New Zero Watermarking Scheme Based on Hyper-catadioptric System Model and Hyperbolic Geometry

Boureima Koussoube[1(✉)], Moustapha Bikienga[2], Telesphore Tiendrebeogo[1], Kodjo Atiampo Armand[3], and Boureima Zerbo[4]

[1] Nazi BONI University, Bobo-Dioulasso, Burkina Faso
koussoubebrm@gmail.com
[2] Norbert ZONGO University, Koudougou, Burkina Faso
[3] Virtual University, Abidjan, Ivory Coast
armand.atiampo@uvci.edu.ci
[4] Thomas SANKARA University, Saaba, Burkina Faso

Abstract. In this paper we propose a new digital watermarking scheme for securing DICOM images in a distributed database. This new technique introduces no distortion to the images and will serve as a means of authenticating them. The database has a hyperbolic structure and its model is based on the Poincaré disk model, in which a hyperbolic tree is built. The coordinates of the tree nodes represent the virtual coordinates of the virtual servers. We assimilate the database structure to the image plane of a hyper-catadioptric system model. The image will be placed in a Euclidean space. Points will then be selected and computed according to the projection model of the hyper-catadioptric system. The set of image points computed constitutes our cryptographic signature. Each image point will be associated with the nearest node, and each server node will store image points and a model parameter, the plane equation and one of its public keys. Using its private key, the receiver can determine the image points and the various parameters to calculate the inverse transform of each image point for comparison. Formal analysis and simulations show that our approach is robust.

Keywords: Zero watermarking scheme · Hyper-catadioptric system model · Hyperbolic tree · Cryptographic signature

1 Introduction

The expansion of new information and communication technologies is making itself felt in the field of medical imaging. It is no longer limited to the production of medical images, but also to the manipulation, storage and transfer of images associated with some information. Since these images and information are transmitted over unsecured networks, it is essential to find safe ways of protecting

A. Sere et al. (Eds.): AFRICOMM 2023, LNICST 588, pp. 220–233, 2025.
https://doi.org/10.1007/978-3-031-81573-7_18

them, given their sensitive nature. Indeed, an altered image can cause a diagnostic or even therapeutic error. The information associated with these images must be protected in order to preserve medical confidentiality. Cryptography, which is generally used to secure documents on unsecured networks, is proving ineffective. Cryptography uses a secret key to encrypt a message and transfer it to a receiver. The receiver also uses a key to decrypt the message. The problem with cryptography is that it offers protection only at the point of transfer (a priori protection). To perpetuate this protection, digital watermarking is used as a complement to cryptography. The aim of watermarking is to conceal information (mark or watermark) in an image. Several watermarking techniques have been proposed in the literature [1–3].

These techniques are adapted to specific use cases and document types. To our knowledge, there is no universal watermarking scheme that adapts to any situation. In our context, our scheme must be adapted to a distributed database with a hyperbolic structure [6]. The hyperbolic structure is represented by a Poincaré disk in which a hyperbolic tree is constructed. Our approach aims to select pixels from a DICOM image and map them to server nodes in the database. To achieve this, we will adapt the structure of the given database to the image plane of the hyper-catadioptric system model. The advantage of this approach is that the schema introduces no distortion and is unpredictable. The approach must also be robust to compression and attack attacks.

Our article is structured as follows: first, we give an overview of image protection and present a database. Next, we study our hypercatadioptric model before proposing our new watermarking scheme. Moreover, we analyze our approach. We end with a conclusion and some perceptive remarks.

2 Image Protection

2.1 Image Encryption

Cryptography is the method used to secure exchanges in applications. It involves encrypting a document using a key, then transferring it to a recipient. The receiver uses a key to decrypt the document (Fig. 1).

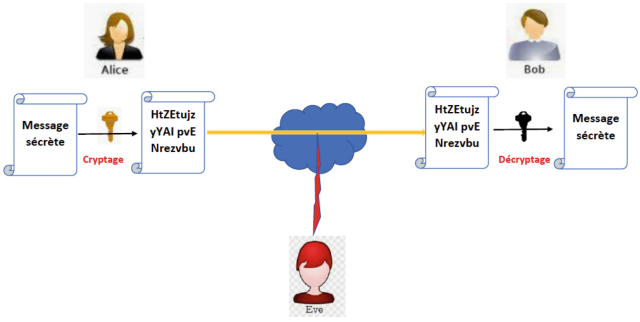


Fig. 1. Cryptography

Several techniques have been proposed in the literature for encrypting images [4,5]. These methods are not very effective. In fact, they provide a priori security, i.e. during transfer between sender and receiver. Once the image has been received and decrypted by the receiver, it is no longer protected.

