International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-9 Issue-3 September 2020

Robust Formal Watermarking Model Based on the Hyperbolic Geometry for Image Security

Telesphore Tiendrebeogo, Cheick Yacouba Rachid Coulibaly, Maliki Badolo

Abstract*: The digital revolution has led to an increase in the production and exchange of valuable digitized documents across institutions, companies and the general public alike. Ensuring the authenticity, integrity and ownership of these official or high-value documents is essential if they are to be considered useful. Digital watermarking is a possible solution to this challenge as it has already been used for copyright protection, source tracking, and video authentication to name just a few applications of its use. It also enables integrity protection, which is of value for numerous documents types (e.g., official documents, medical images). In this paper, we propose a new watermarking solution that is applicable to image watermarking and is based on hyperbolic geometry. Our new solution builds upon existing work in geometrical watermarking.

***Keywords*: Watermarking Hyperbolic Geometry, Poincaré Disk Model, Hypercatadioptric Projection, Cryptography, Image Processing**

I. INTRODUCTION

The protection of digital documents and intellectual property in the digital world is a real concern, especially with the increase of file transfers over the Internet [1]. Such data is easily corrupted by hackers and therefore, given its value, security solutions that protect such data are essential. These security solution protect against the interception, the duplication, the forgery and the corruption of data. Digital watermarking has been developed as one such security solution. It builds on the foundations of physical watermarking. The principle of watermarking consists of inserting into a digital document a visible or invisible mark, containing information resistant to an attacker looking to modify the watermark data [2]. Several watermarking algorithms try to find a compromise between robustness and invisibility. However, none of them fully satisfy either property (robustness, invisibility). They only work for restricted contexts of use and are intended to be used on very specific document types. To date, there is no universal functional model, which can adapt itself to any kind of document.

Revised Manuscript received on August 01, 2020.
Revised Manuscript received on August 05, 2020.
Manuscript published on September 30, 2020.
***** Correspondence Author
Telesphore Tiendrebeogo, Assistant Professor, Nazi Boni University, Burkina Faso.
Cheick Yacouba Rachid Coulibaly, Nazi Boni University, Burkina Faso.
Maliki Badolo, Nazi Boni University, Burkina Faso.

Hyperbolic geometry and its associated models, such as the hypercatadioptric [3] and the Poincaré disk [4] have many properties, which we exploit within the context of this work. Our aim in this paper is to propose a new solution for image watermarking, which complements existing cryptographic techniques for image transmission that have shown their limitations [5].

Furthermore, we use new techniques in image processing [6] that provide a number of novel elements, which we have incorporated into our study, resulting in a more robust and imperceptible solution.

Our paper is structured as follows: we first present related work on watermarking that uses geometry techniques. We then provide an overview of the principles and applications of watermarking, and we describe our model. We orient our approach towards hyperbolic geometry, we explain the Poincaré disk model, and we describe the cryptography principles in the hyperbolic tiling context. Afterwards, we present our image watermarking and cryptography methodology. We provide our results and discussions through a formal analysis of the robustness and perceptibility of our solution. Finally we present our conclusion.

II. RELATED WORK

The increase of digital exchanges has favored illicit exploitation of digital content. To counter this problem, researchers have developed many solutions around digital watermarking. The common principle to the various proposed solutions consists in watermarking (sign or mark) the work or object to be protected with an imperceptible signature which allows for the identification of the owner, while remaining resistant to attacks [7]. The various marking systems proposed in the literature can be classified in either of the two following categories: the systems which act directly in the spatial domain [8][9], and those that act in the frequency domain [8]. Although they present advantages such as simplicity of implementation and calculation, the systems which operate directly on the image are generally vulnerable to geometrical attacks. To insert a mark, the latter use couples or blocks of pixels to which they bring light modifications (imperceptible to the eye) and which respect previously established marking rules. Any geometrical transformation on the image watermark often makes it impossible to extract. Methods which operate in a transformed plan (e.g., DCT, wavelets, Fourier, etc.)

allow the construction of watermarking systems that are robust against attacks of geometrical nature (e.g., rotation, windowing, etc.), or of a signal processing nature (e.g., compression, filtering, etc.). However, spatial techniques remain by far the fastest and the simplest modes of attack compared with techniques which operate in the transformed plan [7]. Compared to the use of cryptography for secure exchanges, watermarking can provide individual documents with persistent authentication and integrity regardless of whether they are stored or in transit.

The watermarking of images can, thus, be a solution to secure the transfer of images. The objective of watermarking is to insert information into the image in a invisible and indelible way. The insertion of the message can be made in the spatial or frequency domain, or in a combination of both domains [10][11].

Several existing techniques insert watermarking into various spatial primitives, such as the distance between a summit and a center of gravity of the meshing [12], the local density of triangulation [13] or the relative position of a summit to its neighbors [14]. Except for methods based on statistical descriptors of shape [15], those techniques are vulnerable to attacks on connectivity. To solve this vulnerability, some algorithms suggest making a preprocessing of re-sampling on the meshing to be tested before the extraction [16].

Another category of algorithms begin by decomposing the meshing in the spectral domain, and then inserting the watermarking into various frequency components according to the aimed application [17][18].

These methods generally provide a better inaudibility and also a better robustness to geometrical attacks. Nevertheless, fragility in the face of connectivity attacks still exists. For example, the Laplacian spectral analysis of a 3D meshing is sensitive to the changes of connectivity [17]; the iterative decimation of edges to build a representation multi-resolution also depends on the connectivity [19]; also most of the tools for analysing the wavelets of a 3D meshing require that the meshing be decomposed is at least semi-regular [20].

To our knowledge, no method based on the hyperbolic geometric and catadioptric projective transformations, while being resistant to various geometric distortion attacks, has yet been proposed. In this paper, we propose a new image watermarking technique which allows for the identification of the owner thanks to an imperceptible signature resistant to attacks. Our technique is based on the projective geometrical transformation of the image in the hyperbolic space before extraction of the points of interest that will be used for marking. The identification of the points of interest is similar to the Harris principle [21].

III. WATERMARKING BACKGROUND

For the understanding of the reader, we provide background information on watermarking principles for the proposed approach, and we highlight some of its applications. To start, we motivate our work by highlighting some of its applications, notably for ensuring document security. We focus on discussing cryptography principles in light of the objective of watermarking.

A. Watermarking for document security

Figure 1: General representation of communication.

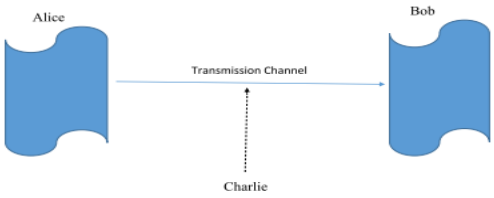

Figure 1: General representation of communication.

Consider the illustration in Figure 1 where a sender named Alice transfers a document to a receiver, named Bob. During this transmission, a third party, Charlie, may attempt to extract or modify the document data. The document can thus be intercepted or its integrity attacked.

Figure 2 illustrates a partial view of the diagram representing key terminology used in document securing, where the root term is Cryptology, i.e., the science of protecting information. Within cryptology, cryptography, steganography and Watermarking constitute the three major methods used. These methods differ in terms of their algorithms, how they manipulate the information as well as the timeline during which the information is protected. For example, Figure 3 illustrates a weakness in processes that use cryptography but where a document is vulnerable to attacks after decryption. However, we can notice some similitude points between these three methods as indicated in Figure 4.

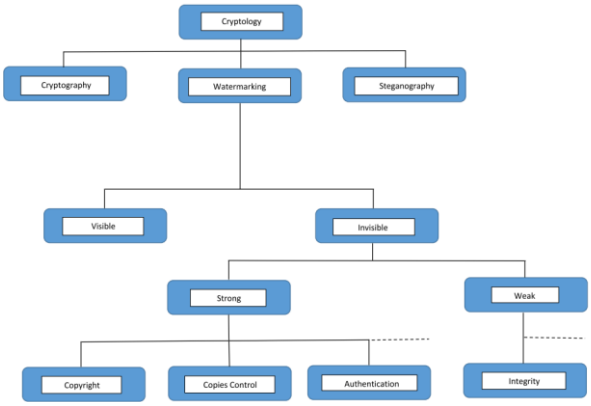

Figure 2: Security and safety methods diagram.

