & 255 & 255 & 0 & 0 & 0 & 0 \\ 0 & 0 & 255 & 0 & 0 & 0 & 255 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$FI_{SEG} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 119 & 118 & 118 & 0 & 0 & 0 & 0 \\ 0 & 0 & 255 & 0 & 255 & 0 & 119 & 0 & 0 \\ 0 & 0 & 0 & 120 & 255 & 255 & 118 & 0 & 0 \\ 0 & 0 & 255 & 255 & 255 & 0 & 0 & 0 & 0 \\ 0 & 0 & 255 & 0 & 0 & 0 & 255 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

The same process is repeated for remaining first row pixels (i.e. $X_{1,4}$ and $X_{1,5}$) and second row first pixel (i.e. $X_{2,1}$) and the filtered image is shown below in FI_{SEG}

$$FI_{SEG} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 119 & 118 & 118 & 118 & 118 & 0 & 0 \\ 0 & 0 & 119 & 0 & 255 & 0 & 119 & 0 & 0 \\ 0 & 0 & 0 & 120 & 255 & 255 & 118 & 0 & 0 \\ 0 & 0 & 255 & 255 & 255 & 0 & 0 & 0 & 0 \\ 0 & 0 & 255 & 0 & 0 & 0 & 255 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Step 4: Move the filtering window to the next pixel, i.e. $X_{2,2}$ as shown below in NZP_{SEG}. Since the center pixel of the filtering mask (i.e. $X_{2,2} = 0$) is corrupted and the median value (S_{med}) of the array is also corrupted (i.e. $S_{med} = 255$), the center pixel is replaced by the mean of the four previously processed pixels in the window, i.e. Mean $\{119,118,118,119\} = 118.5$ as given in FI_{SEG}.

$$NZP_{SEG} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 255 & 255 & 118 & 0 & 0 & 0 & 0 \\ 0 & 0 & 255 & 0 & 255 & 0 & 119 & 0 & 0 \\ 0 & 0 & 0 & 120 & 255 & 255 & 118 & 0 & 0 \\ 0 & 0 & 255 & 255 & 255 & 0 & 0 & 0 & 0 \\ 0 & 0 & 255 & 0 & 0 & 0 & 255 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$FI_{SEG} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 119 & 118 & 118 & 118 & 118 & 0 & 0 \\ 0 & 0 & 119 & 118.5 & 255 & 0 & 119 & 0 & 0 \\ 0 & 0 & 0 & 120 & 255 & 255 & 118 & 0 & 0 \\ 0 & 0 & 255 & 255 & 255 & 0 & 0 & 0 & 0 \\ 0 & 0 & 255 & 0 & 0 & 0 & 255 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

The same process is repeated for all the pixels in the noisy image and final restored image segment after rounding is given below in Y_{SEG}.

$$Y_{SEG} = \begin{bmatrix} 119 & 118 & 118 & 118 & 118 \\ 119 & 119 & 120 & 118 & 119 \\ 119 & 120 & 119 & 119 & 118 \\ 119 & 119 & 120 & 118 & 118 \\ 119 & 119 & 119 & 118 & 118 \end{bmatrix}$$

4.2. Demonstration for an edge region

The 3×3 image segment chosen for illustration is from "Lena.jpg", corrupted by salt and pepper noise of density 90%. The X_{min} and X_{max} are found to be 0 and 255, respectively.

ORIGINAL SEGMENT

$$O_{SEG} = \begin{bmatrix} 57 & 88 & 108 \\ 63 & 94 & 113 \\ 74 & 100 & 116 \end{bmatrix}$$

NOISY SEGMENT

$$N_{SEG} = \begin{bmatrix} 0 & 0 & 108 \\ 0 & 255 & 0 \\ 74 & 0 & 116 \end{bmatrix}$$

FLAG IMAGE

$$F_{SEG} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

The center pixel in X_{SEG} (i.e. 255) is corrupted since it does not satisfy the condition $X_{min} < X_{ij} < X_{max}$. Hence the median value of the window is checked.

$$\text{Median}\{X_{SEG}\} = \text{Median}\{0, 0, 108, 0, 255, 0, 74, 0, 116\} = 0$$

Since the median value is also corrupted, the center pixel should be replaced by the mean of four previously processed pixels in the window. During the filtering of noisy image, the causal pixels {0, 0, 108, 0} are modified as {65, 98, 108, 74}. The center pixel, i.e. '0' will be replaced by the average of the processed causal pixels.