2.2 Image Watermarking

Watermarking techniques are then used in association with cryptography to provide lasting protection. Image watermarking is a technique for visibly or invisibly inserting information (watermark) into an image (host). Digital watermarking uses a secret key for insertion and detection according to Fig. 2.

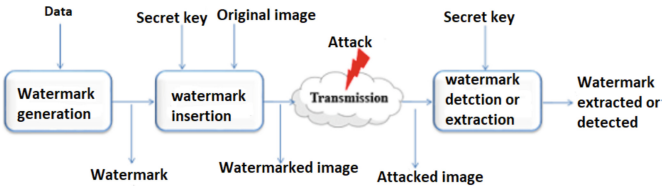


Fig. 2. watermarking process

Several watermarking algorithms have been proposed in the literature. These techniques can be classified according to Fig. 3.

Watermarking techniques can be used alongside cryptographic techniques to reinforce security. Watermarking techniques can be used alongside cryptographic techniques to enhance security. In [9], the various possibilities have been detailed.

2.3 The Different Step of Image Watermarking

Watermark Generation. The watermark generator takes a data item as a parameter in order to generate a mark according to the following formula:

$$GENERATOR(data) = watermark \tag{1}$$

In medical imaging, generators generally use meta-data. In [9], the author used the first letters of the surname and first name as data, and the generator is based on the Jocobian model. Some generators use chaotic functions to generate random sequences. In [10] the authors used a chaotic generator and the characteristics of the original image and the brand. They generated a unique secret key using some sub-band of the original image associated with the watermark. The key, numbers (randomly generated) and brand were used to calculate a matrix that would be sensitive to any modification of the key, and therefore to any modification of the brand or the original image. The difficulty with this approach is storing the key in a safe place. In [11] the authors have just used Arnold's transformation to encrypt a logo (watermark) using a key.

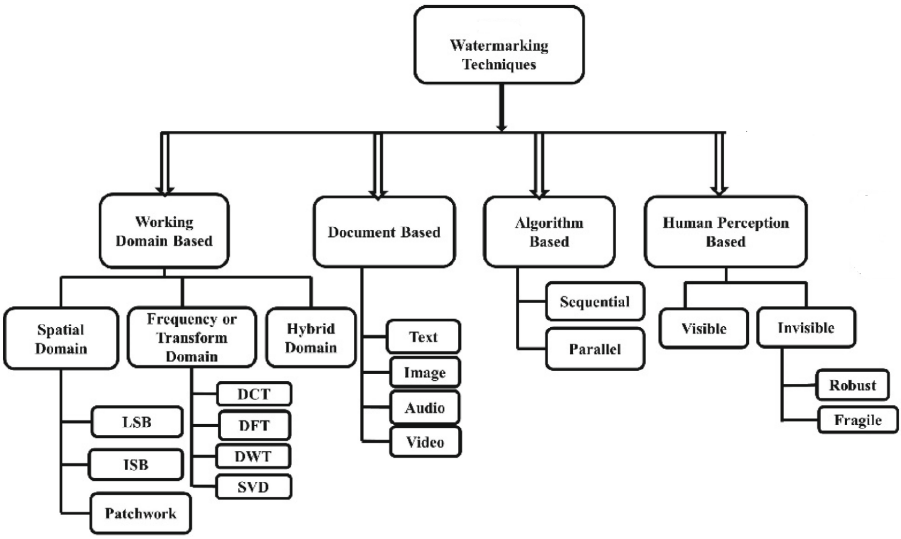


Fig. 3. watermarking process

Watermark Insertion. The watermark is inserted using a function that takes the original image ImO and a secret key K to produce a watermarked image ImW.

$$INSERTION(ImO, K) = ImW \tag{2}$$

Watermark insertion requires the choice of insertion domain (spatial and frequency).

