# A Novel Privacy Technique for Augmented Reality Cloud Gaming Based on Image Authentication

Rahma Gharsallaoui
SupCom, University of Carthage
Tunis, Tunisia
rahma.gharsallaoui@supcom.tn

Mohamed Hamdi
SupCom, University of Carthage
Tunis, Tunisia
mmh@supcom.tn

Tai-Hoon Kim
Dept. of Convergence Security,
Sungshin W. University
South Korea
taihoonn@daum.net

***Abstract*—The evolution of cloud gaming systems is substantially the security requirements for computer games. Although online game development often utilizes artificial intelligence and human computer interaction, game developers and providers often do not pay much attention to security techniques. In cloud gaming, location-based games are augmented reality games which take the original principals of the game and applies them to the real world. In other terms, it uses the real world to impact the game experience. Because the execution of such games is distributed in cloud computing, users cannot be certain where their input and output data are managed. This introduces the possibility to input incorrect data in the exchange between the gamer's terminal and the gaming platform. In this context, we propose a new gaming concept for augmented reality and location-based games in order to solve the aforementioned cheating scenario problem. The merit of our approach is to establish an accurate and verifiable proof that the gamer reached the goal or found the target. The major novelty in our method is that it allows the gamer to submit an authenticated proof related to the game result without altering the privacy of positioning data.**

## I. Introduction

As being substantial in the emerging cloud computing systems, video gaming systems are becaming more mature. With the availability of different platforms that range from personal computers and consoles to handheld devices, smartphones and tablets, the number of people that play games around the world have made the gaming industry one of the fastest growing industries on the planet. Its popularity and market size makes game platforms and individual users ideal targets for cybercriminals who see it as an attractive platform for stealing user information, invading privacy, or spreading malicious content and malware. As such, gamers must be aware of the privacy risks, especially when a majority of the popular games these days have either an online component or a pay-as-you-play business model where in-game items and add-ons can be bought. In this paper, we develop a new privacy solution to thwart the attacks that can be conducted against multimedia transmissions systems. The rest of the paper is organized as follows. Section II reviews the related work work to the context of online gaming. Section III introduces security issues and requirements in augmented reality (AR) games considering Pokemon Go as a case study. Section IV describes the image authentication fundamentals. The architecture of our new privacy technique is introduced in Section V. Finally, Section VI concludes the paper.

## II. Related Works

A.S. Douglas [1], a graduate student at the University of Cambridge, created the very first computer game a modified version of Tic-Tac-Toe [2]. Douglas creation was rudimentary by today's standards, but it generated a significant amount of interest. For instance, during the last decades, the use of online gaming platforms has dramatically increased, and the entertainment value of computer games was improved. Many research in this area are done. However, many security issues are still overseen. Online multiplayer games require a number of human players communicating over computer networks. So, cheating players harm human players instead of computer players; with most traditional games that is characterized as single-palyer games in which computer player utilizes artificial intelligence. So, cheating players only place the computer player as a disadvantage. Cheating can be defined as any action taken by a player to obtain an unfair advantage over the other players. Cheaters inducement can be classified in three types. The first one is the desire to ruin others online experiences, as Pritchard states in[3]. The second motivation is the feeling of victory. In fact, many cheaters want to win without practicing as much as ligitimately good players. So, they win by cheating rather that by skill. Finally, the last motivation is money. For example, the Ultimate Online [4] and EverQuest [5] has result in the auctioning of virtual characters and assets on eBay [6].

## III. Existing Augmented Reality Games: The Pokemon Go Case

Augmented Reality allows to combine the real scene viewed by a user and a virtual scene generated by computer that augments the scene with additional information. AR will truly change the way we view the world. The ultimate goal of AR is to guarantee that a user cannot recognize the difference between the real world and the virtual augmentation of it. There are many Augmented Reality games. Pokemon Go is the most popular nd newest one. Ingress [7], is the first augmented reality game that relies on GPS location and is one of the most similar games like Pokmon GO. Its goal is to hack portals and build them up after choosing one of the teams to fight against the other side. The 3D AUgmented Reality FPS was called Real Strike [8]. It was developed by Yii International. This game combines the real-life with 3D gun animation. It's one of those very few apps like Pokemon Go which lets the

978-1-5090-4372-9/17/$31.00 ©2017 IEEE

experience the full power of augmented reality. Life is Crime [9], is based more real-like concept of criminals. It's different from Ingress or Pokemon Go. In playing Life is Crime, player can join gangs of their choice and can have live chats with follow player.