$$Y_{ij} = \frac{65 + 98 + 108 + 74}{4} = 86$$

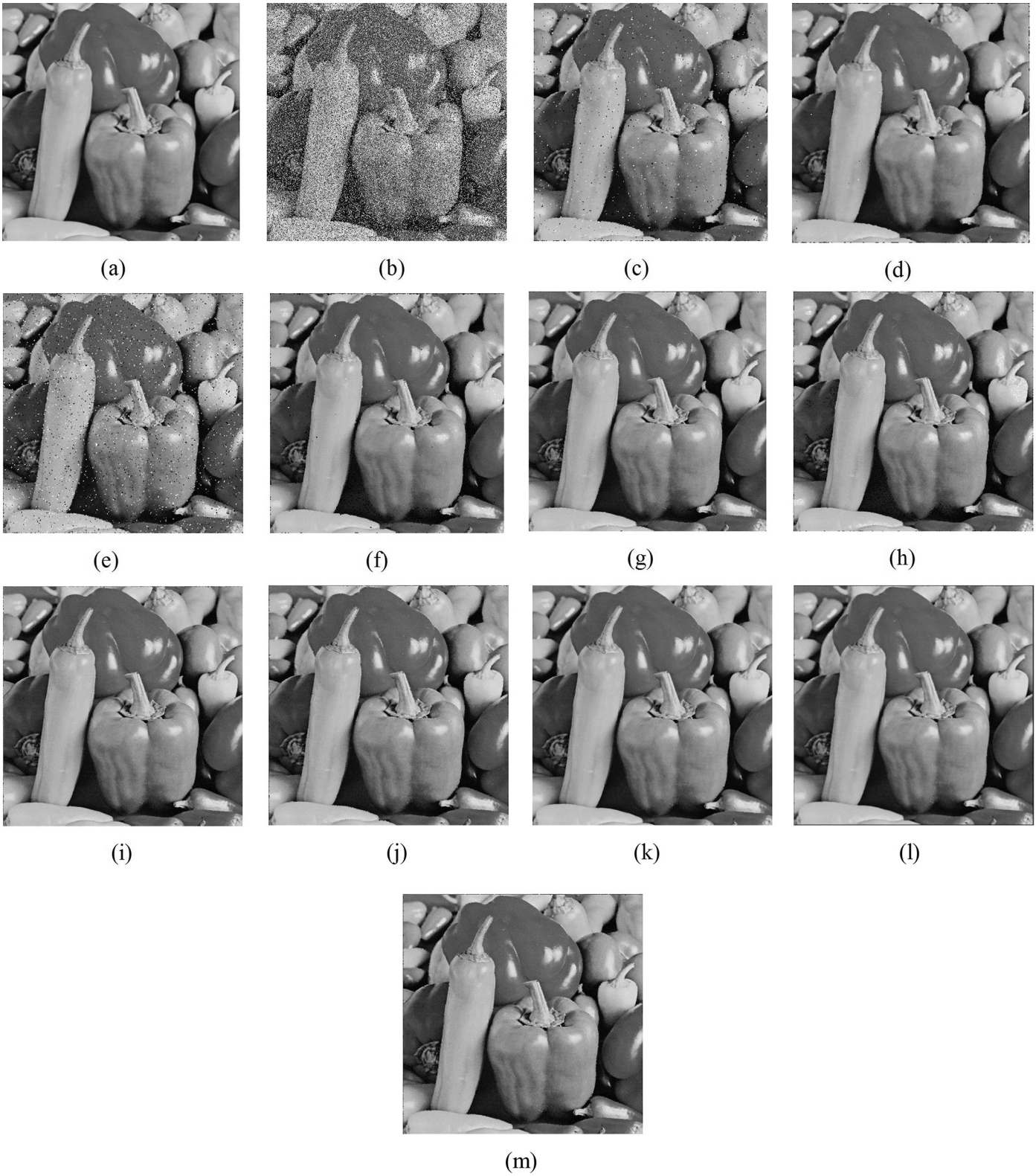


Fig. 3. (a) Original peppers image, (b) noisy image (SP = 30%). Restoration results of (c) SMF, (d) WMF, (e) CWMF, (f) ACWMF, (g) PSMF, (h) AMF, (i) BDND, (j) DBA, (k) SAMF, (l) MDBUTMF and (m) proposed algorithm.