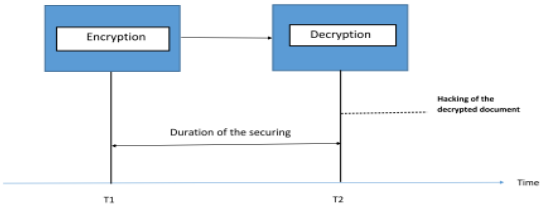

Figure 3: Encrypted document safety duration.

In the remainder of this paper, our focus will be on digital documents. Typically, cryptography allows for the protection of document information during its transmission over a network. It renders the document illegible from the moment it is encrypted until it is ultimately decrypted.

This is made possible through the use of keys. Only owner(s) of key(s) have access to the encrypted information. Such a method has been shown to be efficient for protecting information during its transmission between authorized parties. It is leveraged for example in the military for the transmission of orders when in the field. It is also commonly used to prevent viewing, by non-paying clients, of certain programs on private television channels. The essence of cryptography is the obfuscation of data for security purposes in a time-frame (i.e., between encryption and decryption). To "permanently" protect information (i.e., beyond its transmission time-frame), practitioners often leverage steganography. Steganography is defined as the art of hiding information within a medium.

There are two approaches to steganography:

- The first approach consists of hiding the piece of information to be protected inside another document. It is known as information camouflage or data hiding. The principle of this approach is similar to that of cryptography: information is inserted or extracted from the medium by means of codes generated by keys. Nevertheless, unlike cryptography, the protected information is not visible in the document.
- The second approach to steganography consists of integrating a signature into a document to protect the document and thus prevent any attack to integrity. This approach is known as watermarking. Our work focuses on this approach to steganography. Figure 4 provides a comparative illustration of the features involved in watermarking in comparison with other document security techniques.

There are two distinct approaches that watermarking techniques can modify/alter documents:

a) Semantic watermarking modifies the content of the document.
b) Syntactic watermarking modifies the storage format of the document.

In both cases, changes applied to the document are not supposed to affect its usability. In contrast, attackers of watermarked documents aim to remove, or at least alter, the mark left on the document by the watermarking algorithm.
qualification of the algorithm of watermarking. Indeed, according to the mode of attack, the quality of the watermark can be reduced (a case of strong algorithms) or the watermark can be significantly changed (a case of weak algorithms). In our case, we shall use a hybrid technique, which is a technique that allows for, on the one hand, a modification of the contents in the grey area and on the other hand, a modification of the storage format through a topological change going of that Euclidean in that Hyperbolic. This to give all the chances to a possible attack.

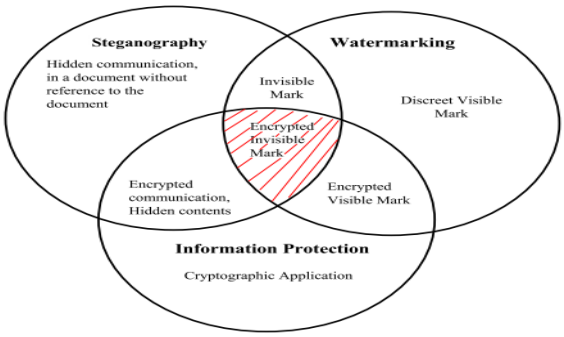

Figure 4: Relations with other safety domain.

Furthermore, there a multiple applications for water-marking in information technologies, such as ensuring the integrity of video streaming; owner identification; proof of ownership; follow-up of transactions; authentication; copy control; meta-data insertion.

B. Watermarking Principles

We consider the following notations in the description of various steps in the watermarking process: let D denote any document and D_0 the original document. Any digital document is defined as a series of binaries: $D \in \{0, 1\}*$. A document is qualified as quality during a transmission if and only if:

$$F_q: \{0, 1\}^* \times \{0, 1\}^* \rightarrow \{0, 1\} \quad (1)$$

Where F_q is a quality function. Thus two documents are of the same quality if and only if:

$$F_q(D, D') = 1 \quad (2)$$

F_q can be considered as psychology perceptive criteria.

With regards to the watermarking model, let us consider the following model:

Let M and D be a pair of algorithms, designated by: (D, M), with M as the marking algorithm and D as the document algorithm. The marking of the document consists of what follows:

$$F_M: \{0, 1\}^* \times \{0, 1\}^* \rightarrow \{0, 1\}^* \quad (3)$$

Where F_M is the marking function associated with

$$M(D, I) = D' \quad (4)$$

where D' corresponds to the watermarked document and I corresponds to the information inserted in the original document (called additional information). In the remainder of this paper, we focus on documents representing digital images.

The syntactic model (consisting of insertion by addition), also referred to as the additive scheme in watermarking, is illustrated in Figure 5: a signature is added to a digital image. We study the case where the signature is generated in a pseudo-random way, on the basis of a key K. The signature is then transformed into a message before being added to the coefficients of the image.

The coefficients of the image arise from the image itself or are the result of a space representation change.

The semantic model (consisting of insertion by substitution), also referred as the substitute scheme of watermarking, is illustrated in Figure 6: certain components of the image are replaced by the signature.

Such a signature is then initially obtained by applying a constraint (for example a relation of order, a criterion of similarity, a geometrical property of the image) to the components
according to the message to be inserted.

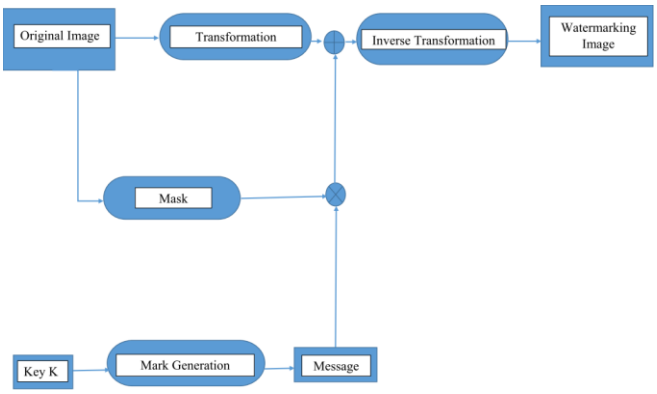

Figure 5: The additive Scheme for the signature insertion.

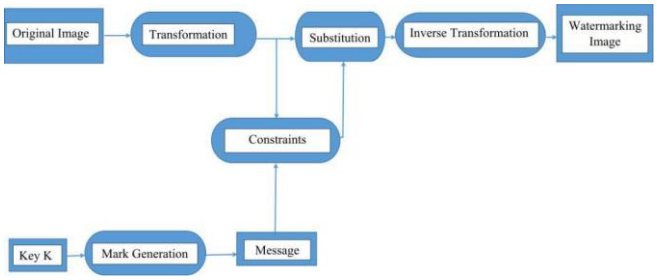

Figure 6: Substitute Scheme of the signature insertion.

With regards to watermarking detection, let us consider the following model:

Let F_D be the detection function that allows for the recognition of the original image. This function is defined as follows:

$$F_D: \{0, 1\}^* \times \{0, 1\}^* \rightarrow \{0, 1\} \quad (5)$$

Let D_0 and I_0 respectively be a suspicious document and any other (supposedly additional) information, then we can state that a document is authentic (original document), if and only if:

$$F_D (D_0, I_0) = 1 \quad (6)$$

where I'= I or I' ≠ I. For the sender or the addressee, I will always be equal to I' (I = I').

Proposition 3.1.:

- ∀{D, I}, F D (F M (D, I), I) = 1. These properties (in total) are called "Adjustment".
- ∀{D, I}, F_q (D, F_M (D, I)) = 1. These properties (in total) are called "Inaudibility".

Figure 7 illustrates the specific case of a simplified detection technique that will be referred to in this paper in the axis of the substitution scheme. In practice, we intend to use a hybrid technique, which involves substitution and addition at the same time. However, with detection based on an additive scheme and when it is about a blind technique, we could use statistical methods (where the original image is not available for detection). In this case, a measure of correlation can be made for example.

