cryptography

MDPI

Article

Tamper and Clone-Resistant Authentication Scheme for Medical Image Systems

Mayssa Tayachi [1,*], Saleh Mulhem [2], Wael Adi [3], Laurent Nana [1], Anca Pascu [1] and Faouzi Benzarti [4]

[1] Laboratoire des Sciences et Techniques de l'Information, de la Communication et de la Connaissance (Lab-STICC), Centre National de la Recherche Scientifique (CNRS), Université de Brest, 29238 Brest, France; laurent.nana@univ-brest.fr (L.N.); ancapascu@icloud.com (A.P.)
[2] Institute of Computer Engineering, University of Lübeck, 23562 Lübeck, Germany; mulhem@iti.uni-luebeck.de
[3] Institute of Computer and Network Engineering, Technical University of Braunschweig, 38106 Braunschweig, Germany; w.adi@tu-bs.de
[4] Laboratoire de Recherche, Signal, Image et Technologie de l'Information (LR-SITI), Ecole Nationale d'Ingénieurs de Tunis (ENIT), Le Belvédère 1002, Tunisie; faouzi.benzarti@ensit.rnu.tn
* Correspondence: mayssa.tayachi@univ-brest.fr; Tel.: +33-7-7327-3437

Received: 22 April 2020; Accepted: 19 June 2020; Published: 6 July 2020

Abstract: Telemedicine applications are more and more used due to the rapid development of digital imaging and information and communication technologies. Medical information which include digital medical images and patient's information are extracted and transmitted over insecure networks for clinical diagnosis and treatments. Digital watermarking is one of the main approaches used to ensure the security of medical images. Nevertheless, in some cases, the only use of digital watermarking is not sufficient to reach a high level of security. Indeed, the watermark could carry essential patient information and needs to be protected. In such cases, cryptography may be used to protect the watermark and to improve the overall secured management in the medical environment. In this paper, we propose a clone-resistant watermarking approach combining a difference expansion watermarking technique with a cryptographic technique based on secret keys generated by a clone-resistant device called Secret Unknown Ciphers (SUCs). The use of SUCs to sign the watermark enforces the security of medical images during their transfer and storage. Experimental results show that the system provides a high level of security against various forms of attacks.

Keywords: watermarking; cryptography; security; authentication; secret unknown ciphers (SUCs); telemedicine; medical images

1. Introduction

In the universal declaration of human rights, health and medical care are considered as fundamental rights of humans [1]. Any try to tamper, exploit, or misuse the healthcare information systems are not only an illegal operation but also threatens human rights. For instance, tampering with medical images can lead to wrong diagnosis and treatment [2]. Therefore, the need for a secure healthcare information system increases steadily every day.

Telehealth and/or telemedicine applications provide a good tool for remote clinical services such as exchanging digital medical images, patient's information, etc. the so-called medical information. These services and others face several challenges, for instance, "developing tools to enable risk assessment, developing a method for unique patient identification, identifying practices to safely manage medical information transmissions" [3]. Particularly, the medical image transmission over

insecure networks has many security challenges; firstly, a small alteration in the region of interest in medical images (region used for the medical diagnosis) can affect the patient's life. Therefore, mandatory security requirements must be followed by users of medical images such as confidentiality, integrity, availability, authenticity, and data traceability [4].

Recently, a new hardware-oriented approach has been presented. It is based on hardware security modules that play an important role in ensuring the trustworthiness and integrity of electronic systems. Such modules provide each electronic device in a system with random digital signatures [5]. In [6], the Physical Unclonable Function (PUF) was proposed to be the backbone of a medical image system. PUFs can here be perceived as device-intrinsic electronic fingerprints. Due to the PUF, the proposed unclonable medical image system in [6] could securely exchange medical images. Unfortunately, the unclonable medical image system such as other similar systems deploying PUFs suffers from the well-known PUF-drawbacks and vulnerabilities such as the noisy and inconsistent responses together with a limited number of PUF- challenge-response pairs [7]. On the other hand, a Secret Unknown Cipher (SUC) was introduced as an alternative to the PUFs in [8]. Physically clone-resistant identities based on SUC were first proposed to provide an electronic device with the so-called electronic DNA (e-DNA) in [8] and [9]. The target of SUCs is to prevent tamper and cloning attacks by embedding a low-complexity, non-repeatable, and unpredictable cryptographic function in an electronic device. Such a function is considered highly consistent and error-free comparing to PUFs. This work presents a possible approach towards constructing a clone-resistant watermarking system by providing each electronic device in the medical image system with a clone-resistant unpredictable unique digital SUC signature.

The main contribution of this paper is to propose a clone-resistant watermarking system for medical images based on difference expansion watermarking and SUC techniques. The unpredictable, unclonable, unique watermark signature is generated by using SUC. Pertinent features extracted from the DICOM image are used as input to the Jacobian model [10] in order to build a meaningful watermark. This watermark is signed with the SUC-output in order to obtain a clone resistant signed watermark. The combination of SUC with watermarking ensures strong integrity, and authenticity and provides a high level of security to the medical image system. Indeed, in addition to the reversibility of the proposed watermarking, which ensures the retrieval of the original medical image at the extraction phase as well as good resistance against image processing attacks, SUC as a clone resistant identity can prohibit any image faking and tampering attacks efficiently.

The paper is organized as follows:

- The state of the art of watermarking, PUFs, and some related works are summarized in Section 2.
- The SUC-creation process is briefly presented in Section 3 to make the paper self-contained.
- Section 4 presents our proposed clone-resistant watermarking approach. The benefits of combining SUC and watermarking are carefully discussed and the proposed system operation scenario and its protocols are presented in detail.
- In Section 5, the threat model and security level of the proposed system are analyzed and evaluated. The performance evaluation of our proposed system is estimated through some experimental results.
- Section 6 concludes the paper.

2. Background Motivation and State of the Art

There are two main approaches to ensure a high-security level of medical image transmission systems [2]: First, watermarking which is defined as a technique of embedding certain information into a medical image [11]. Digital watermarking targets are data-hiding, integrity control, and authenticity [12]. Second, metadata which is defined in this context as the attached data to a medical image. Here, the digital signature is one of the famous techniques of metadata that ensures the integrity and the authenticity of the medical image.

Figure 1 illustrates the previous two techniques to provide medical image transmission systems with a high level of security. In Figure 1a, a digital signature is generated by an asymmetric algorithm after signing a hashed value of the original medical image. The concatenation operator links the original medical image and the digital signature to generate a signed image. On the receiver side, the verification of the validity of the resulting signed image requires the corresponding public key to retrieve the received hashed value and compare it with the computed hashed value from the original medical image. The presented digital signature scheme deploys a hash function and asymmetric encryption. However, the asymmetric encryption algorithms are considered as computationally intensive techniques, relatively slow, and a certificate authority is required to manage the public keys [13].

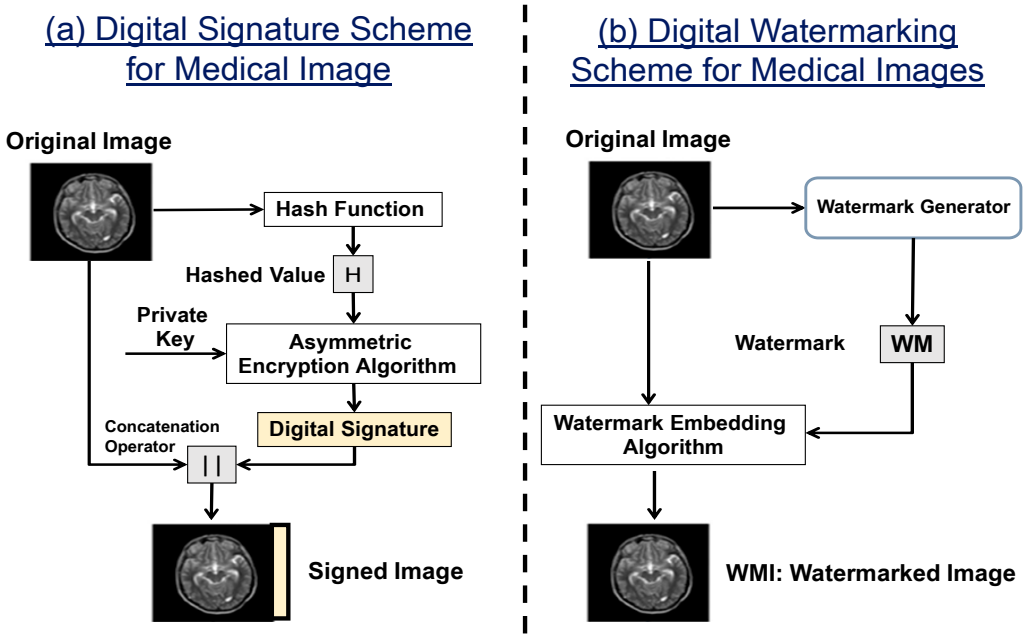

Figure 1. Two state of the art proposals of secure medical image transmission systems.

In Figure 1b, a watermarking system is presented. A watermark (WM) is, in particular, extracted from the original medical image by a watermark generator. Then, the extracted watermark is embedded in the original medical image. Moreover, the medical information such as the patient's information, hospital logo, and Doctor ID can be embedded into the original image as a watermark for authentication, tamper-proofing, and copyright protection as well [14,15]. In [13], a technical discussion about watermarking for medical images and other security techniques was reviewed. The results showed that watermarking techniques are still not accepted yet for modern applications, where the current watermarking techniques suffer from some weaknesses; for instance, the sensitivity of the bit error is very low, and the possibility of detecting a valid watermark image as an invalid watermark image or vice versa is very high [13]. As a solution to such vulnerabilities, several medical image security approaches that merge watermarking and cryptographic techniques for medical image systems were proposed in the literature such as [16–18]. In the following, we briefly present some related works to the combination of watermarking and cryptographic primitives.