1. In the **spatial domain**, pixels are coded on 8 bits (12 bits for DICOM images) and insertion can be performed on the Least Significant Bit (LSB) on selected pixels. Techniques in this domain (Fig. 3) have a good insertion capacity, but remain fragile in the face of geometric attacks.
2. In the **frequency domain**, an image can be decomposed into several components, with the watermark being inserted into one of the components. Unlike the previous domain, frequency-domain techniques (Fig. 3) have a low insertion capacity but are robust against geometric attacks.

The choice of domain and technique depends on the desired objective. Many schemes in the literature are based on a hybrid approach. In [11] the authors proposed a hybrid based on Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT) and Singular Value Decomposition (SVD). In [12] the authors proposed a scheme based on DCT and SVD. These techniques introduce distortion into the image. These distortions can be controlled by computing evaluation metrics, the main ones being : PSNR (Peak Signal to Noise Ratio), SSIM (Structural SIMilarity) and NC (Normalized Correlation).

Possible Attacks. The watermarked image can be the object of several types of attack. These attacks aim to visualize or remove the watermark. In some cases, the attacker will add another watermark to make it difficult for the receiver to extract the watermark. Figure 4 summarizes the most common types of attack encountered in the literature.

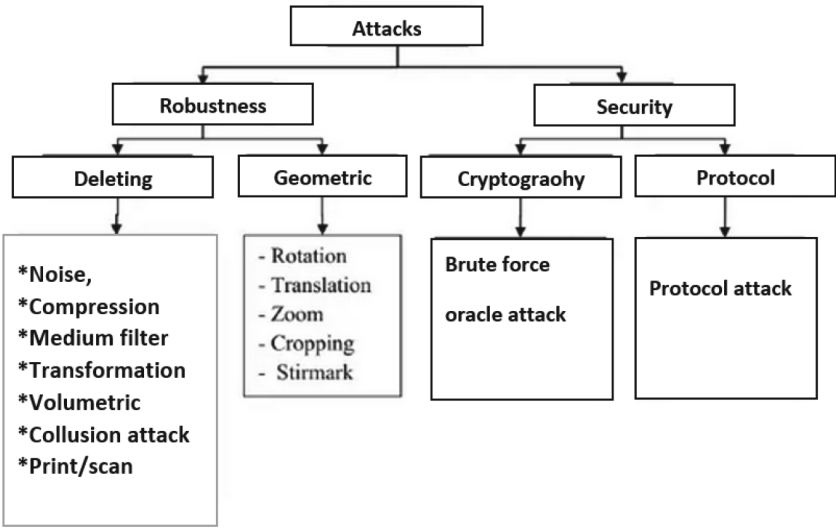


Fig. 4. Attaks

Most watermarking schemes encountered in the literature seek to be robust against geometric attacks and compression: this is the case for robust schemes. For fragile schemes, the solution is generally robust to compression but fragile to geometric attacks, so as to identify any attempts at modification.

Watermark Detection or Extraction. In some applications, the receiver just wants to detect the presence of a watermark. Detection is used to authenticate images. Other applications seek to extract the watermark as faithfully as possible. At this level we can have two possible watermarking schemes.

1. **Reversible watermarking**: this enables the original image to be restored, while removing the mark. It is used for authentication, as well as in military and medical applications.
2. **Irreversible watermarking**: permanently preserves the (often insignificant) changes to the original image when the watermark is inserted, even after the mark has been removed.

Once the receiver receives the watermarked image, the mark can be detected or extracted in one of three ways. These three ways can form a classification.

1. **Non-blind technique**: the sender must send both the watermarked image and the original image. The presence of the latter is essential for detecting or extracting the watermark.
2. **Blind technique**: the watermark is detected or extracted without the original image.
3. **Blind technique**: the watermark detection or extraction can be effected with or without the original image.

2.4 Zero Watermarking

In certain fields of application, these distortions are to be avoided. In such cases, zero watermarking techniques are used. Zero watermarking extracts important and unique characteristics (histogram, median, entropy, energy, co-occurrence matrix, ...) from the original image to build a signature (the watermark). These characteristics are extracted from the properties of the spatial [9] or frequency [10] domain. The signature must be stored securely. It can be used later to identify and authenticate the image.