### A. Security Issues and Requirements

*1) Ability Augmentation:* Cheating in online games not only affects the game-play and the enjoyment of non-cheating players but also the quality of service [14] that the game developer provides. In the case of First Person Shooters (FPS) who possess quick reflexes and great eye-hand coordination. Thus, cheaters often turn to various unfair techniques to augment their abilities in games so that they can compete on the same level as legitimately good players. These techniques are:

1) Aim Hack:In FPS, the most important aspect of this process is the focus of the target because a shot to another player s head is much more lethal than a shot to the arm or leg. In fact, cheaters desire accurate aiming abilities, but they don't want to spend time practicing. As a result, they use an aim hack (also known as auto-aim or aimbot) to attain aiming skills.
   - The first aim hack acts as a proxy between the cheater s game and the gaming server (When the cheater attempts to fire at another player, the aiming proxy inserts additional game commands to ensure the cheater is aiming directly at the nearest opposing player )
   - The second aim hack is actually added to the game, but it provides the same type of functionality as the aiming proxy. However, the second aim hack can be configured to move the cheater s crosshairs and fire automatically
2) Speed Hack: In order to successfully avoid being targeted in these games, cheaters often employ a speed hack which increases the rate at which they can move in the game [14]. The logic behind this cheat is simple: the faster the target moves, the harder it is to shoot.
3) Anti-grenade Hack: cheaters utilize an anti-grenade hack to remove the visual impairment from the screen. Consequently, this cheat makes the cheaters immune to flashbangs, smoke grenades, and various other items that serve to impair the abilities of legitimate players.

*2) Knowledge of Classified Information:*

1) Map Hack: For the Real Time Strategy games (RTS), if a section of the world has not been explored by the player, it is covered by the fog of war. Thus, cheaters employ a map hack which removes the fog of war regardless of whether or not the cheater has explored the entire map.
2) Wall Hack: This technique is more useful in a FPS games. In fact, players are surrounded by various obstacles; if players are hiding behind obstacles, they should not be visible to other players. Games show a player's field of vision by drawing each scene from back to front. A cheater is able to exploit this situation by using a wall hack which draws the obstacles transparently. Thus, players that are hiding behind obstacles are no longer hidden because the obstacles appear to be transparent [11]

### B. Analyse of game concept for Pokemon Go

As a real world adventure, the game uses GPS and augmented reality and is perhaps the most widely played augmented reality game to date. It uses a smartphones GPS location and real-world maps to track players as they move around in search of Pokmons and encourages them to explore their neighbourhood and surrounding areas in order to catch the target. To play the Pokmon Go game you need an account. Niantic wont let you just create one - you need to sign in with an existing account from one of two services - the pokemon.com website or Google. When you grant full account access, the application can see and modify nearly all information in your Google Account . This Full account access privilege should only be granted to applications you fully trust, and which are installed on your personal computer, phone, or tablet.In order to play, the app needs to know your location through your devices GPS and access the camera. We aim to propose new gaming concept for augmented reality (AR) and location-based games in order to establish an accurate an verifiable proof of goal achievement.

## IV. Image Authentication Fundamentals

### A. Image Authentication Requirements

Image authentication is used to verify or validate whether an image is authentic. It provides an agreement that there is no change to the original image and the test image. In the aim to compress an image in order to save memory space or bandwidth to enhance an image and restore it for better perceptual quality or even to convert its format. In this context, the general requirements that are essential for any authentication system are [12]:

- Sensitivity: The authentication system must be able to detect any content modification or manipulation. For strict authentication algorithms, detection of any manipulation is required and not only content modification.
- Robustness: Also called tolerance. The authentication system must tolerate content preserving manipulations. This property is valid just for algorithms that provide a selective authentication service.
- Localization: The authentication system must be able to locate the image regions that have been altered.
- Recovery: The authentication system must be able to partially or completely restore the image regions that were tampered.
- Security: The authentication system must have the capacity to protect the authentication data against any falsification attempts.
- Portability: The authentication system must be able to carry the signature with the protected image during any transmission, storage or processing operation.