2.1. Combining Watermarking with Cryptographic Primitives

Watermarking and cryptographic techniques were deployed to ensure a high level of security of medical images transmissions. In [18], the watermark generator together with an encryption algorithm was proposed to ensure the content-confidentiality of the image. In particular, this system merges an Integer Wavelet Transform (IWT)-(Least Significant Bit) LSB watermarking and an encryption

algorithm using a random permutation and a chaotic keystream-based key generator. Electronic patient record (EPR) and context information are extracted and used as watermarks to be embedded into the original images. Although the proposed encryption algorithm has advantages to secure medical images, it still has disadvantages such as once the image is decrypted, it is no longer protected and it becomes difficult to verify its origin and its integrity [19]. In [20], a robust and secure watermarking approach was proposed for telehealth applications. This approach combines three watermarking techniques of the transform domain: Digital Wavelet Transform (DWT), Discrete Cosine Transform (DCT), and Singular Value Decomposition (SVD). The patient record/identity is embedded in the original medical image. A chaotic encryption algorithm relying on two-dimensional logistic maps was applied on a watermarked image in order to improve patient data confidentiality. In [21], two watermarking algorithms dedicated to medical images in the transform domain were proposed. In the first watermarking algorithm, a digital watermark and EPR are embedded in the Region of Interest (ROI) and Region of Non-Interest (RONI). In the second one, ROI is kept unmodified for telediagnosis reasons and RONI is deployed to hide the digital watermark and EPR. In [22], a medical image watermarking algorithm based on the wavelet was proposed. In the suggested technique, the cover medical image is decomposed into ROI and RONI regions and three different watermarks are embedded into the RONI part using DWT. In [23], a system combining encryption and watermarking in the spatial domain was presented. The encryption relies on the Advanced Encryption Standard (AES) in a Cipher Block Chaining (CBC) mode. Integrity and authenticity factors were checked by the authors. The performance evaluation of the system showed that the Peak Signal to Noise Ratio (PSNR) obtained without attacks was around 49 dB. The experimental result showed an acceptable quality and sufficient capacity for embedding.

It is noted that all previous proposals do not deploy physical marking for the watermark. Such a technique is utilized to mark physically a product for future reference such as origin, authenticity, etc. [24]. This flaw or weak point leaves the medical image device/generator without any proof of the ownership.

2.2. *Unclonable Medical Image Transmission System*

In [6], PUF was proposed to provide the Medical Image System (MIS) with a device-intrinsic electronic fingerprint. Here, each medical image device/generator has PUF. Figure 2 illustrates the designed MIS in [6].

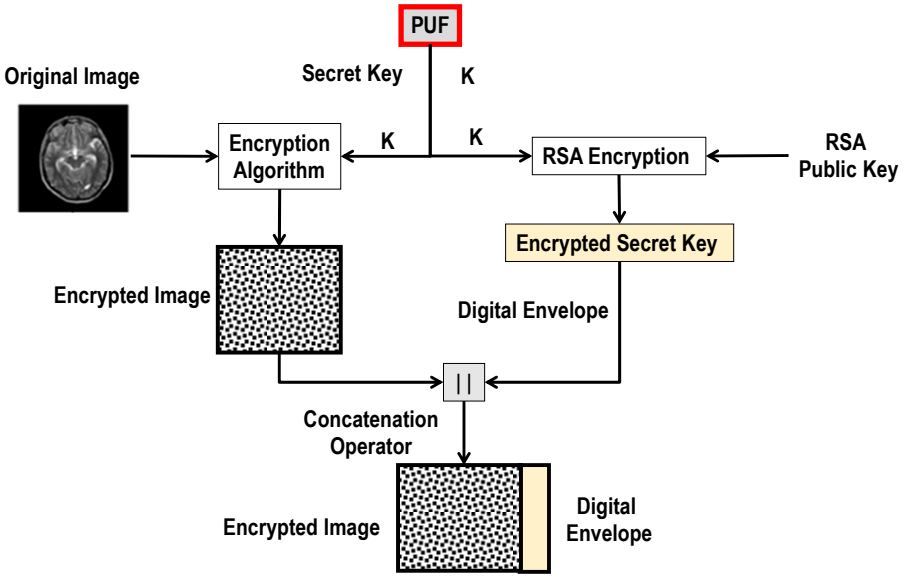

Figure 2. Medical image system deploying the physical unclonable function (PUF) together with an encryption algorithm and RSA system. Adapted from [6].

In particular, PUF generates a secret key K for an encryption algorithm. The generated secret key K is utilized to encrypt the original image. Here, the RSA system as an asymmetric algorithm protects the generated secret key K and generates a digital envelope as an encrypted K by the RSA-public key of the receiver. A medical image device/generator as a sender transmits the resulting encrypted image together with the digital envelope to the receiver side. On the receiver side, the receiver recovers the secret key K from the digital envelope by using its RSA-secret key. Then, the receiver uses K to decrypt the received encrypted image.

Similar to the Pretty Good Privacy (PGP) mechanism for data communication [25], the proposed MIS in Figure 2 provides cryptographic privacy and authentication for digital medical images. The only difference between them is that the proposed MIS utilizes a PUF to generate a secret key K instead of a pseudorandom number generator in the case of PGP. Furthermore, the proposed MIS is a computationally intensive mechanism, relatively slow, and requires a certificate authority to manage the RSA public- and private- keys. On the other hand, several research efforts were published on PUFs in the last two decades such as ring oscillator PUFs [26], TERO-PUF [27], arbiter PUFs [28], Chaos-based PUF [29], etc. Unfortunately, the noisy and inconsistent responses together with a limited number of PUF- challenge-response pairs are considered as the main PUF vulnerabilities [7]. Any attempt to counteract such vulnerabilities makes the PUF implementation more expensive and complicated.

To overcome such weaknesses of MIS, a clone-resistant watermarking technique is proposed for medical images based on SUC defined in [8,30]. SUC is highly consistent and provides each electronic device in the MIS with a clone-resistant unpredictable unique digital signature. The proposed technique combines a watermarking algorithm and a physically clone-resistant identity to generate a clone-resistant watermarking system for medical images. This work introduces a new approach towards constructing a clone-resistant watermarking.

3. The SUC Concept and Its Realization as an Alternative to the PUF

This section is a slightly-modified version of the same section of our earlier publications [31,32] on the SUC design technique. It aims to make the paper self-contained, more understandable, and to provide the reader with further information on SUC-creation process.

Figure 3 illustrates a possible SUC-creation process in a modern System-on-Chip (SoC) Field Programmable Gate Arrays (FPGA). The required SoC FPGA device should fulfil the following requirements:

- A non-volatile/flash-based FPGA-fabric.
- Self-reconfigurable FPGA device.
- FPGA with an internal true random number generator (TRNG) meeting the requirements of a NIST standard.

In such an FPGA, the SUC-creation process may proceed by a program (software package) called GENIE as follows:

- A cipher-class $\{E_1, E_2 \ldots E_\sigma\}$ with large cardinality ($\sigma \rightarrow \infty$) is generated.
- A single-event process with the help of the internal TRNG leads to a one-time random choosing of a cipher E_j from the generated class $\{E_1, E_2 \ldots E_\sigma\}$.
- Lastly, all the dashed symbols (entities) are completely eliminated, irreversibly abolished, and fully removed from the chip in Figure 3. What remains inside the chip is just an irreversible, unrepeatable, and unpredictable cipher module E_j as unknown cipher-choice even to the designer himself.

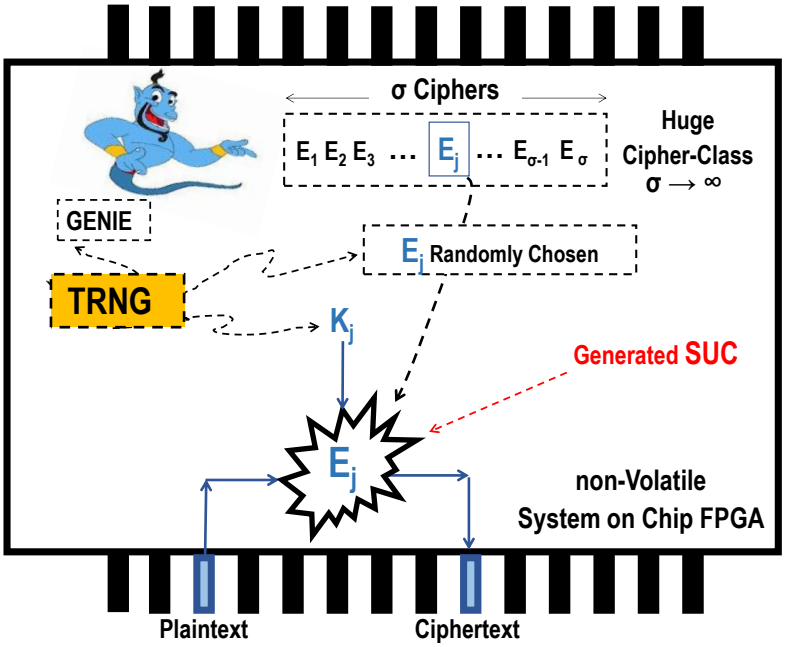

Figure 3. Possible secret unknown cipher (SUC) generation scenario. Adapted from [32].

It should be noted again that an emerging VLSI device with a self-reconfiguring capability is fundamentally required to realize usable unknown structures so-called SUC as "an electronic mutation" [33].

The concept of unknown ciphers is considered as a new security paradigm. The unknown cipher is basically designed and proposed to provide a clone-resistant identity in an authentication scheme [8]. Therefore, the unknown cipher does not violate Kerckhoff's principle for a cryptosystem as long as the unknown cipher does not deal with protecting the communications between at least two parties, which requires the cipher design to be public knowledge and commonly known to all parties except the cipher-key (based on Kerckhoff's principle). It should be also pointed out that the SUC-security paradigm cannot be classified under "security by obscurity", where the cipher is designed to be exclusively known to the designer/manufacturer, and then kept obscure.

Furthermore, if the cipher designer is not able to precisely predict and determine the generated cipher, then the cipher is considered as not known/unknown. Here, we assume that "unclonability" is only possible and attained if unknown structures are generated.

Unknown Ciphers as Clone-Resistant Modules

To construct a clone-resistant watermarking approach, it is required that each medical device embeds its unique SUC as an unclonable or clone-resistant identity. Generating a hardwired function SUC is based on the following key idea: "The only secret which can be kept unrevealed is the one which nobody knows" [34]. Figure 4 shows the SUC-creation phase processed in a secure environment as follows [32]:

1. A software package "GENIE" as an SUC creator is shortly injected by a trusted authority (TA) into a SoC FPGA.
2. The GENIE generates/chooses a cipher with the help of an internal unpredictable bit stream from the internal TRNG.
3. The GENIE is irreversibly eliminated and completely removed from the SoC FPGA. What remains inside the SoC FPGA is an unchangeable, non-repeatable, and unremovable cipher (SUC) which no one knows.