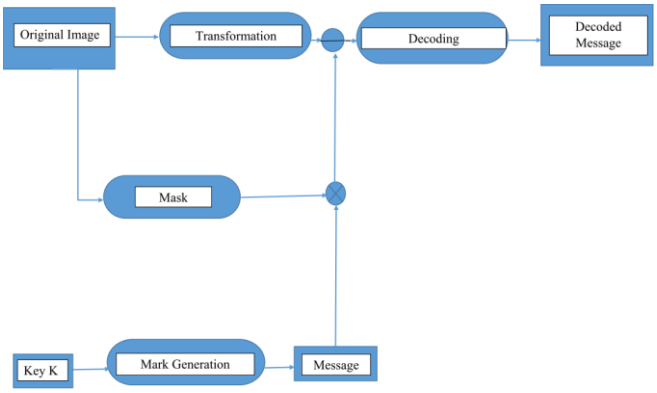

Figure 7: Detection and reading of the signature.

IV. ORIENTATION TOWARDS HYPERBOLIC GEOMETRY

In this section, we introduce the properties of hyperbolic geometry, illustrate the steps for constructing tiles in the hyperbolic plan, before presenting a model of hyperbolic tree. These are essential for investigating the new model of watermarking that we propose.

A. Properties of hyperbolic geometry

The basis of hyperbolic geometric is driven by Euclid's five postulates [22]. Thus hyperbolic geometry must be understood in light of Euclidian geometry.

The basic elements of Euclidian geometry are: the point, the straight line, the right angle, the intersection and the congruence among angles. The five postulates are then as follows:

- The straight line postulate: a straight line segment can be drawn joining any two points;
- The continuation postulate: any straight line segment can be extended indefinitely in a straight line;
- The circle postulate: given any straight line segment, a circle can be drawn having this segment as radius and one of its end-points as center;
- The equal right angles postulate: all right angles are equal;
- The parallel postulate: if two lines are drawn which intersect a third in such a way that the sum of the inner angles on one side is less than two right angles, then the two lines inevitably must intersect each other on that side if extended far enough.

Hyperbolic geometry, also referred to as Lobachevsky geometry, **disagrees with Euclid's fifth postulate** and bases itself on the findings of Legendre [23].

Our work focuses on the hyperbolic space around the dimension n ≥ 2. The hyperbolic plan being of course the hyperbolic space of dimension (i.e., size) 2. The hyperbolic space is an homeomorphous metric space (E, d) in the Euclidean space R^n. This is interesting because of the size of its group of isometry, whichis of dimension n(n + 1)/2; only the Euclidean and spheric spaces are as good.

Although there are many models of this metric space [24], we are particularly interested in the model of the half-hyperboloïd (H^n , d).

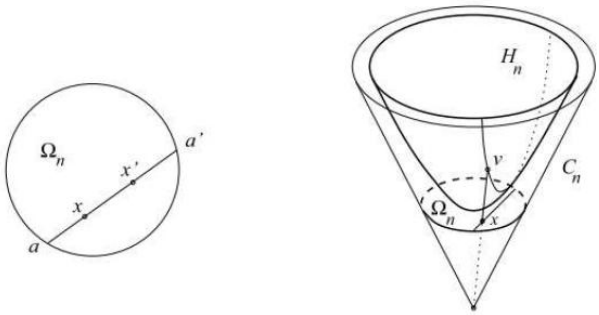

Figure 8: A projective ball and the half–hyperboloïd (from left to right).

Figure 8 illustrates our hyperbolic geometric model where angles and geodesic are deformed. It remains nonetheless useful in describing the isometries of the hyperbolic space. This representation also plays a crucial role in the construction of tilings in following sections. Let us note q the lorentzian quadratic form on the vectorial space V= R
n and b the associated bilinear form. For v = (x_0 , x_n) and w = (y_0 , y_n), we have:

$$b(v, w) = x_0 y_0 + x_1 y_1 + \ldots + x_n y_n$$

and q(v) = b(v, v).

We note C_n as the cone of the future of this lorentzian form and H_n as the top of the hyperboloïd :

$$C^n = v \in R^{n+1} \mid q(v) < 0 \text{ and } x\,0 > 0,$$
$$H^n = v \in R^{n+1} \mid q(v) = -1 \text{ and } x0 > 0. \quad (7)$$

We still define the distance of two points v and v' of H_n as:

$$d(v, v') = |\log([p, p', v, v'])| \quad (8)$$

Where p, p' are the points of the edge of the cone C n which are on the same right as v and v'
and where [p, p', v, v'] is the bi-report of these four aligned points. Given such a model of the hyperboloid, it is easy to describe the group of the isometries of the hyperbolic space. Indeed, the regular hyperbolic tiling is a part of the group of isometries.

By analogy with the Euclidian geometry, we define the angle in hyperbolic geometry. We verify that, for the corresponding ball, it coincides with the Euclidian angle. The angle between two geodesic paths c_1 and c_2 of the hyperbolic space, which arise from the same point x 0 = c_1 (0) = c_2 (0) is the real θ ∈ [0, π] defined by the formula of the rope:

$$2 \times \sin\theta/2 = \lim_{t \to 0} \frac{1}{t} \times d(C_1(t), C_2(t)) \quad (9)$$

This definition does not depend on a specific model. As each of the models are included in an Euclidean space, we can differentiate the hyperbolic angle from the Euclidean angle.

B. Hyperbolic tiling

In this section, we begin with Poincaré's construction of periodic tiling for the hyperbolic plan. This is followed by an overview of the hyperbolic analogues of the theorems of Bieberbach. We begin with the dimension 2. Finally, we present the construction of non-periodic tiling, by means of a single convex tile, for the hyperbolic plan.
Regarding the construction of periodic tiling for the hyperbolic plan, let us begin by describing in full the simplest construction of periodic pavements for the hyperbolic plan as illustrated in Figure 9.

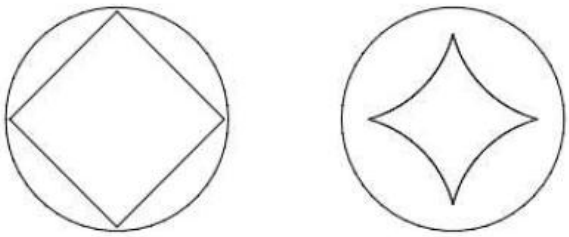

Figure 9: A convex polygon in both projective and conform balls.

As shown in Figure 10, this mechanism can infinitely tile the plan hyperbolic.

C. Poincaré disk model and hyperbolic tree building

The Poincaré disk is the unit disk called D which is the whole universe. Its border consists of unit circles Γ and is infinite. Points are represented by points, however, a Euclidian straight line becomes the arc of a circle, which we call geodesic.

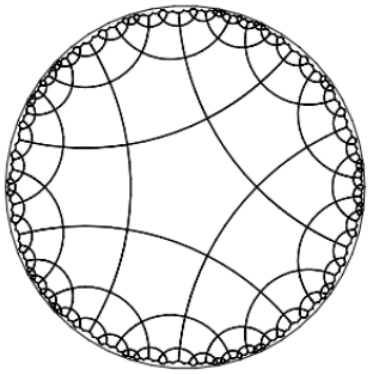

Figure 10: The hyperbolic tiling in an infinity of the regular pentagons in the projective and conform balls [25].

One property of the Poincaré model can be misleading and that is distances are not preserved. If we observe the Poincaré model from an outside perspective, distance appears smaller than in reality (i.e inside the plane). Because the model is a representation of the hyperbolic plane in the Euclidean plane. In fact, the points which seem the closest to the unit circle are, in reality, far away from the latter. The hyperbolic plane has a boundary circle at infinity represented in the Poincaré unit disk model (i.e the open unit disk) by a circle of radius 1 and centered on the origin O. The open unit disk around P 0 is the set of points whose complex modulus is less than 1: |w| < 1 [26].

$$\text{with} \quad |\omega| = \sqrt{(W_{Re})^2 + (W_{Im})^2} \quad (10)$$

It is important to remember certain hyperbolic tiling properties when considering Poincaré disk model and the hyperbolic tree. An elementary property of the Euclidean space is the impossibility of creating more than two half planes without having them intersect. Our embedding is based on the geometric property of the hyperbolic plane which allows for the creation of distinct areas called half planes. As explained in [27], in the hyperbolic plane, we can create n half spaces pair-wise disjoint regardless of the value of n. This property forms the base of our embedded algorithm (red line in Figure 11). Another important

property is that we can tile the hyperbolic plane with polygons of any size, which are called p-gons. Each tessellation is represented by a notation of the form {p, q} where each polygon has p sides with q of them at each vertex. This form is called a schl¨afli symbol. There exists a hyperbolic tessellation {p, q} for every couple {p, q} obeying $(p-2)\times(q-2)>4$. In a tiling, p is the number of sides of the polygons of the primal (the black edges and green vertices in Figure 11) and q is the number of sides of the polygons of the dual (the red triangles in Figure 11).