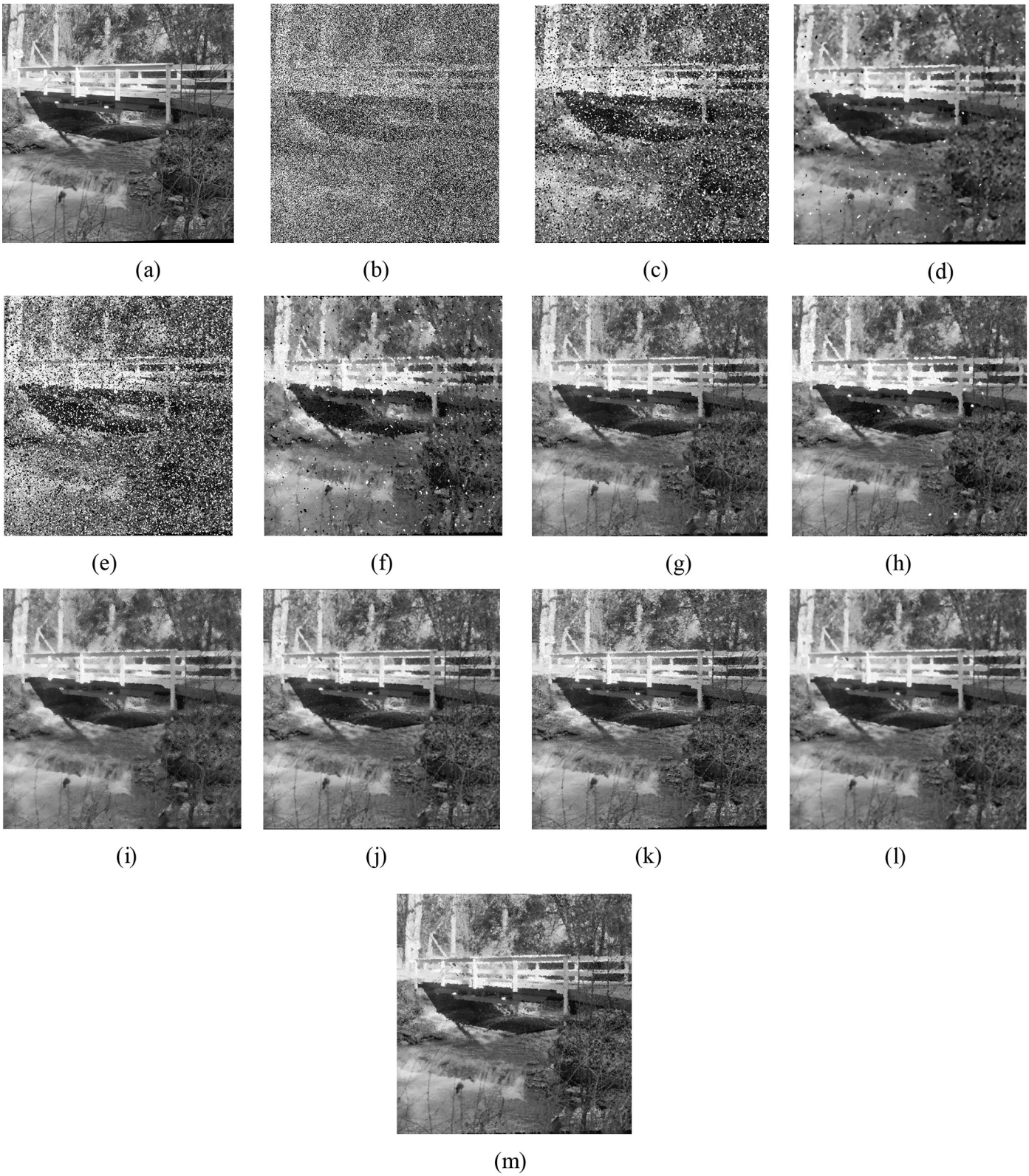


Fig. 4. (a) Original bridge image, (b) noisy image (SP = 60%). Restoration results of (c) SMF, (d) WMF, (e) CWMF, (f) ACWMF, (g) PSMF, (h) AMF, (i) BDND, (j) DBA, (k) SAMF, (l) MDBUTMF and (m) proposed algorithm.