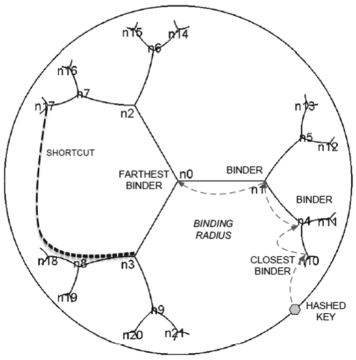
In [9] the author first used static analysis of the host image to extract relevant characteristics. Then he extracted information from the patient before transforming it into a binary matrix. It uses a cumulative subtraction process on the host image to generate a matrix of the same size as the binary matrix. The new matrix is used to define Jacobian functions that generate a Jacobian matrix. The latter is used to construct a signature (key to be transmitted to the recipient). Comparisons show that their solution is better than existing methods for certain types of attack with good metrics. However, it is not as good for other types of attack with low metrics.

In [13] the authors proposed a zero-watermarking solution based on convolutional neural networks (CNNs). They first extracted features and from the trained CNN. The extracted features are and linked to the owner's brand to generate a master share. The main share is stored securely. When an image is subject to an ownership dispute, it is fed into the trained CNN as input and its inherent features are extracted. The extracted image features and the master share are used to retrieve the tattoo pattern. This approach is robust in the case of high distortion with 22 dB PSNR, but the processing time is long.

3 Database for Images

For transfer and archiving, we're going to use a distributed database based on [6]. This database is made up of virtual servers with virtual addresses that are hyperbolic coordinates. The database is chosen for its scalable, reliable and consistent structure. It is ideal for storing large amounts of data, and also supports queries on large data sets.

Setting up the structure of this distributed database is like incrementally building a hyperbolic tree in the Poincaré disk. The hyperbolic tree is characterized by two parameters: degree and depth. Before building the tree, it is



Algorithm 1: Recursive building of our virtual hyperbolic tree.

```
1  Function NodeChildrenCoordComp (Node, q);
   Input  : Know the coordinates of every node: N
   Output: Computethecoordinatesofitschildren : N1...Np
2  step ← argcosh(1/sin(π/q));
3  angle ← 2π/q;
4  childCoords ← Node.Coords;
5  for i ← 1 to q do
6  |  ChildCoords.rotationLeft(angle);
7  |  ChildCoords.translation(step);
8  |  ChildCoords.rotationRight(π);
9  |  if ChildCoords ≠ Node.ParentCoords then
10 |  |  Node.TabChildCoords[i] = ChildCoords;
11 |  end
12 end
13 return ChildrenCoord;
```

Fig. 5. Hyperbolic database structure

necessary to set these two parameters. In Fig. 5 we have a tree of degree 3 . Starting from this figure, the first virtual server (node $n0$) will have address [0,0] (the center of the disk). It will then calculate the addresses of its three children ($n1$, $n2$ and $n3$). From these, each node will calculate the addresses of its two children until it reaches the depth of the tree. In [6], the authors proposed an algorithm for computing the coordinates of a node at each step. Based on this algorithm, we propose an algorithm (shown in Fig. 5) to build our hyperbolic tree.

4 Our Hyper-catadioptric Model

A hypercatadioptric system consists of a lens and a hyperbolic mirror.The camera's optical axis coincides with the mirror's axis of symmetry. Its mathematical model [7] will enable us to move from Euclidean space to hyperbolic space.

4.1 Hyper-catadioptric Model Ant Projection

The model of the hyper-catadioptric system is based on two types of projections [7]. A hyper-catadioptric projection is used to determine the $P_m(X_m, Y_m, Z_m)$ mirror projection of a $P(X, Y, Z)$ point in space. The second projection, called stereographic projection, determines the project $p(x, y)$ of the image plane of the point $P_m(X_m, Y_m, Z_m)$.