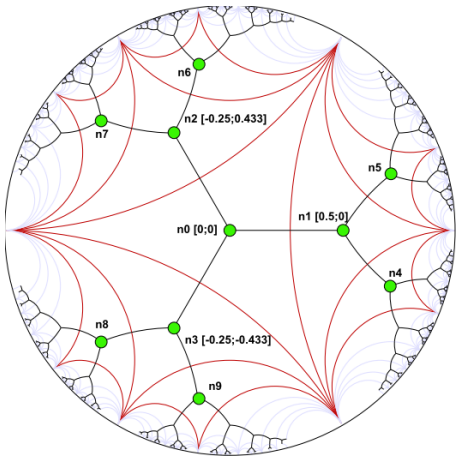

Figure 11: 3-regular tree in the hyperbolic plane.

Our purpose is to partition the plane and address each node uniquely. We set p to infinity, thus transforming the primal into a regular tree of degree q. The dual is then tessellated with an infinite number of q−gons. This particular tiling splits the hyperbolic plane in distinct spaces and constructs our embedded tree. An example of such an hyperbolic tree with q = 3 is shown in Figure 11.

In the Poincaré disk model, the distances between any two points M and N are given by curves minimizing the distance between these two points and are called geodesics of the hyperbolic plane. To compute the length of a geodesic between two points M and N and thus obtain their hyperbolic distance d_H, we use the Poincaré metric which is an isometric invariant:

$$d_H(\mathrm{M},\mathrm{N}) = argcosh(1+2\Delta) \qquad (11)$$

With

$$\Delta = \frac{|M-N|^2}{(1-|M|^2)(1-|N|^2)} \qquad (12)$$

For more details on the Poincaré metric we refer the reader to the proof in [28].

V. Watermarking Methodology

A. Our use of the Central Catadioptric System Geometry

Our watermarking solution, combines hyperbolic mirrors with the Poincaré disk model and can be used in conventional cameras. It functions as a catadioptric sensor which is used by the majority of systems that are based on omnidirectional vision. The constraint on the central point called O_c (corresponding to the second focal spot of the mirror and the optical center of the Poincaré) implies that the straight lines surrounding any point of the space belonging to the original image, which we wish to watermark along with its projection onto the hyperbolic mirror, cross a unique point on the Poincaré disk [29]. Under this constraint, every pixel on the image plan that belongs to the Poincaré disk measures the intensity of the light reflected by the optical beam onto the hyperbolic mirror passing through the central point. This is the first focus/focal point of the optical mirror (called O) in a particular direction. The coordinates of its impact point on the Poincaré disk can be determined as explained in the remainder. Such an approach is interesting as it generates a correct geometric perspective that allows for a simplification of the projection models and thus a simplification of the theoretical and practical image processing. In fact, tools developed within the context of the vision perspective are then often adapted to the set of the central sensors. However, this condition is satisfied only for very particular reflector surfaces. Baker and Nayar in [30] determined the class of all the central catadioptrics. In this case, we are only concerned with the hyper-catadioptric system (i.e. the catadioptric system based on hyperbolic mirrors).

B. Our hyper-catadioptric model for watermarking

Let us consider our catadioptric system obtained by combining an hyperboloïd mirror with a lens in the Poincaré disk form of focal f_e, the optical center of which is merged with the second foyer of the hyperbolic mirror, which we called O_c in Section 5.1. Our approach for building the hyper-catadiotric image on the Poincar´e disk is illustrated in Figure 12.

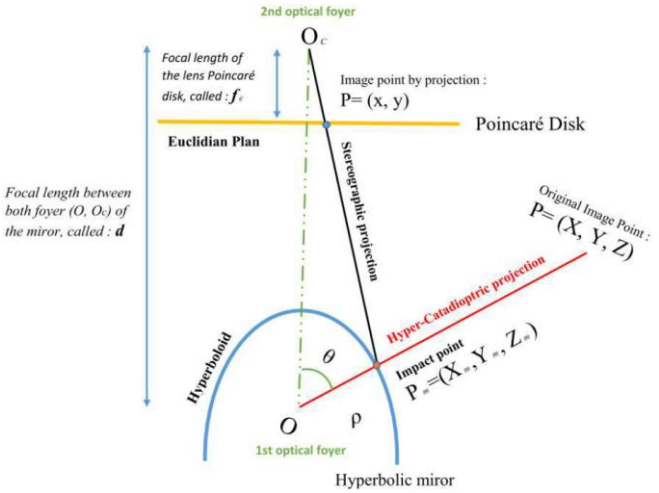

Figure 12: Building the Hyper-Catadiotric image on the Poincaré disk.

The approach shown in Figure 12 uses a subset of original image points that we wish to watermark, called P = (X, Y, Z) (considered to be the beginning of a mark element). Then, we first proceed to a hyper-catadioptric projection on the hyperbolic mirror to obtain points called P_m = (Xm , Ym , Zm), we then make a stereographic projection onto the Poincaré disk of the various points defined by p = (x, y) on the mirror.

C. Image coordinates computing

It has been proved [31], and we agree, that the polar equation of our hyperbolic mirror is:

$$\rho = \frac{p}{1+e\times\cos(\theta)} \qquad (13)$$

In fact, the reduced Cartesian equation of hyperbole is equal to:

$$\frac{X^2}{a^2} - \frac{Y^2}{b^2} = 1 \qquad (14)$$

Let us put $c = \sqrt{a^2 + b^2}$ corresponding to focal half-length. Thus $e = \frac{c}{a}$ et $p = \frac{b^2}{a}$ correspond respectively to the eccentricity and parameter given in the polar equation 13.

Let us consider the projection case. Let the 3D point $P = (X, Y, Z)^T$ be projected onto the hyperbolic mirror at the point $P_m = (X_m, Y_m, Z_m)$ /per-catadioptric projection) where:

$$(X_m, Y_m, Z_m)^T = \frac{\rho}{\sqrt{X^2+Y^2+Z^2}}(X, Y, Z)^T \qquad (15)$$

This point is then projected onto the image plan associated to the Poincaré disk at the point p = (x, y)^T by means of the following projection matrices:

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \sim \begin{pmatrix} f_e & 0 & 0 \\ 0 & f_e & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & d \end{pmatrix} \begin{pmatrix} X_m \\ Y_m \\ Z_m \\ 1 \end{pmatrix}$$

Where d is distance between the optical foyer of the Poincaré disk and the first foyer of the hyperbolic mirror. Thus, to respect the unique point of view, $d = \frac{2\times e\times p}{1-e^2}$ (the Poincaré disk being situated in the Hyperboloid second optical foyer) and as cos(θ) = Z/|P |, we end in the following relation:

$$p = (x, y) = \left(\frac{\frac{1-e^2}{10+e^2} f_e X}{\frac{2e}{1+e^2}\sqrt{X^2+Y^2+Z^2}+Z}, \frac{\frac{1-e^2}{1+e^2} f_e Y}{\frac{2e}{1+e^2}\sqrt{X^2+Y^2+Z^2}+Z}\right) \qquad (16)$$

Before any discussion, it is important to show how algorithmically, we create the virtual hyperbolic tree in our hyperboloid. In fact, this phase with hyperbolic tiling is one of the more important phases in our dynamic process of watermarking as already indicated more formally in Section 4.2. Algorithm 1 is, thus, a process that we have already proposed for hyperbolic tree building. However, in this specific case, it remains configurable depending on the water-marking method chosen.

Algorithm 1: Recursive building of our virtual hyperbolic tree.

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

D. The process of watermarking an image

In this section, we explain two different methods of watermarking that use a whole hybrid technique. In fact, each of these methods use a technique of insertion by substitution that is associated with the insertion by addition technique.