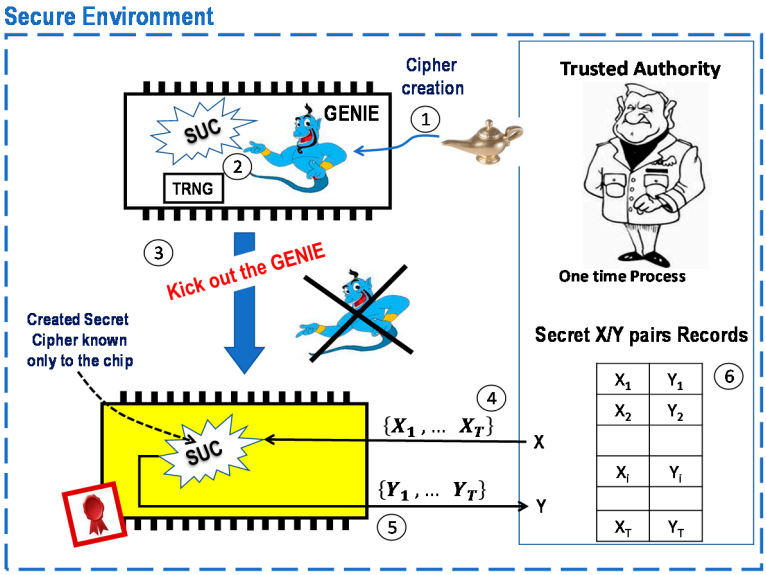

Figure 4. Mutating an SUC into a system-on-chip (SoC) [32].

SUC enrollment phase [32]:

4. TA randomly chooses a set of plaintexts $\{x_1, \ldots x_T\}$ out of the 2^n possible inputs, where the SUC-input size is n bits input-size.
5. TA stimulates the SoC with the set of plaintexts $\{x_1, \ldots x_T\}$ to get the corresponding ciphertexts $\{y_1, \ldots y_T\}$ using its SUC.
6. TA stores the resulting SUC T-(x_i, y_i) pair in a secret pair record for later use.

The random, unpredictable, non-repeatable, and unknown bit stream generated by the TRNG is fully and exclusively responsible for generating the SUC. Therefore, the generated SUC in the SoC is similarly unpredictable, non-repeatable, and unknown. Thus, for every time point $t > 0$.

$$\mathrm{SUC}_t = GENIE(TRNG_t) \tag{1}$$

And for any t_1 and t_2:

$$TRNG_{t_1} \neq TRNG_{t_2} \rightarrow \mathrm{SUC}_{t_1} \neq \mathrm{SUC}_{t_2} \tag{2}$$

With a very high probability.

Furthermore, SUC can mathematically be described as:

$$\mathrm{SUC}_t : \{0,1\}^n \times \{0,1\}^{k_t} \rightarrow \{0,1\}^n \tag{3}$$

where n and k_t are the SUC input/output size and the bit size of the cipher's secret key, respectively. It is well known that the cardinality of the set of all possible permutations from $\{0,1\}^n$ to $\{0,1\}^n$ is $2^n!$ Therefore, $\sigma = 2^n!$ is theoretically the number of all possible ciphers including their key-choices that can be selected as SUCs. Here, the probability P_{SUC} of every resulting SoC FPGA device having its unique and individual SUC is:

$$P_{\mathrm{SUC}} = 1 - \frac{1}{\sigma} \rightarrow 1 \tag{4}$$

In difference to PUFs, SUC is a cipher equivalent to a Pseudo Random Function (PRF). Notice that all 2^n possible pairs are selectable with an equal security level.

SUC authentication phase:

Figure 5 illustrates a generic SUC-based identification protocol for verifying an enrolled SoC_A. The proposed protocol may proceed as follows [32]:

1. TA randomly chooses a pair (x_i, y_i) from the secret records of SoC_A. Then, the TA sends y_i to SoC_A.
2. The SoC_A device decrypts y_i by using its SUC_A and sends the plaintext x'_i to TA.
3. SoC_A is authentic when $x'_i = x_i$. TA then marks the pair (x_i, y_i) as a used pair and never uses it again.

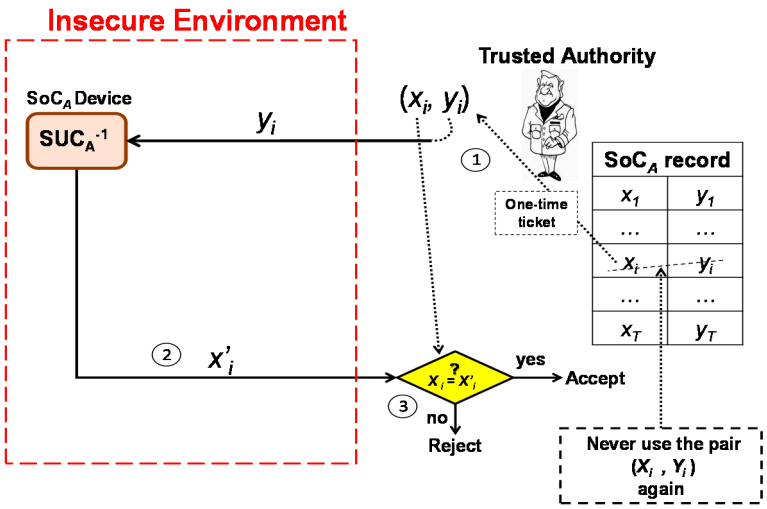

Figure 5. SUC-based generic identification protocol. Adapted from [32].

4. A Proposed New Secured Unclonable Medical Watermarking Scheme

The key idea of the proposed approach is to embed SUC in each medical image device to make them physical unclonable. A medical image generator with an embedded SUC, in particular, becomes a clone-resistant medical image generator. Figure 6 illustrates a sample comparison between a traditional medical device without an SUC identity and a medical device with an embedded SUC.

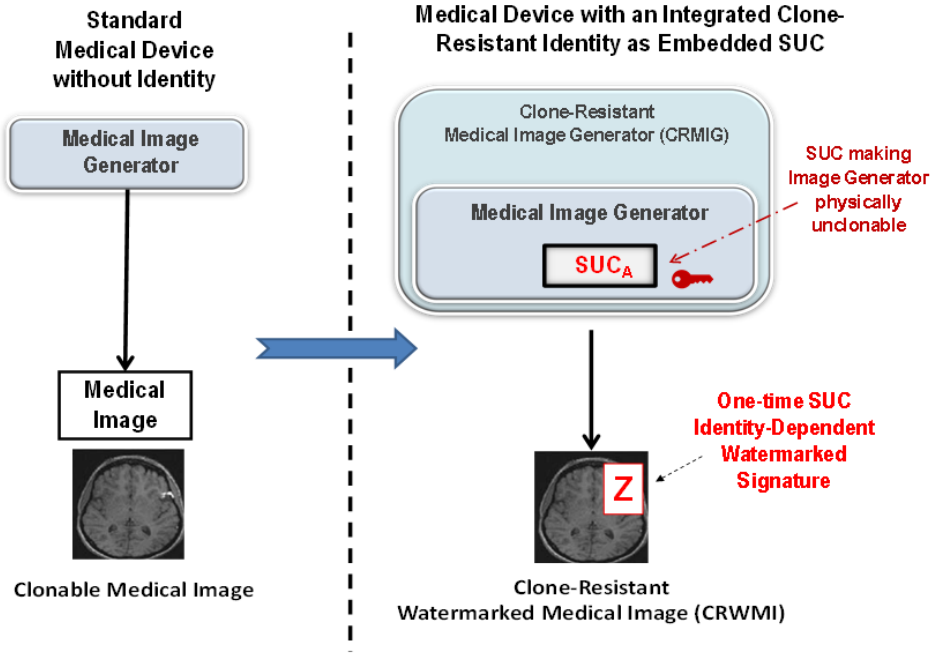

Figure 6. The proposed concept of making medical images clone-resistant by embedding the SUC technique.

The proposed clone-resistant medical image generator (CRMIG) produces a clone-resistant watermarked image as follows: After generating the original image, a watermark (WM) is generated and then it is signed by using one SUC input-output challenge pair as a one-time ticket. The resulting signed watermark (Z) is embedded in the original image as a one-time watermark signature. The resulting MIS attains the following security features:

(i) Medical images are not repeatable and are non-replaceable.
(ii) Medical images are non-splice-able.
(iii) Non-repudiation.
(iv) Provably unique medical images.
(v) Integrity guarantee.
(vi) Authentication.

The proposed CRMIG counteracts all expected splicing and cloning attacks as SUC provides a medical image generator with a unique signature which is non-repeatable and unclonable.

4.1. The Proposed Medical Image System Architecture

The proposed MIS allows a doctor/user to receive securely a medical image through a TA server. The doctor does not communicate directly with a medical image generator. Here, the TA server plays a mediator role in the proposed system. In Figure 7, the proposed system architecture comprises three main components: First, the TA server hosts a secure database (DB). Second, the medical device as an example of the clone-resistant medical generator A. Third: A doctor D as an eligible user with an embedded SUC in his or her own device such as a computer or mobile/token.

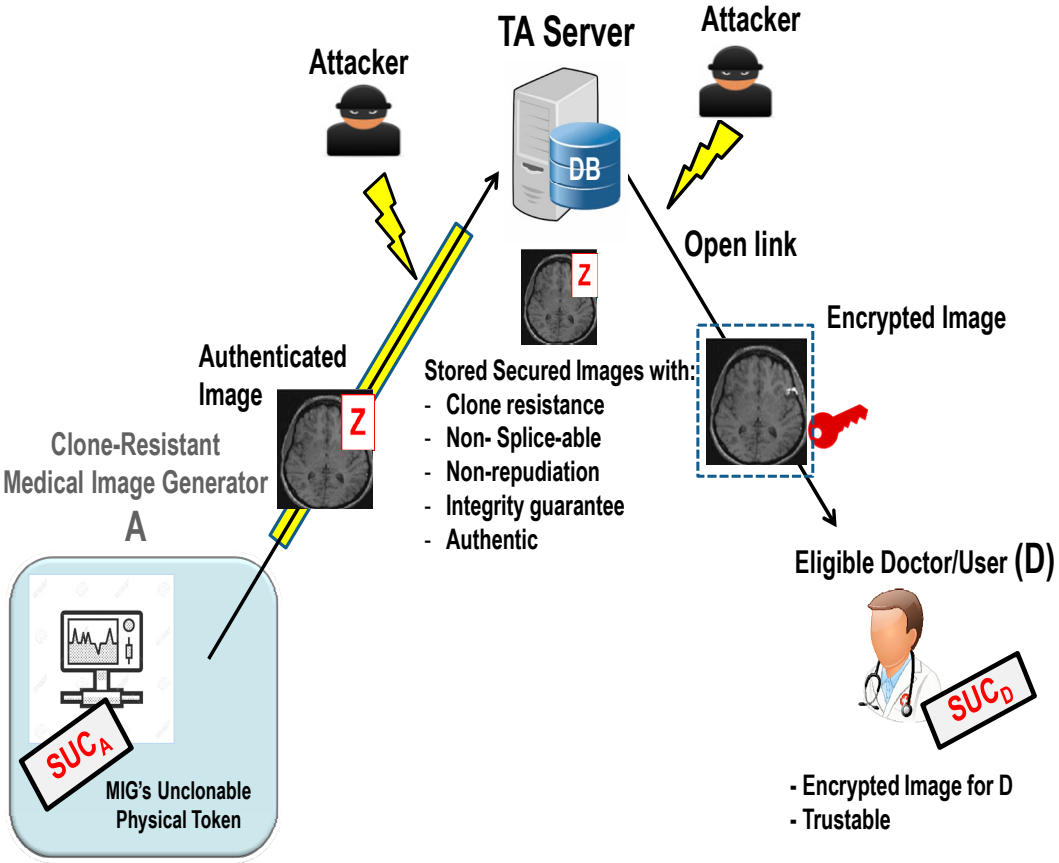

Figure 7. A proposed system operation scenario.