These two transformations can be resumed using the g function:
$P(X, Y, Z) \mapsto p(x, y)$.

$$g(X, Y, Z) = (r_i \frac{X}{\sqrt{X^2 + Y^2}} + u_0, r_i \frac{Y}{\sqrt{X^2 + Y^2}} + v_0) \tag{3}$$

$r_c = (\sqrt{X^2 + Y^2}, Z)$; $r_i = \alpha r_c \frac{\pm\sqrt{k(k-2)(Z^2+r_c^2)} - Z(k-1)}{Z^2 - k(k-2)r_c^2}$

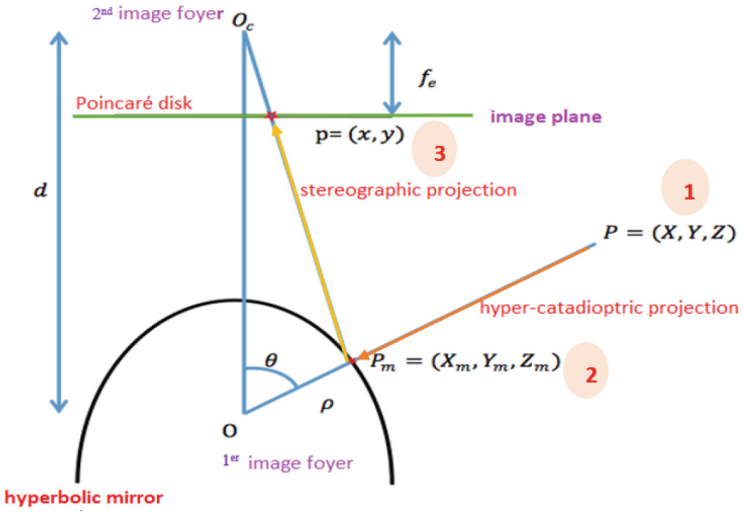


Fig. 6. Hyper-catadioptric and stereographic projections

u_0 and v_0 are the coordinates of the projection of the camera's optical axis. k and α are parameters

The inverse transformation gives the direction to which the image point belongs. g* : $(u, v) \mapsto \overrightarrow{D}$

$$g^*(u,v) = \left(\frac{u}{\sqrt{u^2+v^2}}, \frac{v}{\sqrt{u^2+v^2}}, z\right) \tag{4}$$

$$z = r_i \frac{\alpha(k-1) \pm \sqrt{k(k-2)(\alpha^2+r_i^2)}}{r_i^2 k(k-2)\alpha^2} \tag{5}$$

The implementation of such a system requires the determination of intrinsic and extrinsic parameters. The determination of these parameters remains quite complex, hence the need to use calibration techniques. These are based on the knowledge of the pairs of points (3-D, 2-D). A mapping of these points and their projections will estimate the parameters (u_0 , v_0, k and α) of the model.

4.2 Model Simulation

We then estimate the parameters proposed in [7]. We will then have u_0 =160.49, v_0= 119.02, $k = 3.75$ and $\alpha = 183.45$ The aim of model simulation is to determine the boundary values and observe the various transformations. To visualize the transformation, we'll use one of the characteristics of hyperbolic space. Straight lines in Euclidean space are arcs in hyperbolic space. To achieve this, we'll consider aligned points in our Euclidean space and then determine the images using the g function. After calculation, we obtain images represented by the Fig. 7.

On this figure we observe a convergence towards point P_f On the image plane we will have a disk of center $P_0(u_0, v_0)$ and radius P_0P_f. So our first virtual address will be (u_0, v_0). From this we can determine the address of its descendants until we reach the fixed tree depth.

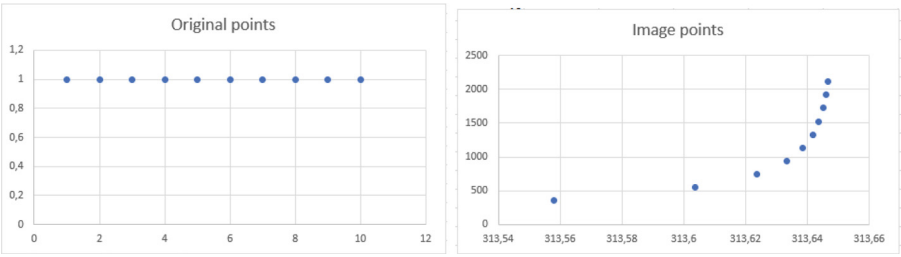


Fig. 7. Original points and Computing the image points

5 Solution

We're going to assimilate the image plane of the model to our hyperbolic space, which is the Poincaré disk. In this disk, we'll build our hyperbolic tree, which is the basic structure of our database. In our approach, each server stores the hyperbolic coordinates of the image points, the model parameters and the equation of the plane.