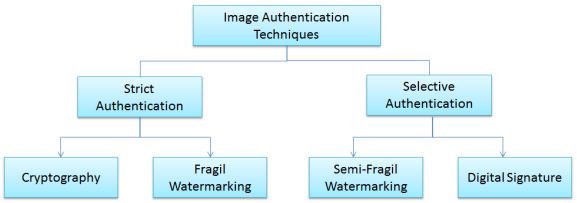


Fig. 1: Classification for Image Authentication


Fig. 2: Strict authentication system by conventional cryptography; generation of authentication Code

- Complexity: The authentication system must use real-time implemented algorithms that are neither complex nor slow.

### B. Classification for Image Authentication

In order to secure an image, it passes through an image authentication technique such as watermarking, hashing etc. It is then processed through a non-secure media or communicated to the receiver. At the receiver, sequence generated by image authentication technique is restored and computed to compare if it matches the original. If there is a match then the image is authentic else not. Image authentication has obtained significance because many areas in science and literature are using images for diagnosis, proof of identity, entertainment etc. There are many image authentication techniques as described in Figure 1. Image authentication is classified into strict and selective authentication. In strict authentication, even if a single image pixel or bit is changed the image is considered as non-authentic. Usually it is rarely used in practical scenarios. In selective authentication, when the protected image needs to be robust to some image processing operation such as geometric transformation, filtering, compression etc the exact pixel match is not encouraged.

*1) Strict image authentication techniques:* Strict image authentication methods do not tolerate any changes in the image data. These methods can be further separated in two groups according to the techniques that are used: methods based on conventional cryptography and methods that use fragile watermarking.

*a) Conventional Cryptography:* It is an image authentication method that amounts to compute a message authentication code (MAC) from the image using hash function [12]. The hash (h) is encrypted with a secret private key $S$ of the sender and then attached to the image. The hash can be encrypted using public key $K1$ to more secure exchange of data. At the server side, the hash is extracted and decrypted using private key $K1$. In fact, the two hashes are compared to check the validity. If any change in the hashes is found, the image is declared manimulated otherwise it is declared authentic.

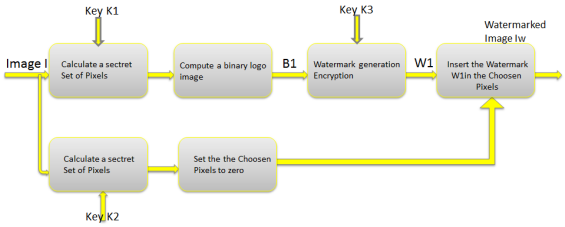


Fig. 3: Strict authentication system by fragile watermarking using image information

*b) Fragile Watermarking:* Watermarking is a technique by which a watermark is computed and hidden in the image. This watermark is computed from a set of image pixels that can be chosen with the help of secret key $K1$. It is then encrypted with a key $K3$. Also, the set of pixels where the watermark is attached can be determined with another secret $K2$ [12].

*2) Selective image authentication ( Content-based ):* There are many application that their decisions are based on image authentication methods. It can tolerate content preserving manipulations. For that, there are new watermarking method called semi-fragil watermarking, and new approaches known as content-based signatures.

*a) Semi-Fragile Watermarking:* It is an image authentication method that consist on inserting a watermark in the original image. The procedures of generating a watermark and attaching it to the image can be dependent on a private or public key system. . This is an exchange between security and computational time [12].

*b) Digital signatures:* Most recent investigations in the domain of image authentication were concentrated on digital signatures applied to the image content. Image authentication systems that use a digital signature based on the semantic content of images consist in extracting specific high level characteristics from the original image; applying a hash function to these characteristics in order to reduce their size; digitally signing the hash value using an existing digital signature algorithm such as a private or public key system to increase the overall security; attaching the signature to the original image or inserting it in the image using techniques for data dissimulation [12]. In order to verify the image authenticity, image signature is generated using the same algorithm; extract the attached signature. Then, compare two signatures using a comparison algorithm to decide whether the image was altered or not, and determine the image regions that were manipulated. When the image is declared as not authentic, information from the original signature could be used to partially or even completely restore the regions that were corrupted.

