A Watermarking Scheme for 3D Objects that is Robust to Molding and Casting Duplication

Hiroshi Yamamoto
School of Information and Telecommunication Engineering, Tokai University,
2–3–23 Takanawa Minato-ku, Tokyo, Japan

Abstract— *In recent years, low-cost 3D printing has rapidly spread among general consumers. On the other hand, like the distribution of other forms of digital content, the fact that once an adversary obtains the data, he can produce any number of reproductions has been pointed out as one of the critical issues confronting 3D printing. There is existing research in which cavities that express embedded information are made in the interior of 3D objects. This method aims at embedding information into a legitimately created object, however, it is not robust against an attack where an adversary obtains the external shape of the object by 3D scanning and reproduces the object, or an attack where an adversary simply makes a mold of the object and produces copies by casting. In this paper, we propose a scheme whereby information is embedded into the external shapes of objects. If information is embedded into 3D objects by the proposed scheme, attackers cannot change the information without changing the external shapes of the objects when they make copies of the original 3D objects. In the proposed scheme, we define the pseudo rotation axis for a 3D object and slice planes that are orthogonal to the axis, and then we embed information into the maximum values of the radii of the cross sections. We conduct experiments in which an actual 3D object is made and into which information is embedded using the proposed method and extracting the information from only the object without any metadata. We show that transmission of information with only the printed 3D object is possible using the proposed scheme.*

Keywords: 3D Printing, Digital watermarking, External shape

1. Introduction

The spread of low-cost 3D printers using fused deposition modeling (FDM) technology has led the general public becoming familiar with 3D printing. In relation to digital content, there is a common problem that if appropriate copyright protection was not applied, an adversary could reproduce a large number of copies easily. It is expected that such problems will also become serious in relation to 3D printing.

There is existing research about copyright protection technology for 3D models. In [1], a method of embedding information into 3D polygonal models of geometry is proposed. The aim of the method is to protect original 3D data and is effective for this purpose. However in the most frequently used ways of making inexpensive reproductions of 3D objects, an adversary obtains the external shape of an object by measuring or making a mold and producing copies of it. Protection using internal data such as a polygonal model does not work effectively because the adversary ignores the internal data expression in this type of attack. To counter this, information has to be embedded into the output of 3D printing, not in the internal data expression. In [2], a method of embedding information into outputs of 3D printing is proposed. Here, cavities are constructed in advance to systematically express information embedded in the interior of a 3D object. The information is extracted by heating the object and then observing the thermographic images of the object to estimate the positions of the cavities in the interior of the object. It is assumed that the object is created legitimately by means of this method. The method is a scheme by which the embedded information can be extracted when legitimately created objects are observed. If the purpose of an adversary is just to copy the external shape of an object, he can do this by measuring or making a mold and making copies of it. Cavities in the interior of the original object are eliminated by this method, therefore the information embedded in the object is lost.

In this paper, we focus on the fact that what adversaries want is the external shape of the object and propose a scheme whereby information is embedded into the external shapes of the objects themselvs. Using the proposed scheme, when an adversary wants to alter or delete the information embedded in an object, the adversary has to change the external shape of the object. Because this is an action that frustrates the aim of the adversary, the proposed scheme is expected to act as a deterrent to those who wish to eliminate embedded information. We describe in detail an embedding procedure and extracting procedure that enable us to transmit information through only the external shape of the 3D object. We conduct experiments to make 3D objects in which information is embedded according to the proposed scheme using an FDM 3D printer and to extract the embedded information by gauging the feature quantities with photographs of the objects.

The proposed scheme is a method in which the external shapes of objects are slightly changed like digital watermarking of 2D images, therefore, there is a trade-off among

ISBN: 1-60132-466-9, CSREA Press ©

reducing the deformation caused by the embedding of information, increasing the amount of information embedded, and increasing robustness against distortion. We also discuss the implications of this trade-off.

2. Proposed scheme

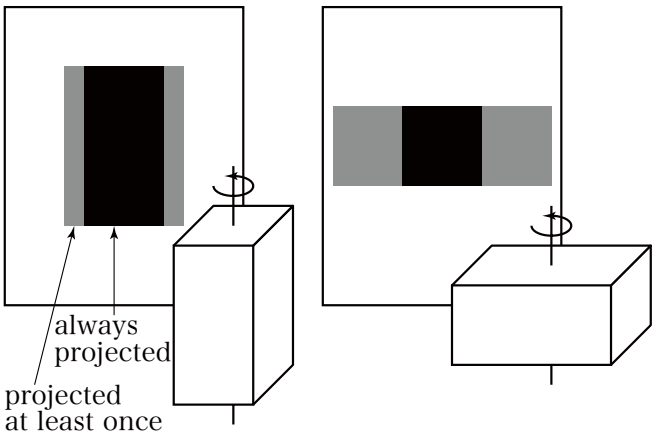
It is an important problem how to define the feature quantities of a 3D object without extra metadata such as the position and direction of the coordinate system with which the object should be observed. We explain the definition of feature quantities we used and then describe the embedding and extracting procedure.

2.1 Feature quantities

Suppose that A embeds information into a 3D object and B extracts the information from it. It is assumed that B knows the procedure that A used to embed information in advance. This is not metadata because the negotiation occurs prior to transmissions and the knowledge of the embedding procedure is independent for each particular transmission. One of the most important problems is how B observes the 3D object with the same coordinate system as A does. Using metadata, such as which direction of the object is the upward direction, B can observe with the same coordinate system as A does but metadata that is extra information ancillary to the object has to be transmitted with the object. Metadata also become the target of attacks and are easily removed by attackers. In this paper, because we consider attacks by molding and casting reproductions, methods using metadata cannot be adopted.