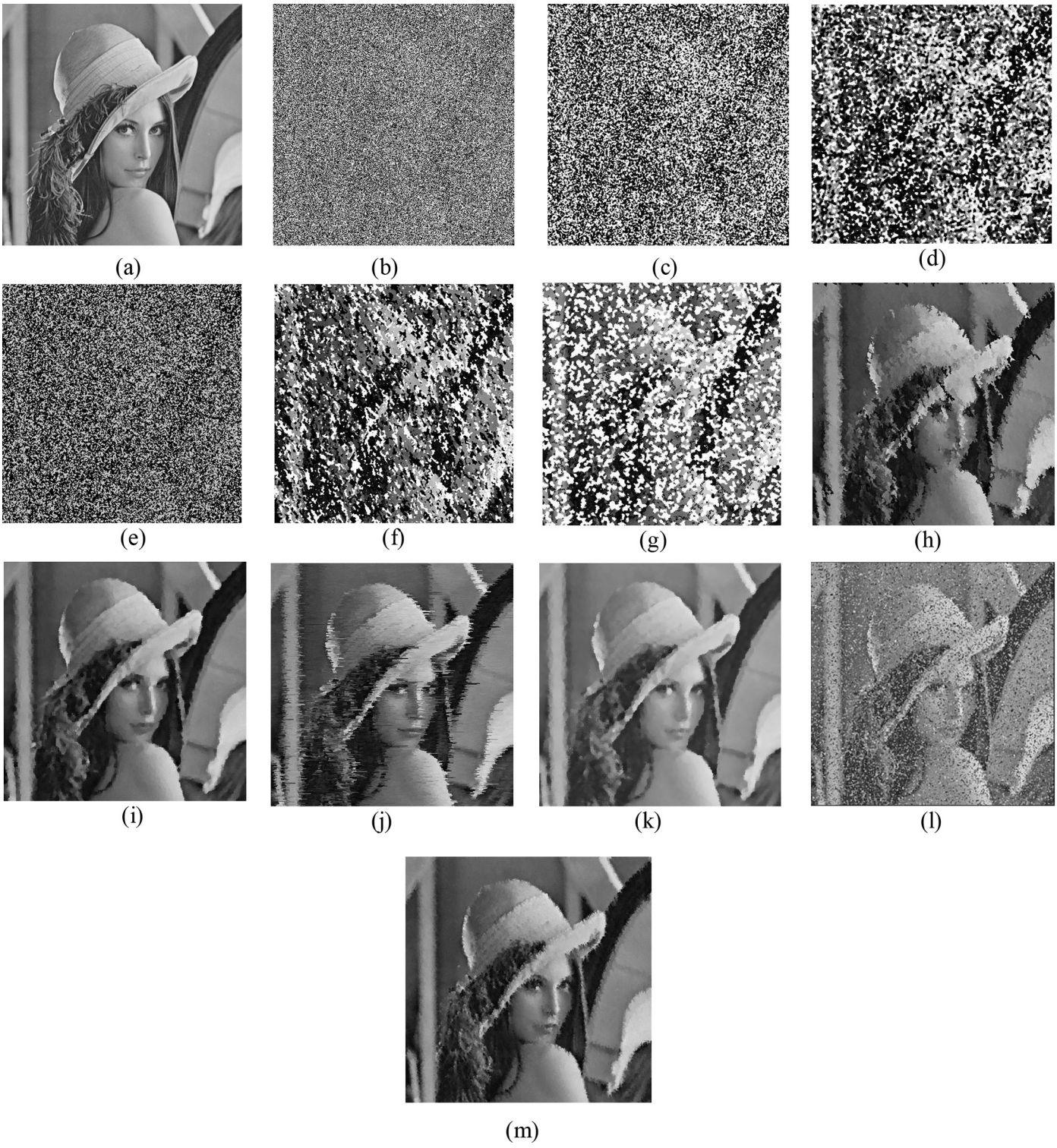


Fig. 5. (a) Original Lena image, (b) noisy image (SP = 90%). Restoration results of (c) SMF, (d) WMF, (e) CWMF, (f) ACWMF, (g) PSMF, (h) AMF, (i) BDND, (j) DBA, (k) SAMF, (l) MDBUTMF and (m) proposed algorithm.

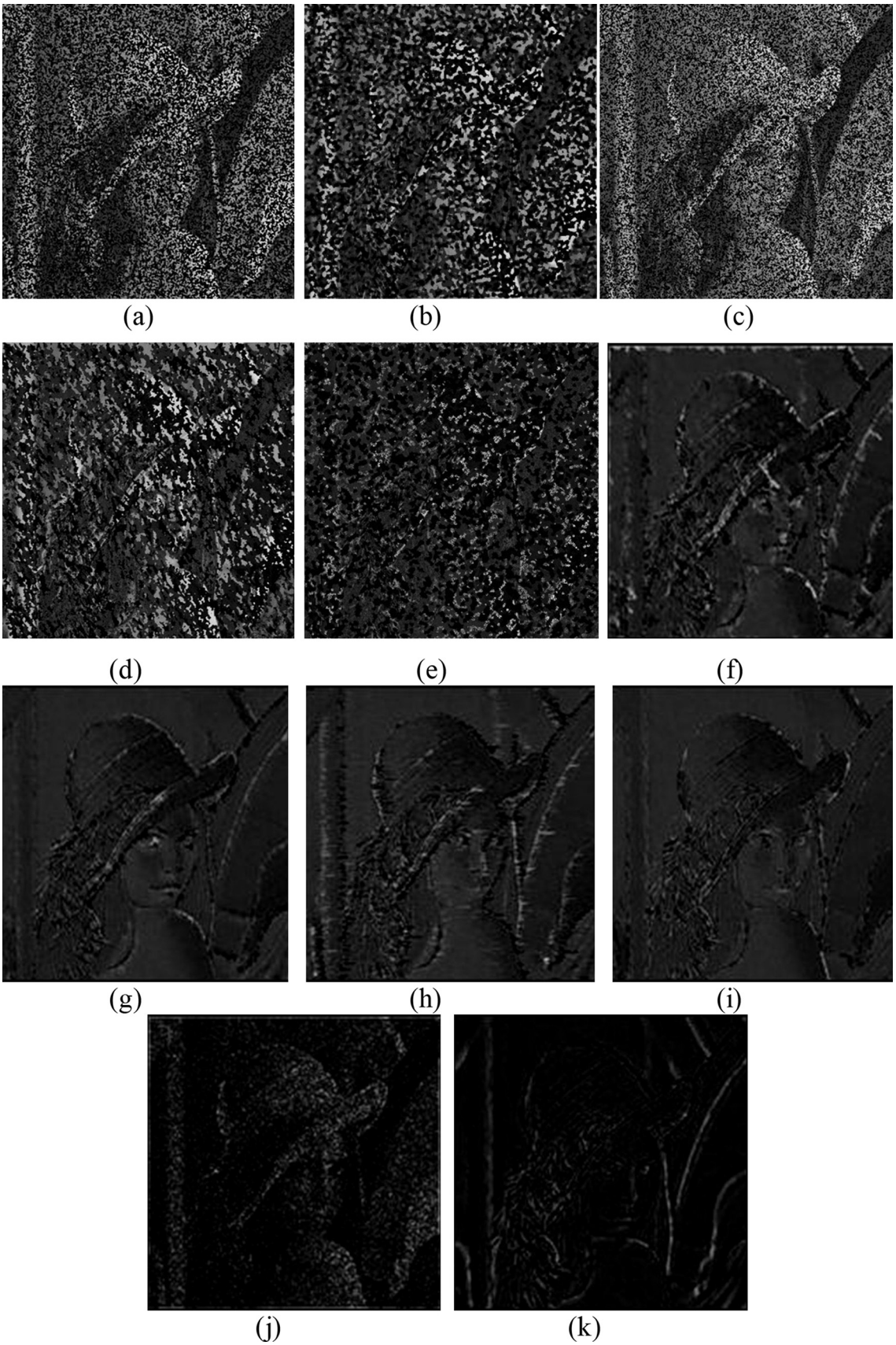


Fig. 6. Error image of different algorithms (a) SMF, (b) WMF, (c) CWMF, (d) ACWMF, (e) PSMF, (f) AMF, (g) BDND, (h) DBA, (i) SAMF, (j) MDBUTMF and (k) proposed algorithm.