## V. Architecture of the Proposed Augmented Reality Approach

In cloud computing infrastructure, bandwidth, memory and power consumption are a big concern as they directly impact the cloud services performances. Consequently, the selection

of image authentication techniques for security support must be accurately done. the growing need for guaranteeing input correct data in the exchange between the gamer's terminal and the gaming platform, lead us to define a new cloud gaming concept based on image authentication. The architecture of the proposed privacy solution is given in Figure 4. It presents a description of our new gaming concept for augmented reality (AR) and location-based games. The main focus of this approach is to establish an accurate proof that the gamer reach the goal. The new features compared to existing schemes is the use of authenticated image streams. In fact, the gamer can verify the proof in a location-based game without sharing private information. We used the digital signature as a selective image authentication technique. In other terms, image streams authentication is used as a content-based techniques. With our new gaming concept, the game application does not need to know location information through GPS device. But, as a real world games, it uses mobile augmented reality (AR). This refers to the concept of overlaying media (eg. graphics, photos, videos, ...) from the environment into a portable device such as an iPad or Smartphone.

## VI. Implementation

Figure 5 describes the implementation of the proposed Image Authentication System. In fact, the system extracts specific characteristics from the original image $I$ . These characteristics are denoted by $C$ where:

$$C = F_e(I). \tag{1}$$

In order to reduce the size of the characteristics, we apply a Hash function on these high level features. Therefore, we obtain $H$ which is equal to:

$$H = F_h(C) \tag{2}$$

Then, the hash value is digitally signed so as to obtain the image signature noted $S_O$ which is attached to the original image $I$.

We give in Figure 6 the implementation of the image authenticity verification process. The system extracts specific characteristics from the received image $I_R$. These characteristics are denoted by $C_R$.

$$C_R = F_e(I_R) \tag{3}$$

In order to reduce the size of the characteristics, we apply a Hash function on these high level features to obtain $H_R$ :

$$H_R = F_h(C_R) \tag{4}$$

Then, the hash value is digitally signed with the same digital signature algorithm such as the same private key system. Finally, we obtain the image signature noted $S_R$ which is attached to the received image $I_R$. After that, we compare the two signatures using a matching algorithm to decide whether the image was altered or not.

## VII. Conclusion

As online games continue to grow in popularity, the ability to establish new solution in order to prevent cheating become important. This paper describes a new privacy solution for cloud gaming. It explored the security issues in augmented reality games. Then, the concept of Pokemon Go online game was analysed. Additionally, we present the image authentication requirements and techniques. We also describe the privacy solution architecture for location based games. The objective of future work is to make the performance analysis for our new gaming concept dedicated to Augmented Reality games.

## References


[1] *http://history-computer.com/ModernComputer/Software/OXOgame.html*
[2] M. Bellis, *The History of Computer and Video Games*, library 'inventors', 2003.
[3] D. Becker, *Online gaming s cheating heart*, CNET News.com, 7 June 2002.
[4] Ultima Online website *http://www.uo.com*.
[5] EverQuest website, *http://everquest.station.sony.com*.
[6] eBay website *http://www.ebay.com*.
[7] *https://www.ingress.com/*.
[8] *https://play.google.com/store/apps/details?id=info.yii.realstrikehl=fr*.
[9] *http://redrobot.com/games/life-is-crime/*.
[10] *http://www.thewalkgame.com/*.
[11] Derroll David and Divya, *Image Authentication Techniques and Advances Survey*, An international journal of advanced computer technology, April-2015 (Volume-IV, Issue-IV).
[12] A.Haouzia and R.Noumeir, *Methods for image authentication: a survey*, PublishedMultimed Tools Appl (2008).
[13] A. Moses,*Cheating Multiplayer Gaming s Achilles Heel?*.
[14] Steve Webb,*A Survey of Cheating Techniques in Online Games*, Mini-Project$_3 Cheating in Online Games$, 2003.