5.1 Our Scheme

Our schema is illustrated by these two Figs. 8 and 9

Sender

1. **Step 1.** Place the image in Euclidian space. The system must save this equation. The knowledge of this equation is necessary to reconstitute the points.
2. **Step 2.** Select pixels using an interest point. Selected pixels must have a good distribution on the image.
3. **Step 3.** Compute the transform of selected points
4. **Step 4.** Group image points to nearest node. Each node can save N_i image points. The set of tuples (N_1, N_2, N_3..., N_n) represents our cryptographic signature. The system must return the number of nodes used.
5. **Step 5.** Generate the image OID (Objet IDentifier). Since OID is considered a private key, the system must ensure its uniqueness. It must be generated by a function that takes metadata information and image characteristics (entropy) as parameters. Any attempt to modify the image or metadata will produce a different OID.

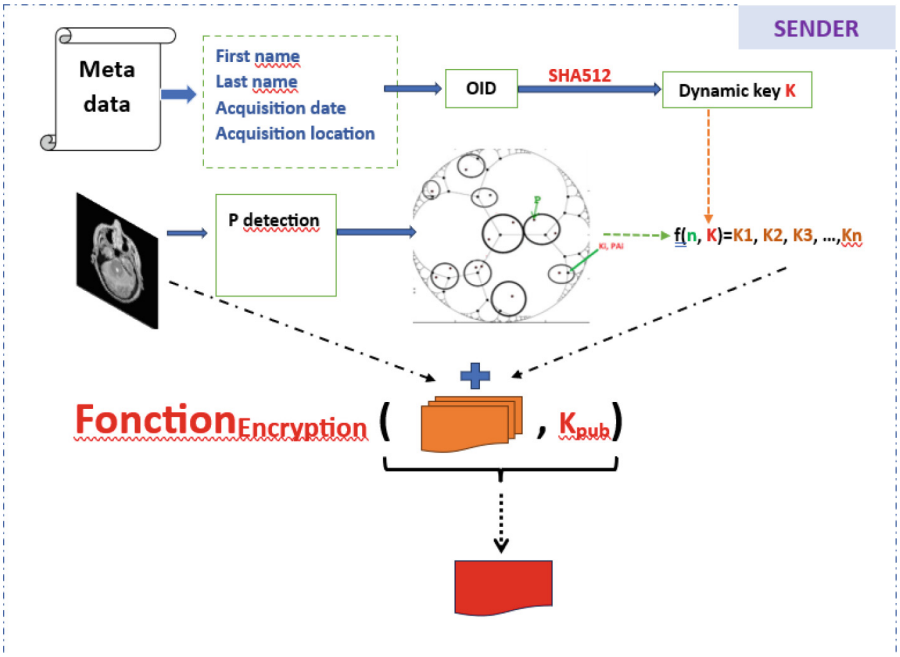


Fig. 8. Sender

6. **Step 6.** Determine the dynamic key K. We will generate K (512 bits) using a hash function (SHA512) parameterized by the image OID.
7. **Step 7.** Split the dynamic key K into subkeys (k_1, k_2, k_3,..., k_n). This decomposition is based on the number of nodes returned in step 4.
8. **Step 8.** Associate each sub-key k_i with the node of the tree and a set N_i. Subkeys represent public keys.
9. **Setup 9.** Encrypt the watermarked image and subkeys with the recipient's public key

Receiver

1. **Step 1.** Decrypt the message with your private key
2. **Step 2.** Search for the k_i associated with your private key
3. **Step 3.** Determine for each sub-key k_i of its server who stores it
4. **Step 4.** Determine the model parameters, the plane equation and the hyperbolic coordinates of each image point.
5. **Step 5.** Compute the inverse transform of each image point
6. **Step 6.** Determine new points of interest using the same detector
7. **Step 7.** Compare new detected points with computed points