Table 1
PSNR (in dB) of various filters for peppers image at different SP noise densities.

ND (%)	SMF	WMF	CWMF	ACWMF	AMF	PSMF	BDND	DBA	SAMF	MDBUTMF	Proposed algorithm
10	32.62	33.02	32.23	36.15	39.63	33.48	37.58	37.27	38.98	36.95	40.57
20	28.41	31.45	25.53	32.40	35.45	31.24	34.99	34.72	35.14	32.53	36.12
30	23.43	28.79	19.82	28.58	33.10	29.73	33.15	32.73	32.92	30.04	33.58
40	18.81	26.10	15.81	25.73	30.83	28.52	31.39	30.98	31.01	27.88	31.48
50	15.12	24.95	12.94	22.73	28.57	26.97	29.77	29.31	30.17	25.49	30.23
60	12.28	22.01	10.65	19.76	26.55	25.76	28.53	27.59	29.12	23.09	28.71
70	9.88	17.37	8.94	16.06	24.24	21.36	27.11	25.59	28.27	20.17	27.36
80	8.05	12.11	7.46	12.62	21.59	14.03	26.16	23.49	26.28	17.06	25.67
90	6.50	7.95	6.27	8.65	17.98	8.39	24.55	19.61	24.39	13.26	22.68

Table 2
MAE of various filters for peppers image at different SP noise densities.

ND (%)	SMF	WMF	CWMF	ACWMF	AMF	PSMF	BDND	DBA	SAMF	MDBUTMF	Proposed algorithm
10	3.13	2.67	2.05	0.62	0.48	0.83	0.51	1.10	0.49	0.54	0.44
20	3.85	3.63	3.37	1.33	0.96	1.50	0.97	1.42	0.96	0.99	0.94
30	5.50	4.15	6.98	2.38	1.68	2.16	1.64	1.89	1.65	1.78	1.58
40	9.49	4.96	13.87	3.73	2.48	2.83	2.38	2.51	2.34	2.62	2.28
50	17.13	5.94	24.55	5.87	3.20	3.65	2.98	3.27	2.81	3.57	2.97
60	29.34	7.65	39.60	9.22	4.39	4.56	3.59	4.23	3.66	4.34	3.88
70	47.55	13.28	57.26	16.41	6.07	7.39	4.55	5.53	4.79	6.54	4.81
80	70.22	31.58	78.82	29.97	9.03	21.58	5.51	7.53	5.07	11.72	6.23
90	97.88	71.95	102.81	64.3	15.47	66.74	7.06	12.64	7.34	24.88	9.45

Table 3
SSIM of various filters for peppers image at different SP noise densities.

ND (%)	SMF	WMF	CWMF	ACWMF	AMF	PSMF	BDND	DBA	SAMF	MDBUTMF	Proposed algorithm
10	0.88	0.89	0.91	0.97	0.98	0.93	0.98	0.95	0.99	0.98	0.99
20	0.83	0.86	0.79	0.94	0.96	0.91	0.97	0.94	0.97	0.97	0.98
30	0.69	0.85	0.52	0.9	0.95	0.9	0.95	0.92	0.96	0.96	0.97
40	0.44	0.81	0.26	0.84	0.92	0.89	0.93	0.9	0.95	0.94	0.95
50	0.23	0.8	0.13	0.74	0.88	0.86	0.91	0.87	0.93	0.91	0.92
60	0.11	0.73	0.06	0.61	0.84	0.84	0.88	0.82	0.91	0.82	0.86
70	0.05	0.53	0.04	0.41	0.77	0.74	0.84	0.78	0.88	0.64	0.81
80	0.03	0.21	0.02	0.22	0.65	0.43	0.8	0.66	0.84	0.39	0.77
90	0.01	0.04	0.01	0.06	0.56	0.1	0.75	0.55	0.78	0.17	0.69

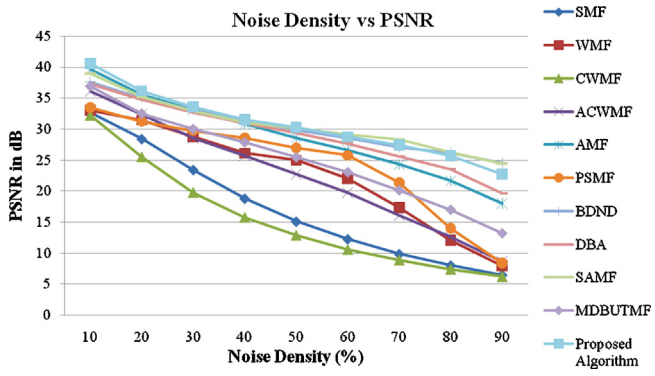


Fig. 7. Comparison of PSNR of various filters for peppers image at different noise densities.