1.First method:

In the first method, a basic constraint must first be explained: the hyperbolic tree must be as well-balanced as possible, furthermore a number of nodes must be equal to 512. We use the Harris' detector [21] to extract the points of interest on the original image. We then compute their images by using our projective method. Once these conditions are verified and when we get back the images of the points of interest on the original image on the Poincaré disk, we group the pixel images, according to their proximity, to a node of the hyperbolic tree that we call binder.

The proximity criterion is obtained by comparing the distance from every point of interest with all the nodes of the hyperbolic tree. Thus, the pixel images are associated with the closest node as illustrated in Figure 13. This process is carried out for every point of interest image. We then look for the coordinates of all the binder nodes that actually have stored image points. Let L× l be the resolution of the original image. Every X-axis and Y-axis point on the Poincaré disk is multiplied (arbitrarily) respectively by L and l (we then have to round off the value to the inferior integer.) We then obtain new coordinates corresponding to those of the pixels that must be modified in the original image. They must be modified either in red (R) or green (G) or blue(B), according to the hyperbolic tree axis (see Figure 13) and white for image points stored by the root. Let us consider an image of resolution L × l = 1200 × 800 with the point P coordinates equal to : P (0.041; 0.0017). The coordinates of the point which must be modified on that original image are: P0 (32; 2).

2.Second method:

In the second method, we first use the Harris' detector [21] to extract the points of interest on the original image. We then compute their images by using our projective method. We first outline a basic constraint: that is the hyperbolic tree has to have a depth equal to 6 and must be q-regular of degree 3. Once these hypotheses are verified, we label the nodes of the tree in binary 0 and 1 according to a rotation +α (computed during the hyperbolic tree building) with the exception of the root and of its immediate children who are named with two bits, such as 00, 01,10, 11 see Figure 14.

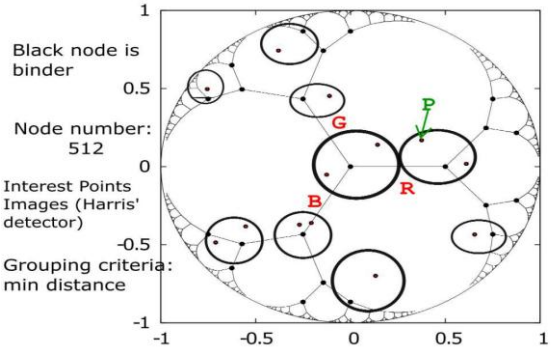

Figure 13: First method of watermarking.

Then, the grouping is made in the same way as in the first case, by storing every image point in the node to which it is closest. However, the comparison is not made with all the nodes of the tree but instead with only three groups of nodes, which are the closest to the image point and which we call: E1, E2 and E3 (having all the ancestors called: A, B and C and direct children of the root called: A, B and C).

In other words, every image point will be closest to three (03) points, unlike in the first case. Then for every image point, reader will be made since the root up to the top of the tree by carrying 0 or 1 according to the label of the node that we go crusader between the root and the top. To specify the binary value of a point, we note the binary values associated with every node from the later towards the root and from the low weight bit towards the high weight bit before eventually finishing with zeros to make 8 bits for each part (E1, E2, E3). Thus every image point gets a code of 3 × 8 bits, corresponding to the code RGB at the grey level. Using the same logic, the color, which we obtain with this color code, will have to be added to the color of the original image point of which it is (knowing that the colors of the interest points are stored at first). Figure 14 shows with red arrows, the shortest distance between the point P and the points associated to the various parts E1, E2 and E3. Thus we find: E1(R): 0000—0001; E2(G): 000—00101; E3(B): 000—00110, corresponding to the grey level of each color (RGB).

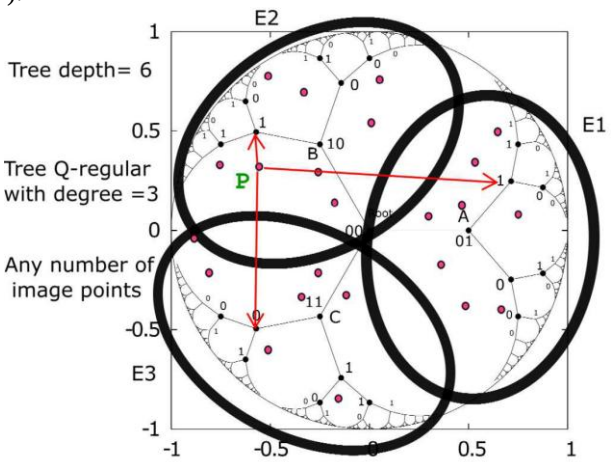

Figure 14: Second method of watermarking.

To summarize, on the one hand our methods use a technique of insertion by substitution because they are partially based on the method of geometrical transformation. In fact, from any image, we can obtain its correspondence in a unit disk of ray equal to 1 and centered at origin. We modify the storage format of the data and we, consequently, make a syntactic watermarking the image. On the other hand, our methods use a technique of insertion by addition because, they allow for a modification of the contents themselves by adding specific levels of grey. We say in this case that we are achieving a semantic watermarking of the image. Thus, we can argue that we are proposing a hybrid watermarking solution.

Algorithm 2 corresponds to our process of watermarking based on hyperbolic geometry properties and catadioptric methods.

E. An image watermarking detection mechanism

Our objective in this section is to outline a solution for detecting the interest points that we use for developing semantic and syntactic (hybrid) watermarking.

First, however, we review the notion of what constitutes an interest point and what we mean by the idea of image processing.

Extant literature already provides several definitions for interest points with regards to image processing, such as Morat [32] and Trichet [33]. We follow Parisot's definition [34], which defines an interest point as being associated with a discontinuity of the grey levels (even colors), of the texture and the geometry, etc. This definition is more general in terms of the type of detectable interest points in an image, and more precise as it considers the intrinsic elements of the image. Parisot's definition is general enough to emcompass the majority of applications for points of interest. Thus, it is also applicable to our application, i.e. for points generated from our original image at the beginning of the process.

A number of tools exist nowadays for image processing. However, many methods employed by existing tools are unsuitable for wide angle images. This is due to the strong distortions that are inherent to this image type, for example images obtained by a hyper-catadioptric method. In these images types the perception of the positions between pixels does not correspond to reality. Thus, the methods of classic filtering, which take into account the position of pixels, are inappropriate for the reconstruction of this image type. Furthermore, the Markov chain process is useful and effective for image processing. It is based on the notion of interdependence between the nearby pixels of an image. Yet as we have just noted, these classic hypotheses are unsuitable and should be modified as wide angle images. That is why it is necessary to adapt the usual methods to take into account the distinctive characteristics of these images. In this context, a reconstruction of the original interest points allows for their conformity to be verified.

Algorithm 2: Hyperbolic watermarking method.

```
Function ImgWatermarking (Img, Resolution);
  Input  : Image (Img) is defined by partners with a given resolution
  Output: Watermarkingimageissupplied
PlanEuc = Process1.getImg();
CreateHyperTree.call(Node.CalcChildrenCoords());
Method = WaterMarking.getMethod();
for i ← 1 to Method.Context do
    PixTab = PlanEuc.generatePix();
    PixCoord = PlanEuc.generateCoord();
end
for i ← 1 to PixTab.Number() do
    TabPm_i = HyperCata.Project();
    Tabp_i = Stereo.Project();
end
for j ← 1 to PixTab.Number() do
    NodeTab = Method.Criteria(Neighbour.Coords);
    Img.OrigPixelTab = NodeTab;
    NodeCoordTab = NoteTab.getCoord();
    Img.OriginCoordX =
      ⌊NoteTab.getCoord().X × Resolution.getX()⌋;
    Img.OriginCoordY =
      ⌊NoteTab.getCoord().Y × Resolution.getY()⌋;
    Img.OriginCoord =
      PointCoord.Put(OriginCoordX,OriginCoordY);
```

```
20  if Method1() then
21  |   SetTreeAxisRGB.Color(PointCoord)
22  end
23  else
24  |   SetBinaryValueRGB.Color(PointCoord)
25  end
26 end                                    25
27 return WatermarkingImg;
```

We have demonstrated that the 3D beam that Corresponds to every pixel of the catadioptric image can be found by the inverse transformation of an hyper-catadioptric projection combined with a stereographic projection. Indeed, Barreto in [35] showed that the non-linear transformation function g of the original image on the Poincaré disk is injective and its reverse g^* is noted.