All medical devices should be registered in TA DB. The proposed MIS attains the following security features:

(i) Medical images are not repeatable and are non-replaceable.
(ii) Provably unique medical images.
(iii) Selective authentication privilege.

Figure 8 illustrates the TA DB structure that stores patient records. Each patient record contains patient's medical images, and some information about their watermarked images.

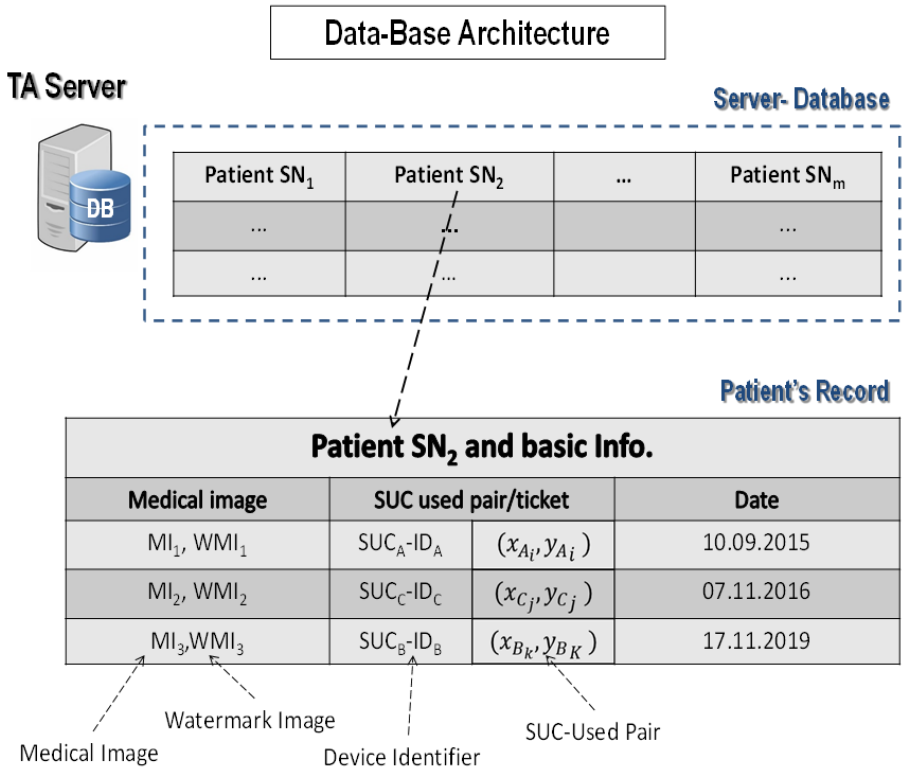

Figure 8. An example of a patient's record in the database (DB).

Figure 8 shows an example about a patient's record consisting of the basic information of the patient, the patient's watermarked images, medical devices IDs and the used tickets for signing watermarks, and the data. Note that the clone-resistant watermarked image is transmitted and stored in TA DB. Therefore, each user/doctor should send a request to the TA server to get a patient's medical image. In this proposed system architecture, the user/doctor cannot communicate directly with the medical device. The communication is only done through the TA server and the communication with the TA server is performed over insecure channels.

4.2. The Proposed Embedding and Extraction of Clone-Resistant Watermarking

The proposed system has two main phases: First, generating and embedding a signed watermark into the original image. Second, extracting the watermark and using it to verify the authenticity and integrity of the watermarked image. These two phases are described as follows:

4.2.1. Generating, Signing, and Embedding Watermarks (One-Time Watermark Signature)

Pertinent features namely skewness, entropy, and median are extracted from the original image [35]. The patient name is extracted from the header of the DICOM image and the corresponding initials (the first letter of the given name and family name) are transformed into a binary matrix of size 16×16.

A matrix of size 16 × 16 is then generated from the original image by a cumulative subtraction process. All this information is used to build a meaningful watermark based on the Jacobian model [10].

The embedding process of the watermark is illustrated in Figure 9. A standard cipher E is deployed to sign the extracted watermark by using a one-time ticket (x_A, y_A) offered by TA for SUC_A of the imaging device. Here, the chosen standard cipher E can be perceived as a tool for the signature mechanism and E should be secure in terms of indistinguishability [36]. The resulting signed watermark can be considered as a one-time clone-resistant watermark signature Z. After that, Z is embedded in the original image using the difference expansion technique to obtain the clone resistant watermarked image (WMI).

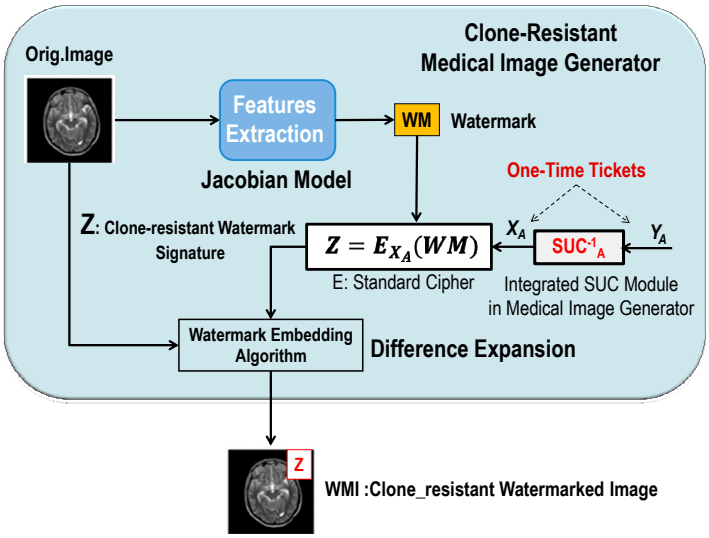

Figure 9. Clone-resistant watermark generation and embedding process.

4.2.2. Procedure of Extraction and Verification of the Watermark

The procedure of extraction and verification of the watermark is the inverse of the watermark embedding and signing phase. Such a process is illustrated in Figure 10. The process starts with extracting the signed watermark Z and recovering the watermark.

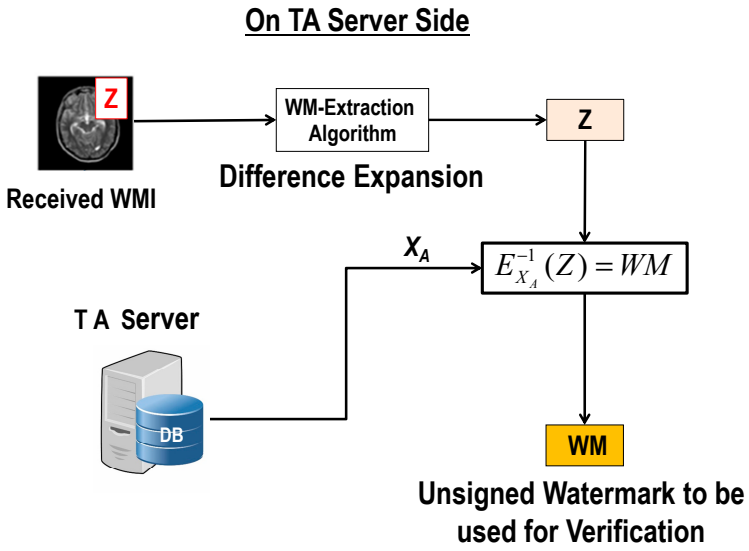

Figure 10. Watermark extraction process.

During this process, the stored used plaintext X_A is obtained from the TA server to complete the verification process. The receiver should compare the unsigned WM with the extracted WM again. The verification (comparison) can be done before clinical procedures and diagnosis.

4.3. System Analysis: Benefits of Combining SUC and Watermarking

The main goal of this section is to highlight the peculiar and efficient watermarking procedures when the SUC technique is involved. For this purpose, two generic primitive protocols for generating and verifying the proposed clone-resistant watermarked images are presented.

4.3.1. Protocol 1: Secured Logging of a Medical Image Transaction

The first proposed generic protocol is designed to illustrate the process of generating a clone-resistant watermarked medical image. Medical device A generates a watermarked image and sends it to the TA server. Then, the TA server verifies the watermarked image and stores it in the DB.

Figure 11 shows the proposed protocol which can proceed as follows:

1. Medical device A asks the TA server to start the process of generating a watermarked image.
2. The TA server randomly selects a ticket $\left(x_{A_i}, y_{A_i}\right)$ from the medical device A's secret record in DB.
3. The TA server answers with y_{A_i}.
4. Medical device A computes x_{A_i} by using its SUC as $\mathrm{SUC}_A^{-1}\left(y_{A_i}\right) = x_{A_i}$.
5. Medical device A generates or selects a medical image MI_1.
6. Medical device A generates a watermark WM_1 from MI_1.
7. Medical device A signs the generated watermark WM_1 by using a standard cipher E with the secret key x_{A_i} as: $Z = E_{x_{Ai}}(WM_1)$.
8. Medical device A embeds the signed watermark Z in the original image MI_1 to generate the clone-resistant medical watermarked image WMI_1.
9. Medical device A sends WMI_1 to the TA server.
10. TA server reverses the embedding algorithm to extract Z and to recover the medical image MI_1 from the received watermarked image WMI_1 and then uses x_{A_i} to recover the watermark $WM\prime_1$.
11. TA server generates WM_1 from the recovered medical image MI_1 and rejects if $WM_1 \neq WM\prime_1$.
12. TA server stores and registers the medical image transaction MI_1, WMI_1, WM_1, and ID_A, together with the used ticket $\left(x_{A_i}, y_{A_i}\right)$ in DB for later use.