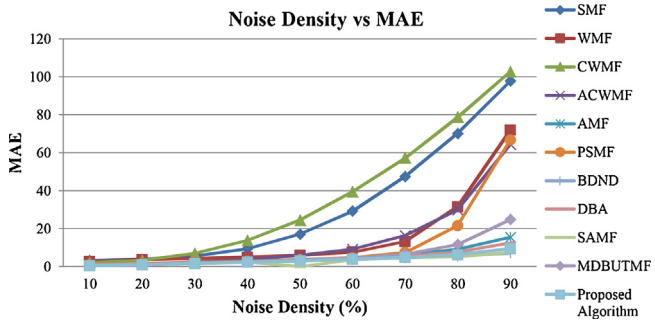


Fig. 8. Comparison of MAE of various filters for peppers image at different noise densities.

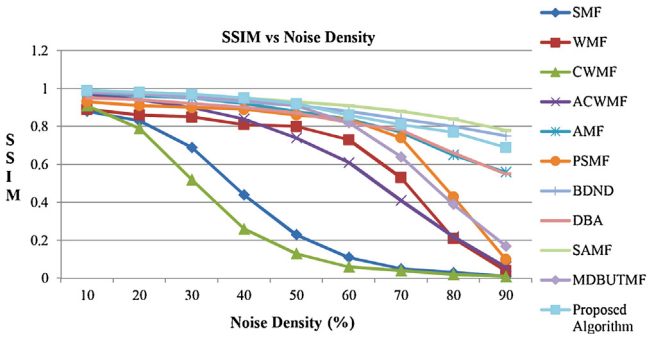


Fig. 9. Comparison of SSIM of various filters for pepper image at different noise densities.

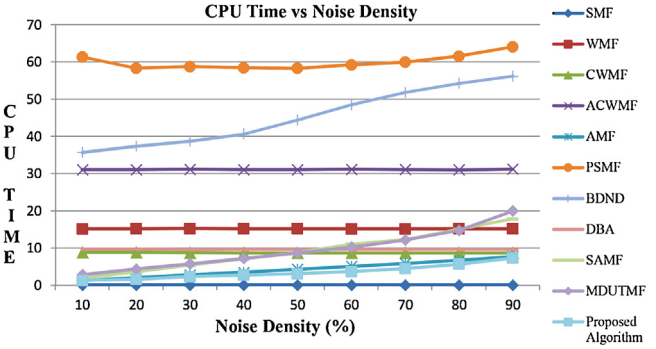


Fig. 10. Comparison of CPU Time of various filters for peppers image at different noise densities.