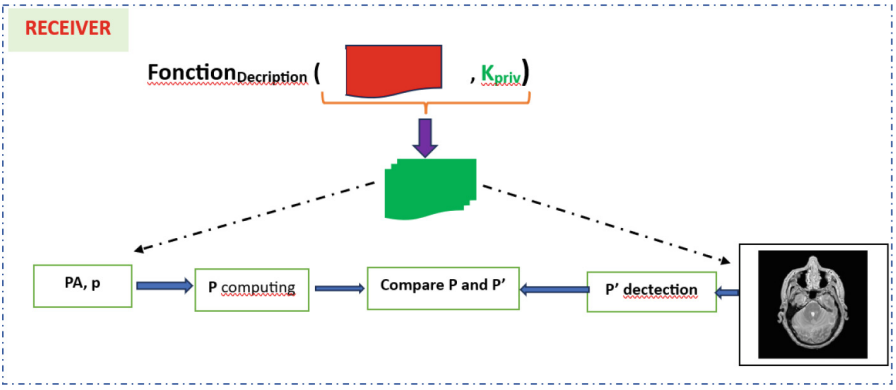


Fig. 9. .

6 Solution Analysis

6.1 Cryptographic System

In our approach the encryption technique is by the asynchronous stream cipher method. Indeed, since the function f of the dynamic key generation is parameterized by an OID which is a series of previously encoded numbers, our encryption algorithm can be considered as an asynchronous stream cipher. This type of encryption is also called self-synchronous stream encryption. The error distribution is limited to the size of the memory. Therefore, if ciphers in the cipher text are deleted or inserted, the receiver is able to resynchronize with the sender thanks to the memory. Concerning active attacks, if an active adversary modifies a part of the ciphers of the coded text, the receiver is able to detect it. It is for these qualities that we have adopted such an approach.

6.2 Formal Analysis

In this section, we present the robustness of our system using a hyperbolic tree topology based on chaos theory. In our context, the step space corresponds to the passage of the image from step i to step i+1 after modification of a pixel. The function f is associated with the composition of two projection functions which are respectively: the hyper-catadioptric projection and the stereographic projection. In particular, we consider discrete dynamical systems.

Definition 1. A discrete dynamical system is a pair (X, f) formed by:

- A non empty topological space (X, p), called the space of steps,
- A continuous function f: X → X, called successor function.

$$\begin{cases} x^0 \in X \\ n \in \mathbb{N}, x^{n+1} = f(x^n) \end{cases} \tag{6}$$

Then we give the elements of the set that allow us to check whether our transformation function is chaotic. These are the properties of the dynamics of regular systems, topological transitivity and sensitivity to initial conditions.

Periodicity. A point $p \in X$ is considered periodic of period k if k is a non-zero integer such that:

$$f^k(p) = p, and \forall h \in [0, k-1] f^h(p) \neq p; \tag{7}$$

We will note $Perk(f)$ the k-periodic set of points of f, and $Perk(f)$ the set of periodic points of any period.

According to Fig. 6 we have: $P \overset{f^1}{\longmapsto} P_m \overset{f^2}{\longmapsto} p \overset{f^3}{\longmapsto} P_m \overset{f^4}{\longmapsto} P$ From this we can say that f is periodical of period 4

Regularity. A discrete dynamical system (X, f) is said to be regular if all periodic points of f, called $Per(f)$, are dense in X. In a metric space (X, d), the dynamical system (X, f) is regular if and only if:

$$\forall x \in X, \forall \epsilon < 0, \exists p \in Per(f), d(x, p) < \epsilon \tag{8}$$

Transitivity. Indeed, in our system for any node of the hyperbolic tree that we take, there exists an image point that minimizes the distance from the node to the image point. Since, for any pair of openings U, V ⊂ X, there exists k > O such that :

$$f^k(U) \cap V \neq \emptyset \tag{9}$$

then f is topologically transitive.

Dependence on Initial Conditions. f has a sensitive dependence on initial conditions if there exists $\delta > 0$ such that, for all x ∈ X and for any neighborhood V of x, it exists y ∈ V and n ≥ O there such that:

$$d(f^n(x), f^n(y)) > \delta \tag{10}$$

δ is called the sensitivity constant of f.

Chaotic System

A function f: X → X is said to be chaotic on X if:

1. (X, f) is regular,
2. f is topologically transitive,
3. f has a sensitive dependence on the initial conditions

Since our transformation function f is chaotic, then the system (X, f) is chaotic, and, according to Devaney, it is unpredictable because of its sensitive dependence on initial conditions. It cannot be decomposed or simplified into two non-interacting subsystems because of topological transitivity.