Figure 15 Illustrates this inverse transformation that we want to establish. In this Figure, as the Poincaré disk presents an angular symmetry, we can reduce the complexity of the problem by considering a 2D angular section. In the section θ, a 3D point $p = [x, y, z]^T$ is represented by $(r_c = \sqrt{x^2 + y^2}, z)$ In the mark $(\vec{R}, \vec{Z})$ with $\vec{R}$ a colinear unitarian vector in the projection of $\vec{FP}$ on the plan $(\vec{x}, \vec{y})$.

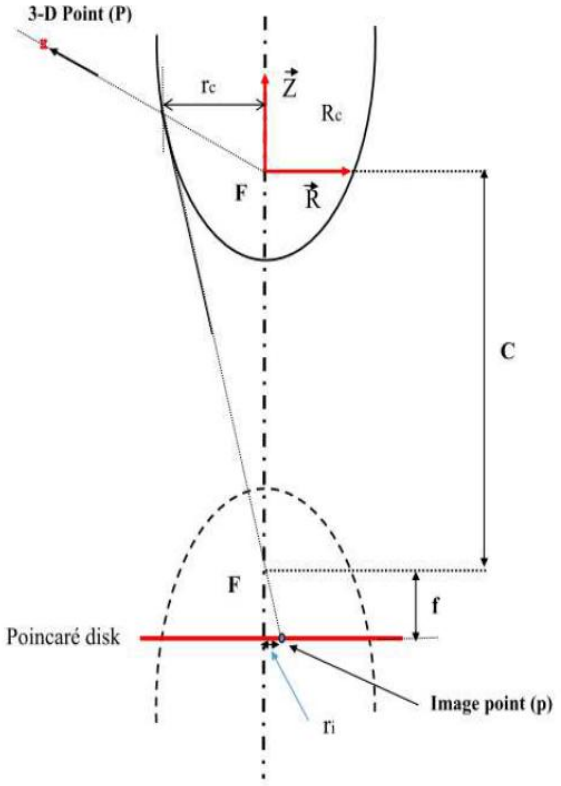

Figure 15: The reverse transformation of our watermarking method.

It is necessary to note, that the transformation function g, that we made in our watermarking approach, is not directly reversable. This is due to the hyper-catadioptric double projection on the hyperbolic mirror and stereographic projection in the Poincaré disk.

Algorithm 3 describes the detection process applied to the watermarking algorithm with the aim of verifying the authenticity of the image.

Algorithm 3: Image detection process in watermarking contex.

```
1  Function Detection (WimageM, TabParam);
   Input  : Gets a watermarking image and parameters: WimageM,
            TabParam
   Output: Verify the conformity of the image
2  ImgParam = WimageM.getParam();
3  DetectImg1 = Process.Calibrate(ImgParam);
4  DetectImg2 = Process.Estimate(DetectImg1);
5  TabIntPoints = Process.ReverseTrans(DetectImg2);
6  NbIntPoints = TabParam.getIntPointNb();
7  for i ← 1 to NbIntPoints do
8  |   NbCorrespond = 0;
9  |   if OrigImgPix! = Process.ChooseImgPix() then
10 |   |   return Makingisnotauthentic;
11 |   else
12 |   |   NbCorrespond + +;
13 |   end
14 end
15 if NbCorrespond == NbIntPoints then
16 |   return Markingisauthentic;
17 end
18 return NULL;
```

The reverse projection g^* only gives the direction in the space associated to the original image points. This direction is important as it stores the parameters, such as the coordinates of the plan, where the original images were placed, as well as the coordinates of each of the angles of the image in the latter. In this way, we can be sure of finding the real pixel that corresponds to the initial interest point.

In order to prove the authenticity of a document, we compare every interest point using our reverse transformation method with pixels that correspond to the interest points of the original image. If the comparison is equal, then, the document is authentic. Otherwise, the document has been altered in some way. Furthermore, in a legal context, when the comparison in not legal, then the document's copyright has been infringed.

Initiallv, let the coordinates be (u, v), we can define r_i as: $(\pm\sqrt{u^2 + v^2})$ The g^* expression is:

$$g^*(u, v) = \left(\frac{u}{\sqrt{u^2+v^2}}, \frac{v}{\sqrt{u^2+v^2}}, z\right) \quad (17)$$

With

$$z = r_i \frac{\propto(k-1) \pm \sqrt{k(k-2)((\propto^2)+r_i^2)}}{r_i^2 k(k-2) - \propto^2} \quad (18)$$

These equations allow us to pass from the 3D space to the image space and vice versa. However the values of the various parameters making up the model of the Poincaré disk are not known. A procedure is thus needed to calibrate the system and estimate the values of these parameters. This procedure is described by Comby in [36].

VI. CRYPTOGRAPHY METHODOLOGY

Nowadays, more and more digital images are transferred electronically. In this section, we outline an example of how our system of watermarking can be used to securely transfer medical images using cryptography.

Thus, our aim is that the encryption and watermarking features of images are inserted at the software level. As well as integrating with our watermarking algorithms, a software component can also access peer-to-peer systems as outlined in our paper dealing with distributed databases management [4]. This component will serve as a basis for encrypting medical images.

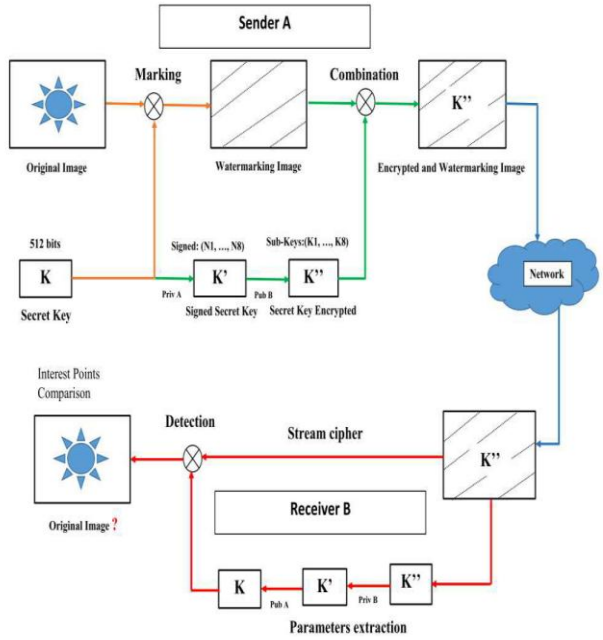

Figure 16: Public and secret key encryption combined with our watermarking.

We can, thus, say that security is not only assured for the transmission of medical images but also for the archiving of these images. The challenge regarding getting the encryption to work with the compression process remains.

Due to the coding process, the size of information (entropy) to be transmitted increases significantly between the original image and the coded image. In the particular case of certain types of medical images, large homogeneous zones appear. These zones can disrupt the efficiency of the encryption algorithms. Paradoxically these homogeneous zones are useless for diagnosis, can be safely used to label medical images for our watermarking algorithm.

Today when a doctor examines a patient he often needs to consult with another specialist before he can make a full diagnosis. Such consultation can be conducted electronically and the patient's images can be sent to the specialist electronically.

Algorithm 4: Combination of encryption and watermarking processes.

1 Function Encryption $(OrgImg, NameImg)$;
Input : Gets an original image and image name
Output: Gives an encrypted and watermarking image
2 $ImgOID = OrgImg.getOID(NameImg)$;
3 $SecretKeyA = OrgImg.Hash512(ImgOID)$;
4 $TabSignGen = Process.RandSign(secretKeyA.size())$;
5 $NbElmtSign = TabSignGen.getNb()$;
6 **for** $i \leftarrow 1$ ***to*** $NbElmtSign$ **do**
7 SubKey[i]=Process.SelectElmt();
8 **end**
9 $WimgM = Process.WaterMaking(OrgImg)$;
10 **for** $i \leftarrow 1$ ***to*** $NbElmtSign$ **do**
11 $Binder[i] = Node.Find(SubKey[i])$;
12 $Binder[i].get(Key, Value) = ProcessVCH.Store(SubKey[i], SecretKeyA, WimgM.Param[i])$;
13 $PublicKeyB[i] = Process.Publish(SubKey[i])$;
14 **end**
15 **return** $CrypImageWat$;

Data networks, however, are complex and open to potential wiretapping. This raises a real problem regarding the safety of the patient's images during data transmission. Ethically, transferring medical images under such risk is not advisable. The best type of protection for such a scenario is encryption.