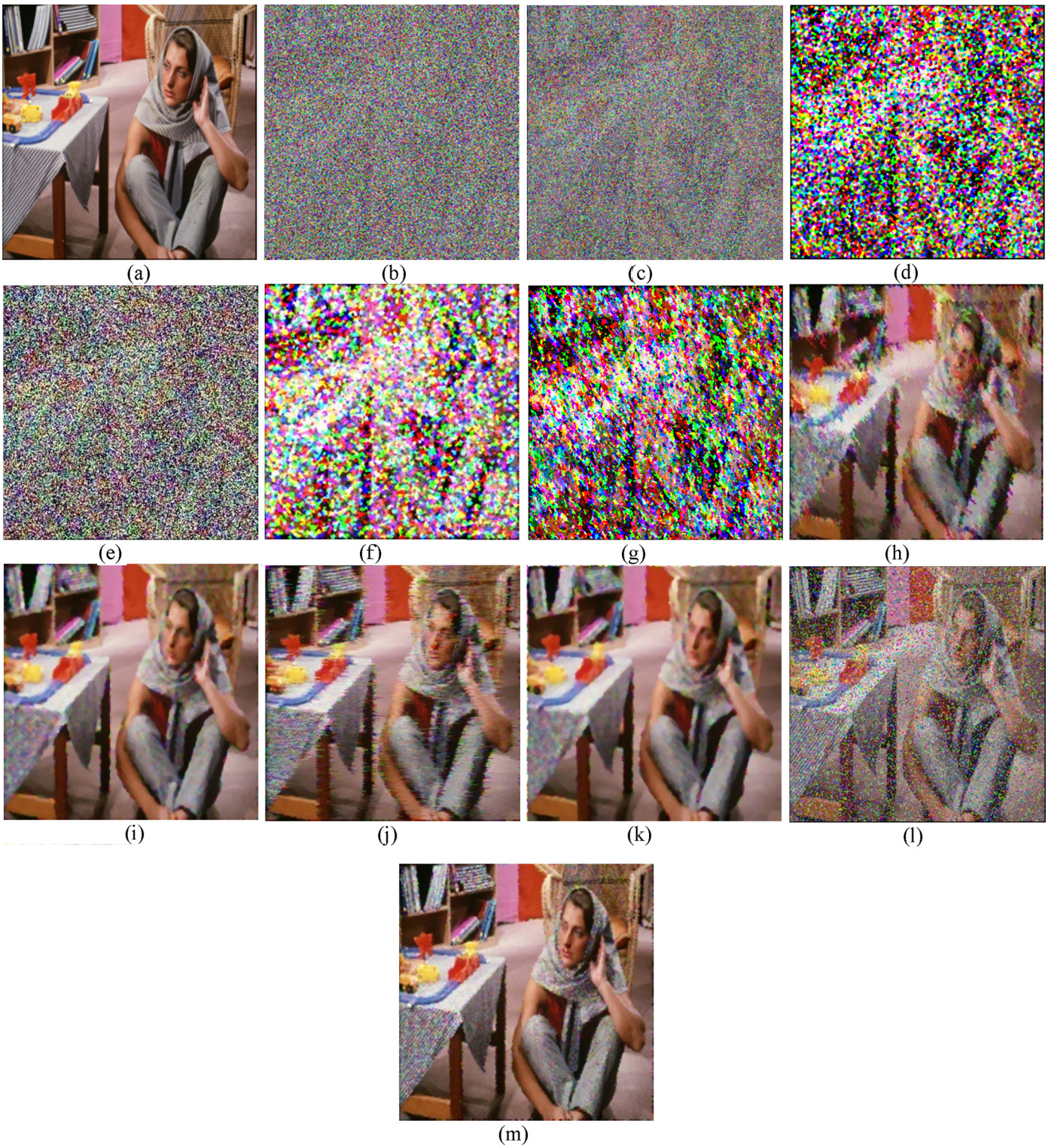


Fig. 11. (a) Original Barbara image, (b) noisy image (SP = 90%). Restoration results of (c) SMF, (d) WMF, (e) CWMF, (f) ACWMF, (g) PSMF, (h) AMF, (i) BDND, (j) DBA, (k) SAMF, (l) MDBUTMF and (m) proposed algorithm. (For interpretation of the references to color in the text, the reader is referred to the web version of this article.)

The restored value 86 is close to the original value 94, which is acceptable for an edge region.

5. Results and discussion

In this section, the proposed algorithm is tested for three different test images namely, Bridge.tiff, Lena.jpg and Peppers.bmp of size 512 × 512, 8 bits/pixel. All the images are corrupted by salt and pepper (SP) noise with different noise densities and applied to the proposed filter. The qualitative performance of the proposed filter is compared with the existing filters such as Standard Median Filter (SMF), Weighted Median Filter (WMF), Center Weighted Median Filter (CWMF), Adaptive Center Weighted Median Filter (ACWMF), Adaptive Median Filter (AMF), Progressive Switching Median Filter

Table 4
CPU Time (in seconds) of various filters for peppers image at different SP noise densities.

ND (%)	SMF	WMF	CWMF	ACWMF	AMF	PSMF	BDND	DBA	SAMF	MDBUTMF	Proposed algorithm
10	0.06	15.17	8.83	31.04	1.28	61.36	35.64	9.72	1.92	2.85	1.33
20	0.07	15.18	8.81	31.05	2.06	58.33	37.31	9.70	3.63	4.35	1.56
30	0.07	15.24	8.70	31.11	2.80	58.70	38.66	9.58	5.41	5.77	2.31
40	0.07	15.21	8.67	31.04	3.48	58.39	40.63	9.59	7.07	7.22	2.72
50	0.07	15.22	8.69	31.03	4.27	58.27	44.39	9.63	8.88	8.67	3.08
60	0.07	15.15	8.67	31.13	5.05	59.17	48.49	9.61	11.12	10.24	3.66
70	0.07	15.17	8.67	31.06	5.86	59.94	51.80	9.63	12.21	12.16	4.47
80	0.06	15.21	8.69	31.01	6.70	61.53	54.27	9.61	15.05	14.74	5.63
90	0.06	15.19	8.69	31.19	7.69	64.05	56.19	9.59	17.86	19.98	7.29

(PSMF), Boundary Discriminative Noise Detector (BDND), Decision Based Algorithm (DBA), Simple Adaptive Median Filter (SAMF) and Modified Decision Based Unsymmetric Trimmed Median Filer (MDBUTMF). A quantitative comparison is performed between the various filters and the proposed filter on the basis of four objective quality measures such as Peak Signal to Noise Ratio (PSNR), Mean Absolute Error (MAE), Structural SIMilarity index (SSIM) [15] and CPU time. The simulations are carried out in a PC (1.86 GHz and 1 GB RAM) equipped with MATLAB 7.1.

Figs. 3–5 show the visual results of existing techniques and the proposed algorithm on salt and pepper noise corrupted 'Peppers' image of noise density 30%, 'Bridge' image of noise density 60% and 'Lena' image of noise density 90% respectively. Tables 1–4 show the performance of the proposed algorithm and the standard filters in terms of PSNR, MAE, SSIM and CPU time for a noisy 'Peppers.bmp' image at various impulse noise density levels from 10% to 90%. The quantitative results in terms of PSNR, MAE, SSIM and CPU time of proposed and other methods are plotted in Figs. 7, 8, 9 and 10, respectively.