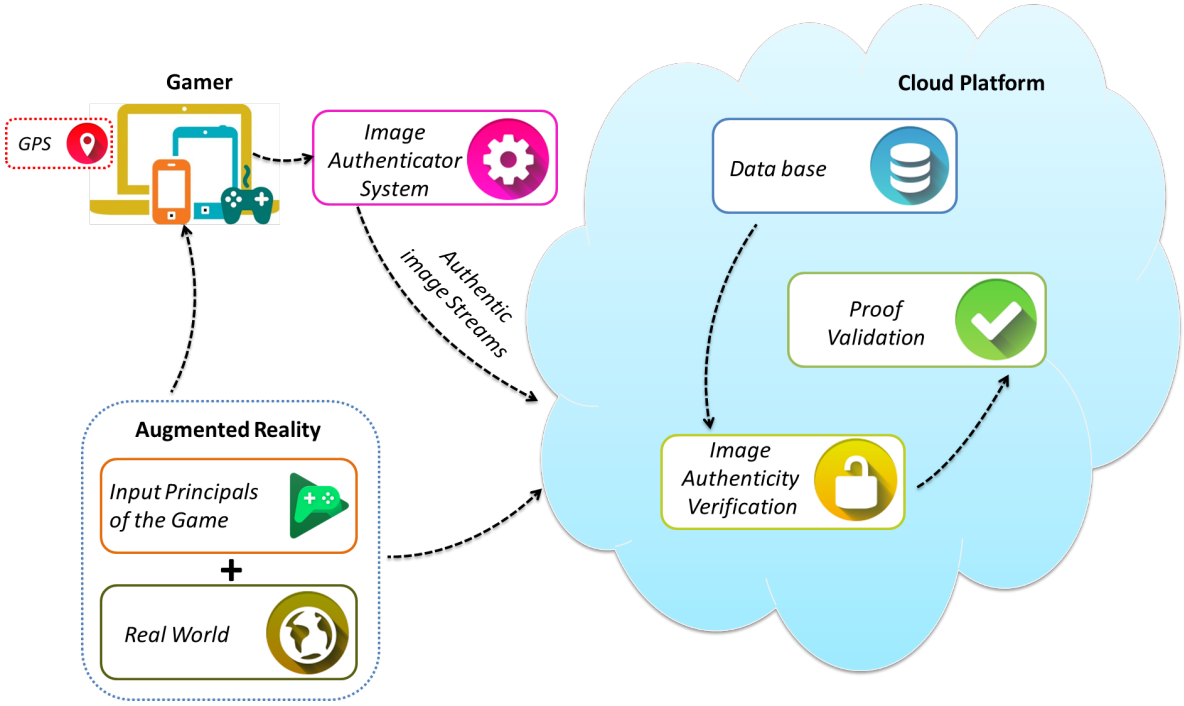


Fig. 4: Privacy solution for Augmented Reality and location based Gaming

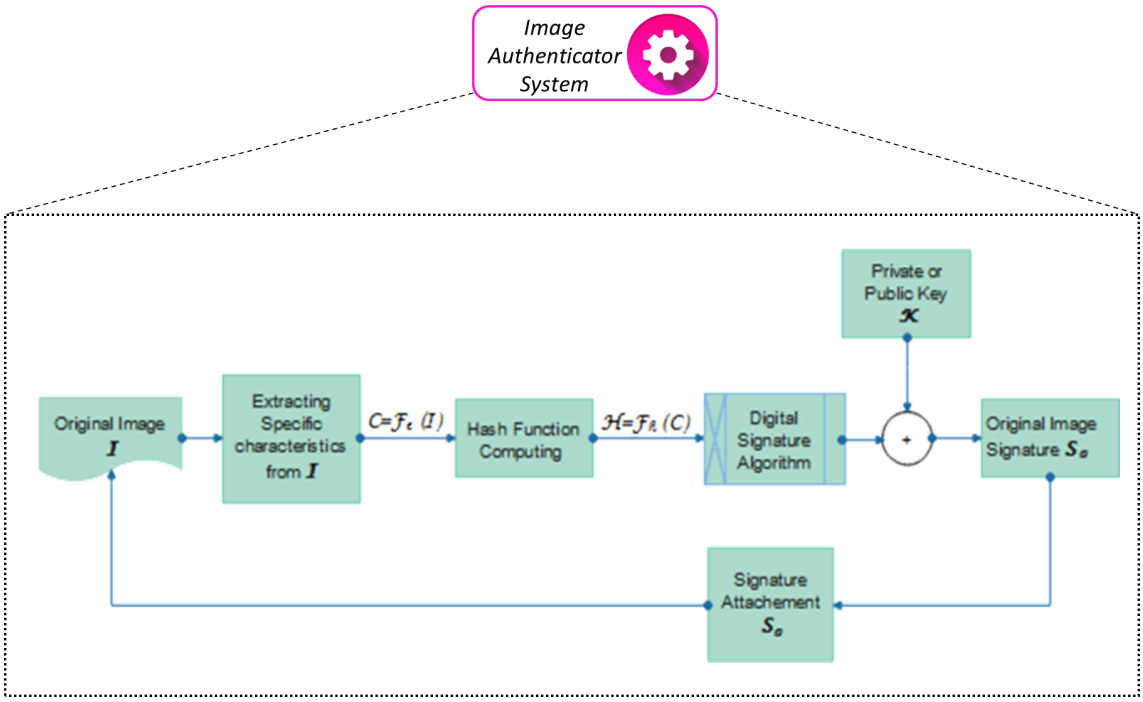