Protocol.1 attains the following security functions:

(i) Medical device A generates a clone-resistant watermarked image by deploying its SUC_A.
(ii) The resulting watermarked image is authentic and tamper-resistant.

4.3.2. Protocol 2: User-Server Authentication Protocol for Image Verification

This sample generic protocol allows a user such as doctor D to request a patient's medical image from the TA server. Then, the TA server answers with the requested image as shown in Figure 12.

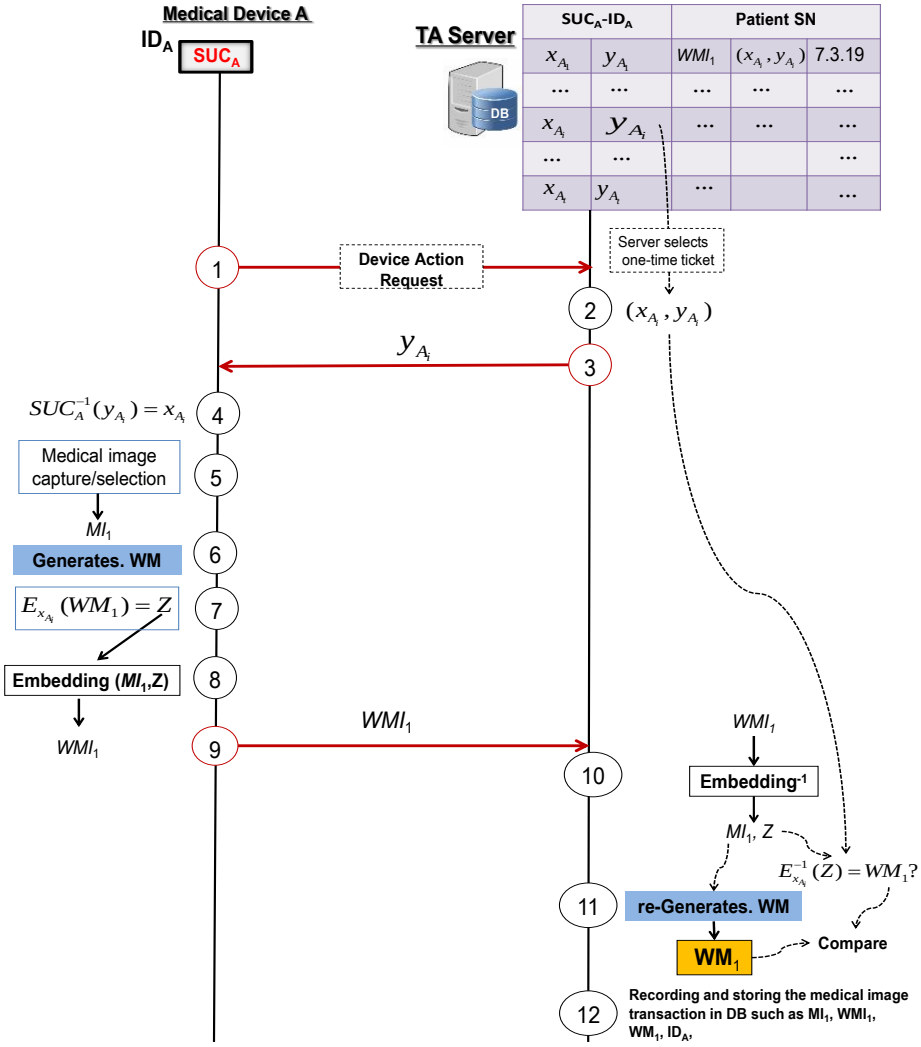

Figure 11. Medical device-server authentication protocol for secured logging of a medical image transaction and image verification.

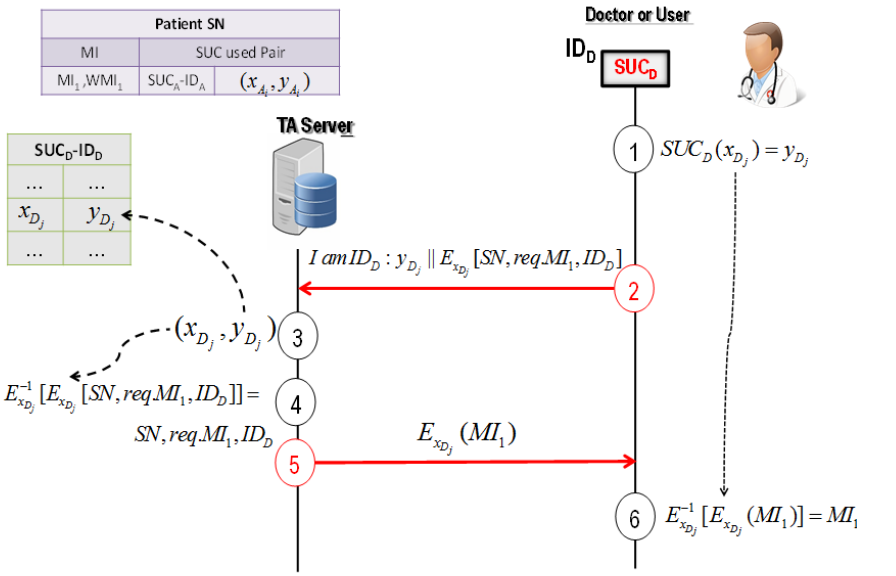

Figure 12. User-server authentication protocol for exchanging registered medical images.

Protocol.2 can proceed as follows:

1. Doctor D randomly selects x_{D_j} and computes the corresponding cyphertext y_{D_j} by using its SUC_D.
2. Doctor D asks the TA server to send the required medical image MI_1 of the patient SN as $y_{D_j} \Big| E_{x_{D_j}}(SN,\ req.MI_1, ID_D)$, where $req.MI_1$ is the request of the medical image MI_1 and ID_D is a public identifier of doctor D.
3. TA server uses y_{D_j} to determine x_{D_j} from the device D's secret record in DB.
4. TA server decrypts the received message $E^{-1}_{x_{D_j}} E_{x_{D_j}}(SN,\ req.MI_1, ID_D) = SN,\ req.MI_1, ID_D$. If the decrypted ID_D matches the public identifier ID_D of doctor D, the TA server registers the request of the medical image MI_1 and doctor D cannot deny using MI_1.
5. TA server answers with $E_{x_{D_j}}(MI_1)$, where MI_1 is the medical image.
6. Doctor D decrypts the received message: $E^{-1}_{x_{D_j}} E_{x_{D_j}}(\ MI_1) = MI_1$. It should be noted that doctor D cannot generate or predict the signed watermark Z of MI_1 stored in DB (see Section 5). Therefore, doctor D cannot change and fake MI_1.

This proposed protocol attains the following security functions:

(i) Doctor D cannot deny using the image generated by medical device A.
(ii) The stored image in the TA server cannot be changed or faked later by doctor D.
(iii) TA server knows undeniably "who and when" a user such as doctor D was using the medical image.

4.4. The Jacobian Model for Generating Watermarks

The Jacobian matrix is a matrix defined from a vector function F and a given point $(x_1, \ldots, x_n) \in R^n$. It is the matrix of partial derivatives of the first order of a vector function.

Let F be a function defined from R^n to R^m, by its m component functions with real values, as follows:

$$F : \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \rightarrow \begin{pmatrix} f_1(x_1, \cdots, x_n) \\ \vdots \\ f_m(x_1, \cdots, x_n) \end{pmatrix} \tag{5}$$

The partial derivatives of these one-point functions M, if they exist, can be arranged in a matrix with m rows and n columns, called the Jacobian matrix of F:

$$J_F(M) = \begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_m}{\partial x_1} & \cdots & \frac{\partial f_m}{\partial x_n} \end{pmatrix} \tag{6}$$

Watermark Generation Using the Jacobian Model

Pertinent features namely skewness, entropy, and median are extracted from the original image. The patient name is extracted from the header of the DICOM image and the corresponding initials (the first letter of the given name and family name) are transformed into a binary matrix of size 16×16. A matrix of size 16×16 called *add_mat* is then generated from the original image by a cumulative subtraction process. All previous information is used to build a meaningful watermark WM based on the Jacobian model.

We suggest 16 functions with 16 parameters to generate a 16×16 matrix that can be exploited to build the watermark. We build all the functions using the binary matrix of the patient name, the three pertinent features (skewness, entropy, and median) extracted from the host image and the matrix *add_mat* extracted from the host image. The proposed Jacobian matrix model is based on a vector Y of 16 functions : $Y_i : R^{16} \rightarrow R$, $I = 1, 2, \ldots, 16$.

These functions $Y_1, Y, \ldots, Y_{16}$ are defined by:

$$Y_i(x_1, x_2, \ldots x_{16}) = \sum_{j=1}^{16} \frac{add\_mat(i,j)}{f\_val_i} \frac{{x_j}^2}{2}, \; j = 1, \ldots, 16 \tag{7}$$

And,

$$f\_val_i = \begin{cases} \text{skewness value if } i = 1, \ldots, 5 \\ \text{entropy value if } i = 6, \ldots, 10 \\ \text{median value if } i = 11, \ldots, 16 \end{cases} \tag{8}$$

The Jacobian matrix J of Y at $(x_1, x_2, \ldots, x_{16})$ is a 16×16 matrix defined as follows:

$$J_Y(x_1 \ldots x_{16}) = \begin{pmatrix} \frac{add\_mat(1,1)}{f\_val_1} x_1 & \cdots & \frac{add\_mat(1,16)}{f\_val_1} x_{16} \\ \vdots & \ddots & \vdots \\ \frac{add\_mat(5,1)}{f\_val_1} x_1 & \cdots & \frac{add\_mat(5,16)}{f\_val_1} x_{16} \\ \frac{add\_mat(6,1)}{f\_val_2} x_1 & \ddots & \frac{add\_mat(6,16)}{f\_val_2} x_{16} \\ \vdots & \ddots & \vdots \\ \frac{add\_mat(10,1)}{f\_val_2} x_1 & \cdots & \frac{add\_mat(10,16)}{f\_val_2} x_{16} \\ \frac{add\_mat(11,1)}{f\_val_3} x_1 & \cdots & \frac{add\_mat(11,16)}{f\_val_3} x_{16} \\ \vdots & \ddots & \vdots \\ \frac{add\_mat(16,1)}{f\_val_3} x_1 & \cdots & \frac{add\_mat(16,16)}{f\_val_3} x_{16} \end{pmatrix} \tag{9}$$

This 16×16 Jacobian matrix is an image matrix used as a watermark intended for embedding in the original image. Examples of watermarks generated with the Jacobian model are presented in Figure 13.