The visual results presented indicate that proposed method clearly outperforms almost all the compared techniques for low to high noise densities. From the Table 1, it is inferred that though AMF shows equally good PSNR at low noise densities, its performance degrades significantly at higher noise levels as the window size is increased. The BDND and SAMF give better results in terms of PSNR, MAE and SSIM at high noise ratios above 60%. This is due to the reason that BDND and SAMF is adaptive window algorithm whereas the proposed algorithm is a fixed window algorithm. Also BDND and SAMF has the major drawback of being time consuming as they involves sorting of 21×21 window for noise detection while the SAMF uses a maximum size of 15×15 window for noise filtering respectively. The memory requirement of BDND and SAMF are also very high. The proposed algorithm gives superior quantitative metrics than DBA and also removes streaks which occur in DBA at high levels of noise as seen in Fig. 5. From Table 4, it is inferred that with respect to the CPU time, proposed algorithm proves to be the best making it efficient for hardware implementation. In comparison with the recently proposed MDBUTMF, the proposed algorithm shows superior performance in terms of noise removal and edge preservation for low to high density noise levels. In order to verify the edge preservation capability of the proposed algorithm, an error image of various filters obtained by subtracting the original and restored Lena image which is corrupted with 90% salt and pepper noise is presented in Fig. 6. The error image of the proposed algorithm shown in Fig. 6(k) clearly shows that the proposed algorithm gives better edge preservation than the other methods.

The performance of the proposed algorithm is also tested for color image such as Barbara of size 512×512, 8 bits/pixels using scalar median filtering approach. The restoration results of various filters for Barbara image corrupted with 90% salt and pepper noise are given in Fig. 11(c)–(m). Fig. 11(i) and (k) shows that the restored image by BDND and SAMF completely removes the salt and pepper noise at the cost of blur effect. From Fig. 11(m), it is clearly shown that the proposed algorithm removes the salt and pepper noise effectively and also preserves fine details.

6. Conclusion

In this paper, a fast switching median–mean filter (FSMMF) is proposed. It uses a small fixed 3×3 size window for processing the noisy image and restores the original image effectively. The proposed filter effectively overcomes the problem of streaking effects in DBA and poor noise removal capability of MDBUTMF at higher noise densities. In addition to that the proposed filter gives good visual and quantitative results as comparable to the popular techniques like BDND, SAMF and PSMF which are much time consuming though they produce good results. The proposed algorithm also makes an alternate replacement that preserves edges without compromise on time complexity thus making its hardware realization feasible. Simulation results show that the proposed algorithm outperforms the state-of-art filters in removing salt and pepper noise and preserving fine details in the image up to a noise density as high as 90%.

References

[1] Pitas I, Venetsanopoulos AN. Nonlinear digital filters: principles and applications. Boston, MA: Kluwer Academic; 1990.
[2] Astola J, Kuosmanen P. Fundamentals of nonlinear digital filtering. Boca Raton, FL: CRC; 1997.
[3] Yin L, Ruikang Yang, Moncef Gabbouj, Yrjo Neuvo. Weighted median filters: a tutorial. IEEE Trans Circuits Syst II 1996;43(3):157–92.
[4] Ko S-J, Lee YH. Center weighted median filters and their applications to image enhancement. IEEE Trans Circuits Syst 1991;38(9):984–93.
[5] Hwang H, Haddad RA. Adaptive median filters: new algorithms and results. IEEE Trans Image Process 1995;4(4):499–502.
[6] Chen T, Wu HR. Adaptive impulse detection using center-weighted median filters. IEEE Signal Process Lett 2001;8(1):1–3.
[7] Wang Z, Zhang D. Progressive switching median filter for the removal of impulse noise from highly corrupted images. IEEE Trans Circuits Syst II 1999;46(1):78–80.
[8] Ng P-E, Ma K-K. A switching median filter with boundary discriminative noise detection for extremely corrupted images. IEEE Trans Image Process 2006;15(6):1506–16.
[9] Srinivasan KS, Ebenezer D. A new fast and efficient decision-based algorithm for removal of high-density impulse noises. IEEE Signal Process Lett 2007;14(3):189–92.
[10] Haidi I, Nicholas SPK, Theam FN. Simple adaptive median filter for removal of impulse noise from highly corrupted images. IEEE Trans Consum Electron 2008;54(4).
[11] Esakkirajan S, Veerakumar T, Subramanyam AN, PremChand CH. Removal of high density salt and pepper noise through modified decision based unsymmetric trimmed median filter. IEEE Signal Process Lett 2011;18(5):287–90.
[12] Chan RH, Ho C-W, Nikolova M. Salt and pepper noise removal by median type noise detectors and detail preserving regularization. IEEE Trans Image Process 2005;14(10):1479–85.
[13] Zhang S, Karim MA. A new impulse detector for switching median filters. IEEE Signal Process Lett 2002;9(11):360–3.
[14] Chao Lin T. A new adaptive center weighted median filter for suppressing impulsive noise in images. Int J Inform Sci 2006;117:1073–87.
[15] Wang Z, Bovik AC, Sheikh HR, Simoncelli EP. Image quality assessment: from error visibility to structural similarity. IEEE Trans Image Process 2004;13(4):1–14.