Protecting information during its lifecycle can be categorized as follows: protecting the data while it is stored, handled and transferred by an information system. Other considerations include existing legislation, safety policies and protection mechanisms. These measures should be jointly considered for data security requirements according to CIA (Confidentiality, Availability and Integrity). Encryption algorithms can be separated according to several characteristics: the systems that use a secret key (symmetric systems) and those that use public/private keys (asymmetric systems) in [37] Symmetric systems are those that allow for encoding and decoding with the same key. In such a scenario, the data transmitter and the data receiver must have previously exchanged the secret key using a secure means of communication. Asymmetric systems allow for the mitigation of this exchange problem by using one key to encode, and another key to decode (Algorithm 5). In our case, we adopt a hybrid strategy, using concurrently the secret key encryption algorithm and a public key as explained in the following. Furthermore, we argue that our encryption algorithm satisfies the conditions of a stream cipher algorithm. Generally, stream cipher algorithms consist of two steps. The first step is the generation of a dynamic key, corresponding in our case to the use of a hash function (SHA512) parametrized by the image OID to generate the key K. The second step is the creation of an encryption function that is dependent on the dynamic key, corresponding in our case to the generation of sub-keys K_i (with $1 \leq i \leq 8$) resulting from a function f parametrized by the key K. To describe our encryption process (Algorithm 4), we must initially generate an identifier of 512 bits associated, for example, with the image name.

Consider this identifier, OID (Object IDentifier), as a private key called K, we associate the values of the image plan equation with the coordinates of the interest points. In parallel with running our watermarking algorithm (already described 5.4), we deconstruct, in a pseudo-random way, the key (K) of 512 bits into 8 parts of varying sizes indicated by: K = f(K 1 , K 2 , ..., K 8).

Algorithm 5: Combination of decryption and detection processes.

```
Function Decryption (CrypImageWat, SecretKeyB);
  Input  : Gets an encrypted and watermarking image + SecretKeyB
  Output: Image decryption and authentication verification
NbPublicSubKey = Process.getSubKeyNb();
if StreamCipher() = true then
    Process.ReverseTrans(ParamList);
    if Process.Compare(OrgImg) = true then
        return Sucess;
    else
        return Failure;
    end
else
    for i ← 1 to NbPublicSubKey do
        if Process.Lookup(SubKey[i]).contain(SecretKeyB) then
            Param[i] = Process.getParam(SuKey[i]);
            ParamList = Process.put(Param[i]);
        else
            Process.Write("SubKeynotvalid");
            continue;
        end
    end
    if ParamList.getNb() = NbPublicSubKey then
        Process.ReverseTrans(ParamList);
        if Process.Compare(OrgImg) = true then
            return Sucess;
        else
            return Failure;
        end
    else
        return Failure;
    end
end
```

The function f is a concatenation function of different sub-keys and the n-uplet (K_1, K_2, ..., K_8). Each sub-key K i has an associated number of bits N_i, the n-uplet (N_1, N_2, ..., N_8) constitutes our cryptographic signature. In this signature, every sub-key K_i ($1 \leq i \leq 8$) is associated with a parameter P_i of the watermarking. These sub-keys K i can be published on the network. We note that according to the model of data distribution in VCH (Virtual and Consistent Hyperbolic-Tree) [4], each sub-key allows for the calculation of node coordinates (data server) that store the private key K and other watermarking parameters (see Algorithm 4).

For the addressee who has the private key B, it is enough to find all sub-key K_i published for whom values contains his private key. Thus, the receiver of the image can reconstitute the image as they have all required parameters to apply the detection function 5.5 for verifying the image watermark. The Figure 16 illustrates this process, which is also described in Algorithm 5.

VII. RESULT AND DISCUSSION

In our crypto-watermarking approach, we propose a set of hybrid methods both for watermarking and for encrypting the image. In this section, we demonstrate the performance of our solution. We start by demonstrating that our encryption technique uses an asynchronous stream cipher methodology. Our encryption algorithm can be considered an asynchronous stream cipher because the function f, which generates the dynamic key, uses an OID parameter, which in turn is a series of previously encoded digits [38]. This type of encryption is also called a self-synchronising stream cipher. The distribution of the errors is limited to the size of the memory. Consequently, if some encoded text is erased or inserted, the receiver can re-synchronize with the sender through using memory. Regarding active attacks, if an active opponent modifies a part of the encoded text, the receiver can detect it. It is for these qualities that we have adopted such an approach. We shall now detail these aspects in a thorough analysis.

A very strong link exists between topology and surface geometry. Our hyperbolic tree topology associated with hyperbolic plan, is generalized by the hyperbolic space. We define our topological space by the couple (X, ρ), where X is the set of the our hyperbolic tree nodes and ρ is the family of nodes associated with the image pixels from our mathematical transformation. In this section, we present the robustness of our system using an hyperbolic tree topology based on chaos theory. Chaos theory is defined as being a dynamical system with complex, unpredictable behavior [39]. However, before we outline the proof, it should be noted that it is thanks to diverse topological definitions that we are allowed to build such an idea. We consider in our proof discreet dynamic systems.

Let f : X → X, an application of a topological or metric space X in itself.

We consider the continuation of iterations defined by the recurrence relation:

$$\begin{cases} x^0 \in X \\ \forall\, n \in N,\ x^{n+1} = f(x^n) \end{cases} \tag{19}$$

Definition VII.1. A discreet dynamic system is a couple (X, f) formed by:

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

In this context, the space of steps corresponds to the passage of the step image i into the step i + 1 once a pixel is modified. Function f is associated with the composition of two projection functions: a hyper-catadioptric projection and a stereographic projection respectively.

We define the notion of a reversible discrete dynamic system with reference to our reverse mathematical transformation.

Definition VII.2. A discrete dynamic system (X, f) is said to be reversible if f is a homeomorphism (topological), i.e. if f is a bijective, bicontinuous function.

In our case, hyper-catadioptric and stereographic projections are homeomorphic [40]. Consequently these two transformations are reversible as we have already shown in Section 5.5.

Furthermore, in topology, the concept of the density of subset A, of a topological space X that allows for the translation of the idea that: for any node of our hyperbolic tree called x of the set X, we can find a point A which is as close to x as we like [41].

Another aspect of importance in chaos theory is the notion of periodicity. Chaos theory posits that the behaviour of a discreet dynamic system $x_{n+1} = f(x^n)$ may or may not be planned, given we can estimate the course of a point x given during the transformation. The following definition is relative to this concept.

Definition VII.3. A point p ∈ X is considered periodic of period k if k is a non-null integer such as:

$$f^k(p) = p, et\ \forall\ h\ \in\ [0; k-1], f^h(p) \neq p$$

We shall note $Per_k(f)$ the k-periodic set of points *f*, and $Per_k(f)$ the set periodic points of any period.

Subsequently, we define the set elements which allow us to verify if our transformation function is chaotic. This relates to the properties of general dynamic systems, topological transitivity and of the sensitivity of the original conditions.

Definition VII.4. A discrete dynamical system (X, *f*) is said to be regular if all the periodic points of *f*, called Per(*f*), are dense in X.

In a metric space (X, d), the dynamic system (X, *f*) is regular if and only if:

$$\forall\ x\ \in X, \forall\ \varepsilon\ > 0, \exists\ p\ \in Perf(f), d(x,p) < \varepsilon$$

For all nodes of the hyperbolic tree which we take in our system, an image point, which minimizes the distance from node to image point exists.

Similarly, for any open couple U, V ⊂ X, there exists k > 0 such as $f^k(U) \cap V \neq \emptyset$ hen f is topologically transitive.

Definition VII.5. f has a sensitive dependence on the initial conditions if it exists δ > 0 such as, for all x ∈ X and for any neighborhood V of x, it exists y ∈ V and n ≥ 0 there such as $d(f^n(x), f^n(y)) > \delta$. δ is called constant of sensibility of *f*.

Definition VII.6. Now, we can give the definition of Devaney: 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 original conditions.