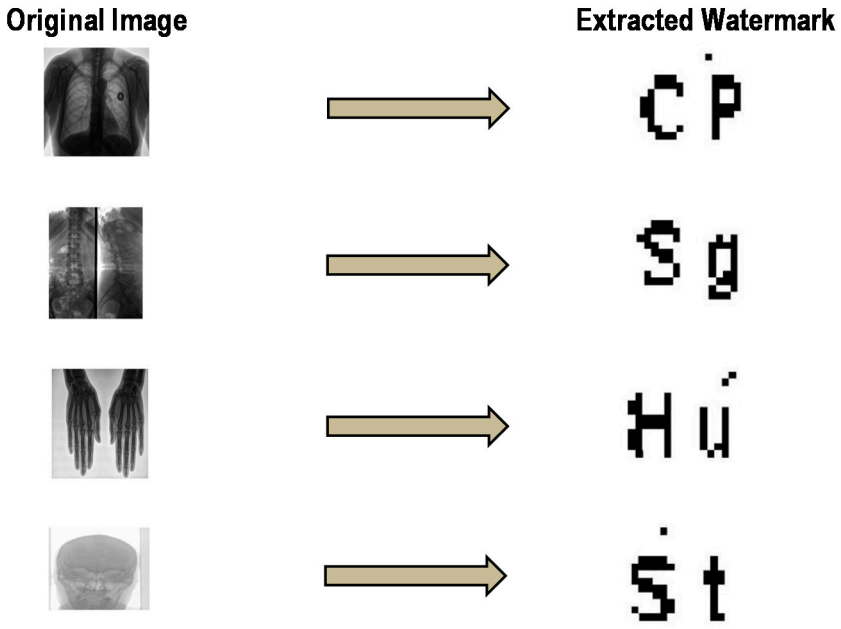

Figure 13. Original images and corresponding watermarks examples.

5. Watermarking Analysis and Security Evaluation

In the following section, the experimental results and the security analysis of the proposed method are presented. Here, AES-128 with the input size of 128 bits is deployed as a standard cipher E. Therefore, the tickets generated by the SUC have the same size, i.e., 128 bits.

5.1. Security Analysis of the Proposed Protocols

This section is dedicated to the security analysis of proposed protocols deploying SUCs. The security analysis of such protocols firstly requires determining the adversary model and then analyzing the possible attack scenarios on the proposed protocols.

5.1.1. Adversary Model

The adversary' assumptions are as follows [37]:

- Ψ can run any medical device with an integrated SUC.
- Ψ can listen to the transmitted and exchanged messages between the TA server and the medical devices.
- Ψ can exchange messages with the medical devices and the TA server.

Such an adversary model can be used in the security evaluation of the proposed protocols. The adversary tries to take advantage of vulnerabilities and drawbacks of the proposed watermarking system. In the following, two attack scenarios are defined and analyzed based on the proposed adversary model: First, Man-in-the-middle Attack (MIM), and second, tampering or faking a medical device with an integrated SUC.

5.1.2. Man-in-the-Middle Attack

In MIMA, an adversary intercepts all exchanged data between a medical device (or a user) and a TA server. The target of the adversary is to eavesdrop and later to deliver false data. Therefore, a successful MIMA is when an adversary can fool a TA server.

In the proposed protocol.1:

The MIMA-adversary intercepts the messages in steps 3 and 8. In this case, the adversary can extract the signed watermark Z from step 8 by using the inverse of the public embedding algorithm.

To deliver a false message to the TA server, a MIMA-adversary should be able to use the signed watermark Z again/later, which is equivalent to the fact that there are two watermark images WM_1 and WM_2 having the same signed watermark $Z_1 = Z_2$. The size of the key space is 2^n, so, the probability of such a collision is 2^{-n}. Therefore, the proposed protocol.1 of MIS is secure against MIMA.

Note that the same analysis can be used to prove that the proposed protocol 2 is secure against MIMA.

5.1.3. Tampering Attacks

In this proposed scheme, tampering attacks refer to an adversary who tries to make changes to the original medical image [38] and then produces a valid signed watermark Z.

For instance, in the proposed protocol 1, a successful tampering attack is equivalent to the successful prediction of x_{A_i} for a specific WM_1 in $E_{x_{A_i}}(WM_1) = Z$. In this case, the adversary can produce a valid signed watermark Z' for a tampered WM by using the predicted x_{A_i}. The following theorem shows that the adversary has a negligible advantage to recover x_{A_i}. However, the definition of pseudorandom functions (PRFs) is required for the proof of the theorem. In [39], Goldreich et al. presented the concept of PRFs as follows:

Definition 1. *PRF is a family of functions F with the following properties:*

- *Every function* $F_K \in F$ *can be uniquely identified by a specific key K.*
- *Every probabilistic polynomial time (p.p.t.) adversary has a negligible advantage to distinguish between the output of* $F_K(.)$ *and a random value.*

Theorem 1. *The success probability of tampering attack a WM generated by device A with an embedded SUC is negligible for every adversary.*

Proof. For the proposed protocol.1, an adversary Ψ interacts with a challenger. The challenger performs the following security experiment (Game) that acts as follows:

- The challenger arbitrarily selects one bit $b \overset{U}{\leftarrow} \{0,1\}$.
- The challenger returns $P \overset{U}{\leftarrow} \{0,1\}^n$, if $b = 1$ to Ψ; otherwise, it returns $P \leftarrow E_{x_{Ai}}(.)$, within time t.

The adversary Ψ then sends a limited number (polynomial number) of queries (q) to the challenger such as y_{A_i}, where $i = 1, \cdots, q$. Then, the adversary returns $b\prime$. Thus, the advantage of Ψ to distinguish the output of $E_{x_{Ai}}(.)$ from a random value is defined as:

$$adv^{E}_{PRF}(\Psi) = \left|\Pr[b = b\prime] = 1\right| \tag{10}$$

Here, Ψ is a probabilistic polynomial time algorithm, i.e., p.p.t. adversary.

Now, assume by contradiction that there is an adversary Ψ who can predict x_{A_i}, for every $i > 0$, with non-negligible probability in the protocol.1 and then the adversary Ψ can tamper the original image generated by medical device A. According to this assumption, the adversary Ψ sends y_{A_i} to medical device A and collects the corresponding $E_{x_{A_i}}(WM_1)$ for $i = 0, 1, \cdots, q$ as Ψ has full access to steps 3, 6, and 7 in protocol 1. After that, the adversary recovers x_{A_i} with non-negligible probability. This means that the adversary Ψ has a non-negligible advantage to distinguish between the output of $E_{x_{Ai}}(.)$ and a random value. Apparently, this contradicts the indistinguishability and the pseudo randomness of the chosen standard cipher E. Therefore, the adversary has a negligible advantage to recover x_{A_i} as:

$$adv^{E}_{PRF}(\Psi) \leq 2^{-n} \tag{11}$$

where 2^n is the number of the all possible x_{A_i}. □

It turns out that the adversary cannot tamper a medical image generated by a device with an embedded SUC. Therefore, the SUC provides a MIS with a security bound of $O(2^n)$.

5.2. Experimental Results

The performance of the proposed method was evaluated using four grayscale medical images in the DICOM format, "Chest", "T-spine"," Hands", and "Skull" of the size of 512 × 512 pixels as host images. A binary watermark of size 16 × 16 is generated from the host images to be embedded. The experiment is performed on a computer with an Intel Core i5, 2.6 GHz CPU, 4 GB memory, windows 10 and MATLAB 2016b (the MathWorks, Natick, MA, USA).

The proposed watermarking system's performance is evaluated in terms of imperceptibility and robustness against various attacks. To measure the imperceptibility of the watermark, SSIM (Structural Similarity Index) and PSNR (Peak Signal to Noise Ratio) values are used. To measure the robustness, BER (Bit Error Rate) and NC (Normalized Correlation) values are used. The original images used to investigate the performance of the proposed method are presented in Figure 14.

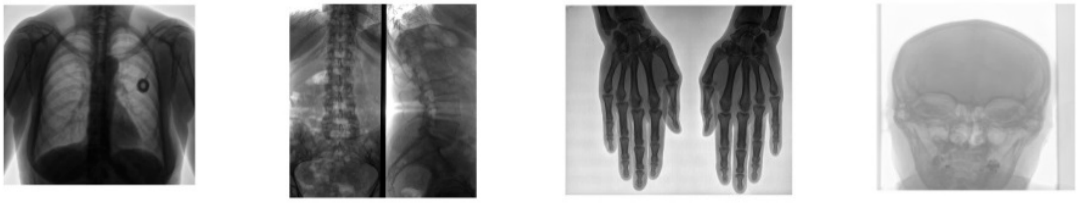

Figure 14. DICOM images used in experiments.

Figure 15 presents the watermark generated from the hands image.

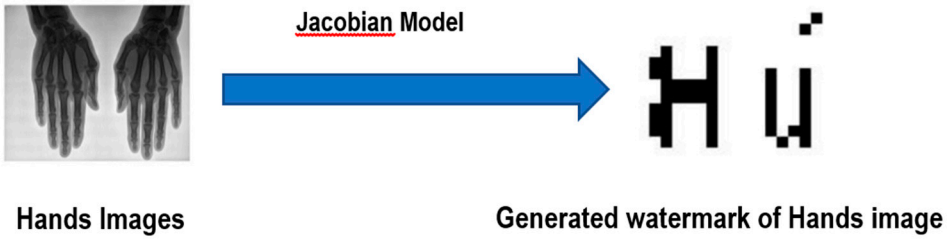

Figure 15. Hands image and generated watermark used in experiments.

5.2.1. Imperceptibility Analysis

Watermark's imperceptibility is evaluated by calculating PSNR and SSIM between original and watermarked images. Watermarked and original images should be very similar. Higher PSNR values indicate higher imperceptibility and less distortion. SSIM values should be close to 1 to indicate that there are no substantial distortions in the watermarked image in comparison to the original image.

Table 1 show that the PSNR values exceed 37 dB and all SSIM values are very close to the exemplary value 1. Figure 16 shows an example of the original image, corresponding generated watermark, watermark signed by a one-time ticket generated by the SUC, and the resulting clone –resistant WM image. To complete the signing process, AES-128 has been used as mentioned above. As one can see in this figure, there is no significant perceptual difference between original and Clone-Resistant Watermarked versions of the image.