7 Conclusion

In this paper, we propose a new robust zero watermarking scheme for authenticating medical images. This scheme is based on the hyper-catadioptric system model and hyperbolic geometry. The main contributions of this new approach are as follows. Firstly, through simulations, we have determined the characteristics of the center and radius of the image plane. Then we propose to adapt our image plane to the structure of the database. We therefore propose to use a selection of points of interest well distributed over the whole image to ensure the integrity of the whole image. In addition, we propose to use an asynchronous stream encryption system to restore the image after an attack. Finally, we propose a new zero-watermarking scheme to secure and authenticate images in the distributed database. Implementing this model enabled us to observe transformations and adapt our watermarking scheme to the structure of the distributed database. The formal analysis of our schema reveals the chaotic aspect of the watermarking scheme and therefore its robustness. We made three major contributions. Using simulations, we determined the various characteristics of the hyper-catadioptric model. Then we related the hyperbolic structure of the distributed database to the image plane. Finally, we proposed a new watermarking scheme based on the hyper-catadioptric model and the hyperbolic structure. In the course of our work, we will implement the watermarking scheme proposed in this paper and make a comparative analysis of our solution with existing ones in terms of performance. We will exploit the regions of non interest to insert more data in the frequency domain.

References

1. Singh, O.P., Singh, A.K., Srivastava, G., Kumar, N.: Image watermarking using soft computing techniques: a comprehensive survey. Multimedia Tools Appl. **80**(20), 30367–30398 (2021)
2. Mohanarathinam, A., Kamalraj, S., Prasanna Venkatesan, G.K.D., Ravi, R.V., Manikandababu, C.S.: Digital watermarking techniques for image security: a review. J. Ambient Intell. Human. Comput. **11**(8), 3221–3229 (2020)
3. Kamaruddin, N.S., Kamsin, A., Por, L.Y., Rahman, H.: A review of text watermarking: theory, methods, and applications. IEEE Access **6**, 8011–8028 (2018)
4. Tiken, C., Samli, R.: A comprehensive review about image encryption methods. Harran Üniversitesi Mühendislik Dergisi **7**(1), 27–49 (2022)
5. Geetha, S., Punithavathi, P., Infanteena, A.M., Sindhu, S.S.S.: A literature review on image encryption techniques. Int. J. Inf. Secur. Priv. (IJISP) **12**(3), 42–83 (2018)
6. Tiendrebeogo, T., Magoni, D.: Virtual and consistent hyperbolic tree: a new structure for distributed database management. In: Bouajjani, A., Fauconnier, H. (eds.) NETYS 2015. LNCS, vol. 9466, pp. 411–425. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-26850-7_28
7. Comby, F., de Kerleau, C.C., Strauss, O.: Étalonnage de caméras catadioptriques hyperboloïdes. Traitement du Signal **22**(5), 419–431 (2005)
8. Cox, I.J., Doërr, G., Furon, T.: Watermarking is not cryptography. In: Shi, Y.Q., Jeon, B. (eds.) IWDW 2006. LNCS, vol. 4283, pp. 1–15. Springer, Heidelberg (2006). https://doi.org/10.1007/11922841_1

9. Tayachi, M.: Sécurité des images par tatouage numérique et cryptographie dans les applications médicales. PHD thesis, school: Université de Bretagne occidentale-Brest; Université de Tunis El Manar (2021)
10. Zainol, Z., Teh, J.S., Alawida, M.: A new chaotic image watermarking scheme based on SVD and IWT. IEEE Access **8**, 43391–43406 (2020)
11. Alzahrani, A., Memon, N.A.: Blind and robust watermarking scheme in hybrid domain for copyright protection of medical images. IEEE Access **9**, 113714–113734 (2021)
12. Mohammed, A.A., Jebur, B.A., Younus, K.M.: Hybrid DCT-SVD based digital watermarking scheme with chaotic encryption for medical images. In: IOP Conference Series: Materials Science and Engineering, vol. 1152, no. 1, p. 012025. IOP Publishing (2021)
13. Fierro-Radilla, A., Nakano-Miyatake, M., Cedillo-Hernandez, M., Cleofas-Sanchez, L., Perez-Meana, H.: A robust image zero-watermarking using convolutional neural networks. In: 2019 7th International Workshop on Biometrics and Forensics (IWBF), pp. 1–5. IEEE (2019)