If our function of transformation f is chaotic, then the system (X, f) is chaotic, and, according to Devaney, it is unpredictable because of its sensitive dependence on the original conditions. It cannot be decomposed or simplified in two
sub-systems which do not interact, because of the topological transitivity.

Because the initial condition is based on the Harris' interest points detection method, we are assured that our watermarking approach is resistant to attacks in the following ways:

- Noise addition;
- Filtering;
- Compression with losses, essentially JPEG; 630
- Geometrical transformations.

Consequently, we show that our system protects the integrity and the confidentiality of images and in particular medical images.

VIII. CONCLUSION AND FUTURE WORK

In this paper, we have proposed a new watermarking and encryption technique for images based on properties of hyperbolic projective geometry. Our solution is a crypto-watermarking system, which applies syntactic and semantic hybrid watermarking to an image and integrates both symmetric and asymmetric cryptography.

It is based on the use of a hyperboloid mirror and a sensor in the shape of a Poincaré disk. We have formally described our model and have shown how to use a function with chaotic iteration allowing subspace-security [39, 42].

Our future work will consist of implementing every aspect of our solution and conducting a performance analysis between our solution and existing ones.

REFERENCES

1. B. Macq, P. R. Alface, M. Montanola, Applicability of watermarking for intellectual property rights protection in a 3d printing scenario, in: Proceedings of the 20th International Conference on 3D Web Technology, 2015, pp. 89–95. doi:10.1145/2775292.2775313.
2. Y. Z., L. L., Digital image watermarking algorithms based on dual transform domain and self-recovery, International Journal on Smart Sensing and Intelligence Systems 8 (1) (2015) 199–219.
3. D. X., W. F., W. Y., F. Duan, C. L., W. H., Self-calibration of hybrid central catadioptric and perspective cameras, Computer Vision and Image Understanding 116 (6) (2012) 715–729.
4. T. T., M. D., Virtual and consistent hyperbolic tree: A new structure for distributed database management, in: 3rd International Conference on Networked Systems, Lecture Notes in Computer Science vol. 9466, 2015.
5. M. M., T. K., A cryptographic method for secure watermark detection, in: Information Hiding, Lecture Notes in Computer Science vol. 4473, 2006, pp. 26–41.
6. K. M., K. V., A survey on digital image watermarking and its techniques, International Journal of Signal Processing, Image Processing and Pattern Recognition 8 (5) (2015) 145–150.
7. C. G., S. R., Y. K. R., Classification of watermarking based upon various parameters, International Journal of Computer Applications & Information Technology 1 (2) (2012) 16–19.
8. Y. U., S. J.P., S. D., S. P.K., Different watermarking techniques & its applications: A review, International Journal of Scientific & Engineering Research 5 (4) (2014) 1288–1294.
9. D. P., K. K., A study on spatial and transform domain watermarking techniques, International Journal of Computer Applications 71 (14) (2013) 38–41.
10. N. K.D., D. D.S., Performance comparison of two hybrid techniques for image steganography in frequency domain, International Journal of Inno- vative Research in Computer and Communication Engineering 3 (6) (2015) 68–74.
11. G. M., H. E.M., M. M., An improved image watermarking method in frequency domain, Journal of Applied Security Research 12 (2) (2017) 260–275.
12. A. Y.B., T. I., D. N., B. M.S., Euclidean distance distortion based robust and blind mesh watermarking, International Journal of Interactive Multi-media and Artificial Intelligence 4 (2) (2016) 46–51.
13. H. O., S. W.M., Y. B. A. B., A. M.A., Public watermarking scheme for 3d laser scanned archeological models, in: IEEE Symposium on Computers and Communications, 2012, pp. 382–389.
14. G.-J. L., K.-Y. Y., An improved double image digital watermarking scheme using the position property, Journal Multimedia Tools and Applications 74 (17) (2015) 7261–7283.
15. S. B., S. L., Efficient descriptor for full and partial shape matching, Journal of Multimedia Tools and Applications 75 (6) (2016) 2989–3011.
16. K. Wang, G. Lavoué, F. Denis, A. Baskurt, Hierarchical watermarking ofsemiregular meshes based on wavelet transform, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY 3 (4) (2008) 620–634.

17. S. S.S., Blind wavelet based watermarking technique for image authentication, International Journal of Advanced Research in Computer Science 6(1) (2015) 127–131.
18. W. Y.H., M. S.D., Data hiding technique using audio watermarking, International Journal Of Engineering And Computer Science 4 (3) (2015) 11109–11112.
19. A. N., T. H., Pde based scheme for multi-modal medical image watermarking, International Journal BioMedical Engineering 14 (2015) 108–126.
20. B. L., S. H.I., A. M.B., Enhanced watermarking scheme for 3d mesh models, in: 7th International Conference on Information Technology, 2015, pp. 612–619.
21. P. W., X. Hongling, W. L., S. Wenlong, Harris scale invariant corner detection algorithm based on the significant region, International Journal of Signal Processing, Image Processing and Pattern Recognition 9 (3) (2016) 413–420.
22. H.D., "Foundations of geometry,thesis in mathematics", in: The Open Court Publishing Company, Univerty of G¨ottingen, 1950, p. 105.
23. M. P., Premiers principes de la métagéométrie ou géométrie générale, Revue néo-scolastique. 3ème année 1896 (10) (1896) 143–170.
24. T. S., Hyperbolic geometry: history, models, and axioms, U.U.D.M. Project Report (2004).
25. B. Y., Hyperbolic geometry tiling (08 2006).
26. T. T., A. D., M. D., Reliable and scalable distributed hash tables harnessing hyperbolic coordinates, in: IFIP International Conference on New Technologies, Mobility and Security, 2012, pp. 1–6.
27. M. A., Un afficheur générique d'arbres à l'aide de la géométrie hyperbolique, Journées francophones des langages applicatifs (JFLA) (2000).
28. B. A. F., M. D., The hyperbolic metric and geometric function theory, in: International Workshop on Quasiconformal Mappings And Their Applications, 2006.
29. S. L. A catadioptric sensor withmultiple viewpoints, In Robotics and Autonomous Systems 51 (2005) 667–674.
30. B. S., N. S. K., A theory of single-viewpoint catadioptric image formation, International Journal of Computer Vision 35 (2) (1999) 1–22.
31. B. D. A., Geometry (06 2002).
32. M. J., Vision stéréoscopique par ordinateur pour la détection et le suivi de cibles pour une application automobile, Ph.D. thesis, Institut National Polytechnique de Grenoble (2008).
33. T. R., Suivi d'objet pour la television interactive, Ph.D. thesis, Ecole TELECOM ParisTech (2008).
34. P. P., De l'importance des points d'int´erˆet et du maillage 2d, Ph.D. thesis, Institut National Polytechnique de Toulouse (2009).
35. B. J.P., General central projection systems : Modeling, calibration and visual servoing, Ph.D. thesis, University of Coimbra (2003).
36. C. F., D. K. C. C., S. O., étalonnage de caméras catadioptriques hyper-boloïdes, Traitement du signal:Vision omnidirectionnelle 22 (5) (2005).
37. D. W., H. M.E., New directions in cryptography, IEEE Transactions on Information Theory 26 (6) (1976) 644–654.
38. J. D., P. K., The self-synchronizing stream cipher, Springer Lecture Notes in Computer Science 4986 (2008) 210–223.
39. D. R. L., An introduction to chaotic dynamical systems (04 1989).
40. B. I., V. P., G. J.-P., Continuous wavelet transform on the hyperboloid, Applied and Computational Harmonic Analysis 59 (2) (1975) 375–382.
41. S. L., Analyse: Topologie générale et analyse fonctionnelle, in: Hermann, 1970, p. 432.
42. J. Bahi, C. Guyeux, Hash functions using chaotic iterations, Journal of Algorithms and Computational Technology 4 (2) (2010) 167–181.

AUTHORS PROFILE

Telesphore Tiendrebeogo PhD and overlay network and assistant professor at Nazi Boni University. I have a master's degree in multimedia and real time system. My current research is on big data and image watermarking.

Cheick Yacouba Rachid Coulibaly I have a master's degree from Nazi Boni University in information systems and decision support systems. My interest research topic is image watermarking for decision support and geolocation system.

Maliki Badolo I have a master's degree in information systems and decision support systems. My interest research topic is image watermarking for decision support and multimedia system.