Table 1. Structural similarity index (SSIM) and peak signal to noise ratio (PSNR) average values between watermarked and original images without attacks.

Image	SSIM	PSNR
Chest	0.9861	38.15
Tspine	0.9895	37.77
Hands	0.9997	49.52
Skull	0.9995	52.89

Figure 16. An example of the original image, corresponding generated and signed watermarks, and the resulting watermarked image.

We can see from Table 2 that the average value of SSIM between the original image and the attacked watermarked image is equal to 0.9823, and the average value of PSNR between the original image and the corresponding attacked watermarked image is equal to 53.45 dB which shows that the proposed watermarking approach ensures a good level of imperceptibility.

Table 2. SSIM and PSNR average values between watermarked and original images in case of attacks.

Attacks	Average SSIM	Average PSNR
Median filtering 2 × 2	0.9776	50.49
Median filtering 3 × 3	0.9748	54.80
Salt and pepper (0.01)	0.9820	50.69
Average filtering 3 × 3	0.9624	55.92
Cropping left top corner	0.9741	52.23
Gaussian filtering 3 × 3	0.9844	50.00
Histogram equalization	0.9874	50.15
Gaussian noise (0.01)	0.9779	53.72
Rotation 1°	0.9977	52.12
Rotation 5°	0.9906	49.99
Rotation 10°	0.9838	55.60
Sharpening	0.9854	57.25
Translate (10)	0.9782	52.85
Blurring	0.9847	57.69
Contrast Enhancement	0.9999	56.96
Scaling	0.9882	52.69
Wiener filtering	0.9707	55.58

5.2.2. Robustness Analysis

Robustness analysis is evaluated by calculating BER and NC. The BER is the number of bit errors divided by the total number of bits of the watermark. It is calculated to measure the similarity between the extracted attacked watermark and the original one. Lower BER expresses high robustness of watermarking against different attacks. The NC is used to indicate the similarity between original and extracted watermark, its value is between [1,−1]. When the NC= 1 the original and extracted watermarks are absolutely identical. When NC= 0 the original and extracted watermarks are divergent. When NC = −1 the original and extracted watermarks are completely anti-similar.

The watermark should be robust against attacks (the distortions due to attacks should remain minimal). In our experiments, we consider some geometric and non-geometric attacks. These attacks consist of median filtering, salt-and-pepper, average filter, Wiener filtering, cropping, contrast enhancement, scaling, Gaussian filtering, low pass filtering, histogram equalization, noise, rotation, sharpening, and translate attacks. Detailed results of BER and NC in an average for all images are summarized in Table 3.

We can see from Table 3 that the average values of NC between original and extracted watermarks are close to 1 except in one case, and the average values of BER between the original watermark and the extracted one are close to 0, which shows that the proposed scheme is robust against different processing attacks.

To demonstrate the effectiveness of the proposed method, comparisons with other works are presented in Tables 4 and 5.

From Table 4, we can see that our method has a better BER value for salt and pepper noise and noise attack (0.01) than the method of J. Dagadu et al. [18], while the method of J. Dagadu et al. [18] performs well than our method in the case of the cropping left top corner (25%) attack with a BER value equal to 0.

Table 3. NC and BER average values between the original and extracted attacked watermarks.

Attacks	Average BER	Average NC
Median filtering 2 × 2	0.0080	0.9494
Median filtering 3 × 3	0.0214	0.9427
Salt and pepper (0.01)	0.0333	0.9099
Average filtering 3 × 3	0.0203	0.9407
Cropping left top corner	0.0575	0.8445
Gaussian filtering 3 × 3	0.0172	0.9488
Histogram equalization	0.0918	0.4929
Gaussian noise (0.01)	0.0284	0.8980
Rotation 1°	0.0221	0.9881
Rotation 5°	0.0235	0.9260
Rotation 10°	0.0243	0.9226
Sharpening	0.0047	0.9852
Translate (10)	0.0202	0.9287
Blurring	0.0847	0.9904
Contrast Enhancement	0.0126	0.9530
Scaling	0.0112	0.9558
Wiener filtering	0.0536	0.9819

Table 4. Comparison of the average BER value of the proposed method with [18,21,22,40].

Attacks	Proposed Method	[18]	[40]	[21]	[22]
Cropping left top corner 25%	0.0575	0	-	0.0566	-
Noise attack (0.01)	0.0284	0.1418	-	-	-
Salt and pepper noise (0.01)	0.0333	0.4323	-	0.0175	-
Sharpening	0.0047	-	0.0180	0.0026	0
Histogram equalization	0.0918	-	0.0259	0.0080	-
Gaussian filter	0.0102	-	0.0117	-	-
Median filtering 2 × 2	0.0080	-	0.0027	0.0596	0.0383
Wiener filtering	0.0536	-	-	0.0488	0
Average filtering	0.0150	-	-	0.0654	-
Gaussian noise (0.0001)	0.0994	-	-	0.0800	-
Gaussian noise (0.01)	0.0284	-	-	-	0
Rotation 1°	0.0221	-	-	0.0259	-
Rotation 5°	0.0235	-	-	0.0283	-
Rotation 10°	0.0243	-	-	0.0330	0.0597
Blurring	0.0847	-	0.0738	-	-
Contrast Enhancement	0.0126	-	0.0131	-	-

Table 5. Comparison of the average NC value of the proposed method with [18,21,40,41].

Attacks	Proposed Method	[18]	[40]	[21]	[41]
Cropping left top corner 25%	0.8445	0.9997	-	1	0.9966
Noise attack (0.01)	0.9114	0.9589	-	-	-
Salt and pepper noise (0.01)	0.9099	0.9589	-	-	0.9758
Sharpening	0.9852	-	0.9018	0.9977	0.8898
Histogram equalization	0.4929	-	0.8556	0.9921	0.6038
Gaussian filter	0.9488	-	0.9322	-	-
Median filtering 2 × 2	0.9494	-	-	-	0.6973
Median filtering 3 × 3	0.9427	-	0.9845	0.9430	-
Wiener filtering	0.9819	-	-	0.9539	-
Average filtering	0.9407	-	-	0.9354	-
Gaussian noise (0.0001)	0.9856	-	-	0.9215	0.9979
Gaussian noise (0.01)	0.9114	-	-	-	0.9144
Rotation 1°	0.9881	-	-	0.9728	0.9460
Rotation 5°	0.9260	-	-	0.9695	-
Rotation 10°	0.9226	-	-	0.9653	-
Gaussian low pass filter	0.9488	-	-	-	0.5406
Image scaling ×1.1	0.9558	-	-	-	0.9309

Comparing our method with that of Chauhan et al. [40], one can see that our method is more robust in the case of sharpening, Gaussian filter, and contrast enhancement attacks. The results show that our method performs well for these three attacks as BER is close to 0. However, when we consider the histogram equalization attack, the method of Chauhan et al. [40] has a better BER value than ours.

The method of S.A. Parah et al. [21] is more robust than ours in the case of the cropping left top corner (25%), salt and pepper noise (0.01), sharpening, histogram equalization, Wiener filtering, and Gaussian noise (0.0001), but it is less robust than our method for the other attacks.

The method of Singh et al. [22] has been tested for only sharpening, median filtering 2×2, Wiener filtering, Gaussian noise (0.01), and rotation (10°). The average BER values of sharpening, Wiener filtering, and Gaussian noise are equal to 0. Therefore, this method is very robust and performs well with these three attacks while in the case of median filtering 2×2 our method is more robust.

A comparison of the proposed technique with [18,21,40,41] for average NC values is shown in Table 5. The comparison of the results with [18] proves that the technique proposed by Joshua Dagadu et al. [18] is more robust than ours in the case of cropping, salt and pepper noise, and noise attacks but in [18] the other attacks were not tested. Comparing our results with [40], our NC values between the original watermark and the extracted watermark in the case of sharpening and Gaussian filtering are better than the results of [40].

By comparing our NC values with the NC values of [21], one can see that in the case of average filtering and rotation (1°) our method is more robust than the method of [21]. While in the case of the other attacks such as cropping left top corner, sharpening, histogram equalization, median filtering, rotation (5°) and rotation (10°), the method of S.A. Parah et al. [21] is more robust than our method but there is no big difference. Comparing the results of our method with the method of S.Thakur et al. [41] in terms of NC, we can see that the results obtained after applying sharpening, median filtering 2×2, rotation (1°), Gaussian low-pass filter, and image scaling $\times 1.1$ attacks to the watermarked image are better with our method while in the case of attacks such as cropping, salt and pepper, histogram equalization, the method in [41] is more robust than ours.

The experimental results of our method show that after all attacks the extracted watermarks are visually recognizable and all extracted watermarks are similar to the original watermark. The average NC value is equal to 0.9055 which is a good ratio, the BER value on average is equal to 0.0374, the SSIM on average is equal to 0.9823, and the PSNR on average is equal to 53.45 dB. Therefore, our method is robust against different attacks.

6. Conclusions

In this paper, we have proposed a clone-resistant watermarking approach for telemedicine applications. Our scheme extracts the patient name and pertinent features from the original image to generate a watermark using the Jacobian model. A one-time ticket is extracted from the Secret Unknown Ciphers (SUCs) of the medical device to sign the watermark in order to generate a one-time watermark signature. The signed watermark is then embedded in the medical image of the patient using a reversible watermarking technique (Difference Expansion).

By combining watermarking and SUC, the proposed approach offers several advantages: Resistance to cloning, confidentiality, authentication, non-repudiation, and integrity of the medical image. Moreover, the reversibility of the watermarking technique used in the proposed approach makes it possible to recover not only the watermark but also the original image. Such recovering of the original image is a critical requirement for medical image applications.

Experimentation results show that the proposed scheme is robust against watermarking attacks (geometric and non-geometric) and provides good bases to withstand other security attacks such as the man in the middle and tampering attacks.