Fig. 5: Image Authentication System

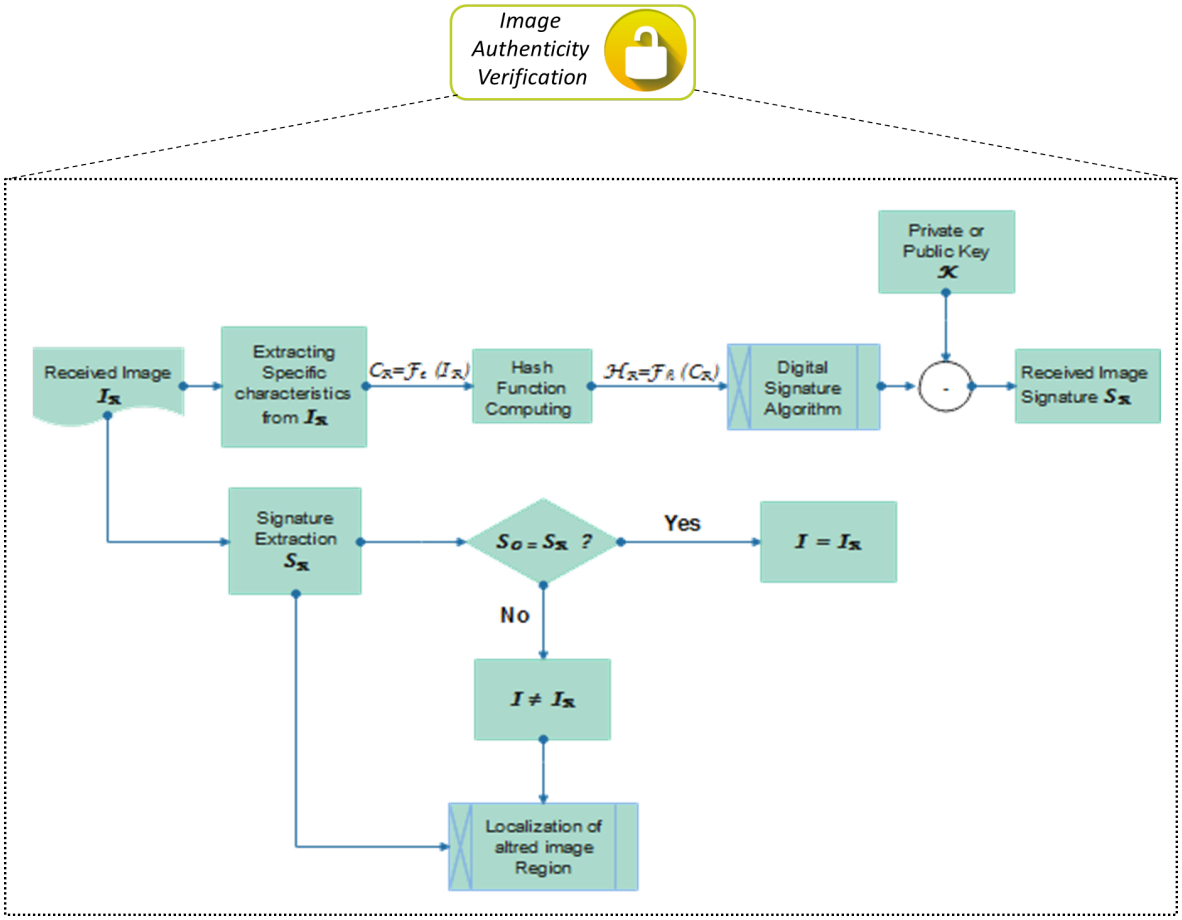


Fig. 6: Image Authenticity Verification