Author Contributions: Conceptualization, S.M., M.T., L.N. and W.A.; methodology, M.T. and S.M.; software, M.T. and S.M.; supervision, A.P., L.N., F.B. and W.A.; validation, L.N., S.M. and A.P.; formal analysis, S.M. and M.T.; visualization, W.A.; writing—original draft preparation, S.M. and M.T.; writing—review and editing, L.N. and W.A.; project administration, W.A. and L.N. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the DAAD Research Grants Doctoral Programs in Germany, under grant number 57214224 and the German Federal Foreign Office scholarship funding (STIBET) program and indirectly by Microsemi, a Microchip Company, San Jose, CA, USA and Volkswagen AG—Germany. A support was also provided by the MathSTIC Doctoral school of Université de Bretagne Loire in France.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Universal Declaration of Human Rights | United Nations. Available online: https://www.un.org/en/universal-declaration-human-rights/index.html (accessed on 8 January 2020).
2. Kobayashi, L.O.M.; Furuie, S.S.; Barreto, P.S.L.M. Providing integrity and authenticity in DICOM images: A novel approach. *Proc. IEEE Trans. Inf. Technol. Biomed.* **2009**, *13*, 582–589. [CrossRef] [PubMed]
3. Sittig, D.F.; Wright, A.; Coiera, E.; Magrabi, F.; Ratwani, R.; Bates, D.W.; Singh, H. Current challenges in health information technology-related patient safety. *Health Inform. J.* **2018**, *26*, 181–189. [CrossRef] [PubMed]
4. Coatrieux, G.; Maître, H.; Sankur, B.; Rolland, Y.; Collorec, R. Relevance of watermarking in medical imaging. In Proceedings of the IEEE/EMBS Region 8 International Conference on Information Technology Applications in Biomedicine, ITAB, Arlington, VA, USA, 9–10 November 2000; IEEE: Piscataway, NJ, USA, 2000; pp. 250–255.
5. Bhunia, S.; Tehranipoor, M. Hardware Security Primitives. In *Hardware Security*; Elsevier: Amsterdam, The Netherlands, 2019; pp. 311–345.
6. Tu, Y.S.; Chen, J. A secure and unclonable medical image transmission system by using embedded physical uncloneable function. In Proceedings of the 2016 International Conference on Communication Problem-Solving, ICCP, Taipei, Taiwan, 7–9 September 2016; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2016.
7. Delvaux, J.; Peeters, R.; Gu, D.; Verbauwhede, I. A Survey on Lightweight Entity Authentication with Strong PUFs. *ACM Comput. Surv.* **2015**, *48*, 1–42. [CrossRef]
8. Adi, W.; Ouertani, N.; Hanoun, A.; Soudan, B. Deploying FPGA self-configurable cell structure for micro crypto-functions. In Proceedings of the 2009 IEEE Symposium on Computers and Communications, Sousse, Tunisia, 5–8 July 2009; IEEE: Piscataway, NJ, USA, 2009; pp. 348–354.
9. Adi, W. Clone-Resistant DNA-Like Secured Dynamic Identity. In Proceedings of the 2008 Bio-Inspired, Learning and Intelligent Systems for Security, Edinburgh, UK, 4–6 August 2008; IEEE: Piscataway, NJ, USA, 2008; pp. 148–153.
10. Ghadi, M.; Laouamer, L.; Nana, L.; Pascu, A. A novel zero-watermarking approach of medical images based on Jacobian matrix model. *Secur. Commun. Netw.* **2016**, *9*, 5203–5218. [CrossRef]
11. Van Schyndel, R.G.; Tirkel, A.Z.; Osborne, C.F. A digital watermark. In Proceedings of the International Conference on Image Processing, ICIP, Austin, TX, USA, 13–16 November 1994; IEEE Computer Society: Piscataway, NJ, USA, 1994; Volume 2, pp. 86–90.
12. Chao, H.M.; Hsu, C.M.; Miaou, S.G. A data-hiding technique with authentication, integration, and confidentiality for electronic patient records. *IEEE Trans. Inf. Technol. Biomed.* **2002**, *6*, 46–53. [CrossRef]
13. Nyeem, H.; Boles, W.; Boyd, C. A review of medical image watermarking requirements for teleradiology. *J. Digit. Imaging* **2013**, *26*, 326–343. [CrossRef]
14. Coatrieux, G.; Lecornu, L.; Sankur, B.; Roux, C. A review of image watermarking applications in healthcare. In Proceedings of the Annual International Conference of the IEEE Engineering in Medicine and Biology, New York, NY, USA, 30 August–3 September 2006; IEEE: Piscataway, NJ, USA, 2006; pp. 4691–4694.
15. Memon, N.A.; Keerio, Z.A.; Abbasi, F. Dual watermarking of CT scan medical images for content authentication and copyright protection. *Commun. Comput. Inf. Sci.* **2013**, *414*, 173–183. [CrossRef]
16. Bouslimi, D.; Coatrieux, G. A crypto-watermarking system for ensuring reliability control and traceability of medical images. *Signal Process. Image Commun.* **2016**, *47*, 160–169. [CrossRef]

17. Metkar, S.P.; Lichade, M.V. Digital image security improvement by integrating watermarking and encryption technique. In Proceedings of the 2013 IEEE International Conference on Signal Processing, Computing and Control, ISPCC 2013, Shimla, India, 26–28 September 2013; IEEE: Piscataway, NJ, USA, 2013.
18. Dagadu, J.C.; Li, J. Context-based watermarking cum chaotic encryption for medical images in telemedicine applications. *Multimed. Tools Appl.* **2018**, *77*, 24289–24312. [CrossRef]
19. Bouslimi, D.; Coatrieux, G.; Cozic, M.; Roux, C. Combination of watermarking and joint watermarking-decryption for reliability control and traceability of medical images. In Proceedings of the 2014 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, EMBC, Chicago, IL, USA, 26–30 August 2014; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2014; pp. 4495–4498.
20. AlShaikh, M.; Laouamer, L.; Nana, L.; Pascu, A.C. Efficient and robust encryption and watermarking technique based on a new chaotic map approach. *Multimed. Tools Appl.* **2017**, *76*, 8937–8950. [CrossRef]
21. Parah, S.A.; Sheikh, J.A.; Ahad, F.; Loan, N.A.; Bhat, G.M. Information hiding in medical images: A robust medical image watermarking system for E-healthcare. *Multimed. Tools Appl.* **2017**, *76*, 10599–10633. [CrossRef]
22. Singh, A.; Dutta, M.K. A robust zero-watermarking scheme for tele-ophthalmological applications. *J. King Saud Univ.–Comput. Inf. Sci.* **2017**. [CrossRef]
23. Bouslimi, D.; Coatrieux, G.; Roux, C. A joint encryption/watermarking algorithm for verifying the reliability of medical images: Application to echographic images. *Comput. Methods Programs Biomed.* **2012**, *106*, 47–54. [CrossRef] [PubMed]
24. Chaduvula, S.C.; Dachowicz, A.; Atallah, M.J.; Panchal, J.H. Security in cyber-enabled design and manufacturing: A survey. *J. Comput. Inf. Sci. Eng.* **2018**, *18*. [CrossRef]
25. Zimmermann, P. *PGP User's Guide*; MIT Press: Cambridge, MA, USA, 1991.
26. Gassend, B.L.P. Physical Random Functions. Ph.D. Thesis, Massachusetts Institute of Technology, Cambridge, MA, USA, 2003.
27. Marchand, C.; Bossuet, L.; Mureddu, U.; Bochard, N.; Cherkaoui, A.; Fischer, V. Implementation and Characterization of a Physical Unclonable Function for IoT: A Case Study With the TERO-PUF. *IEEE Trans. Comput. Des. Integr. Circuits Syst.* **2018**, *37*, 97–109. [CrossRef]
28. Lim, D.; Lee, J.W.; Gassend, B.; Suh, G.E.; van Dijk, M.; Devadas, S. Extracting secret keys from integrated circuits. *IEEE Trans. Very Large Scale Integr. Syst.* **2005**, *13*, 1200–1205. [CrossRef]
29. Gołofit, K.; Wieczorek, P. Chaos-Based Physical Unclonable Functions. *Appl. Sci.* **2019**, *9*, 991. [CrossRef]
30. Adi, W.; Zeitouni, S.; Huang, X.; Fyrbiak, M.; Kison, C.; Jeske, M.; Alnahhas, Z. IP-core protection for a non-volatile Self-reconfiguring SoC environment. In Proceedings of the 2013 IFIP/IEEE 21st International Conference on Very Large Scale Integration (VLSI-SoC), Istanbul, Turkey, 6–9 October 2013; IEEE: Piscataway, NJ, USA, 2013; pp. 252–255.
31. Mulhem, S.; Adi, W. New Mathblocks-Based Feistel-Like Ciphers for Creating Clone-Resistant FPGA Devices. *Cryptography* **2019**, *3*, 28. [CrossRef]
32. Mulhem, S.; Mars, A.; Adi, W. Low-Complexity Nonlinear Self-Inverse Permutation for Physically Clone-Resistant Identities. *Cryptography* **2019**, *4*, 6. [CrossRef]
33. Adi, W.; Soudan, B. Bio-Inspired Electronic-Mutation with genetic properties for Secured Identification. In Proceedings of the ECSIS Symposium on Bio-inspired, Learning, and Intelligent Systems for Security, Edunburgh, UK, 9–10 August 2007; IEEE: Piscataway, NJ, USA, 2007; pp. 133–136.
34. Mulhem, S.; Mohammad, M.; Adi, W. A New Low-Complexity Cipher Class for Clone-Resistant Identities. In Proceedings of the 2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 20–24 May 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 971–976.
35. Fekri-Ershad, S. A Review on Image Texture Analysis Methods. *arXiv* **2018**, arXiv:1804.00494.
36. Bellare, M.; Rogaway, P. Introduction to Modern Cryptography. 2005. Available online: http://almuhammadi.com/sultan/crypto_books/BR.2005.pdf (accessed on 3 July 2020).
37. Mulhem, S.; Zarrouk, R.; Adi, W. Security and Complexity Bounds of SUC-Based Physical Identity. In Proceedings of the 2018 NASA/ESA Conference on Adaptive Hardware and Systems (AHS), Edinburgh, UK, 6–9 August 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 317–322.

38. Mishra, M.; Adhikary, M.C. Detection of Clones in Digital Images. *Int. J. Comput. Sci. Bus. Inform.* **2014**, *9*, 91–102.
39. Goldreich, O.; Goldwasser, S.; Micali, S. How to construct random functions. *J. ACM* **1986**, *33*, 792–807. [CrossRef]
40. Chauhan, D.S.; Singh, A.K.; Kumar, B.; Saini, J.P. Quantization based multiple medical information watermarking for secure e-health. *Multimed. Tools Appl.* **2019**, *78*, 3911–3923. [CrossRef]
41. Thakur, S.; Singh, A.K.; Ghrera, S.P.; Elhoseny, M. Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications. *Multimed. Tools Appl.* **2019**, *78*, 3457–3470. [CrossRef]