We consider information transmission that uses only the printed object without any metadata ancillary to it. The volume of objects and their maximum outer length are values that are independent of the direction of observation. A method in which information is embedded into the value for volume or the maximum outer length is possible but it is impractical because the magnitude of the carrier signal is too small to embed a certain amount of data. The proposed method embeds information into external shapes in specific multiple positions of the object in order to embed a greater amount of information. Therefore, it is critically important for the positions of embedding to be shared between A and B.

First of all, we define the pseudo rotation axis of 3D objects, which are defined only by the external shape of the object, in order to share the coordination system for observation of the object by A and B. Intuitively, the pseudo rotation axis is the axis of revolution when the 3D object is approximated as a solid of revolution. Consider that we choose an axis for a 3D object and rotate the object around the axis. The area of images on a projection plane that is parallel to the axis by parallel projection may vary with the rotation (Fig. 1). We call the ratio of the minimum value of the area of images to the maximum value of the aria



a. small ratio of change b. large ratio of change

Fig. 1: Variation of projection area

of images the ratio of change for the axis. The maximum value of the ratio of change for an axis is 1. If the object is a solid of revolution and the axis corresponds to the axis of revolution, the ratio of change for the axis is 1.

Definition 1: Pseudo rotation axis
We call the axis for which the ratio of change is the maximum the pseudo rotation axis of the object.

In this definition, the pseudo rotation axis of a sold of revolution corresponds to the axis of revolution. There exist objects for which a unique pseudo rotation axis cannot be defined, such as spheres or cubes. In many cases, objects that have more than one pseudo rotation axis are highly symmetric geometric solid figures, therefore, we think these objects rarely cause copyright problems and don't consider them in this paper.

We assume that A and B define the identical pseudo rotation axis about a 3D object. A and B define the z axis of the coordinate system to observe the object as the pseudo rotation axis. Let l be the length between both ends of points in the intersection of the z axis with the object. We call l the axis length of the object. A and B independently place one end of the points in the intersection of the z axis with the object on the point $(x, y, z) = (0, 0, 0)$ and the other end on the point $(x, y, z) = (0, 0, l)$. At this point, A and B may place the object in the opposite direction. A and B slice the object by $2n + 1$ planes that are orthogonal to the z axis between the plane $z = 0$ and the plane $z = l$ at even intervals (Fig. 2). We call the plane $z = \frac{il}{2(n+1)}$ the i-th cut plane.

Consider the cross section of the object on the i-th cut plane ($i = 1, 2, \ldots, 2n + 1$). We call the maximum value among the distance from the z axis to points in the cross section the pseudo radius in the i-th cut plane. We denote the pseudo radius in the i-th cut plane by r_i. We assume that A and B use an identical pseudo rotation axis, but they may observe the object in the opposite direction. In this case,

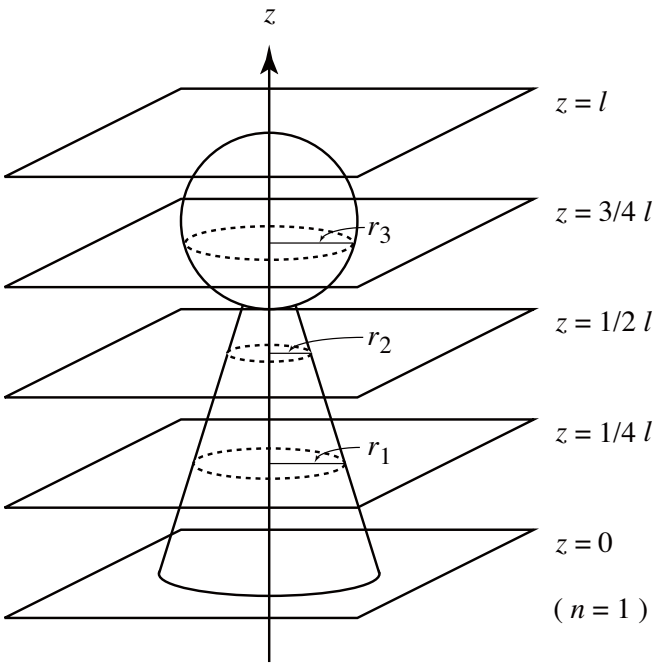


Fig. 2: The z axis and cut planes

r_1 and r_{2n+1}, r_2 and r_{2n}, ..., r_n and r_{n+2} are exchanged between A and B and this case must be considered. In order not to depend on the direction of observation, we define the feature quantities $(f_1, f_2, \ldots, f_{n+1})$ of an object as follows:

- f_1: the ratio of r_{n+1} (the pseudo radius in the center cut plane) to l
- f_2: the ratio of max(r_n, r_{n+2}) (the larger value between the radii of the cut planes that are adjacent to the center cut plane) to l
- f_3: the ratio of max(r_{n-1}, r_{n+3}) to l
  $\vdots$
- f_{n+1}: the ratio of max(r_1, r_{2n+1}) to l

The reason we use the ratio to l is to ensure robustness against a scaling attack on the object.

2.2 Embedding

We assume that A and B agree about the embedding scheme and the following information:

- The number of slice planes is $2n + 1$
- The bit position to start embedding is s
- The number of bits to embed into each plane is k

We explain how the information is embedded by A. When A decides on an object into which embed information, A determines the pseudo rotation axis and the $2n+1$ cut planes. A measures the axis length l and pseudo radii r_i $(1 \leq i \leq 2n + 1)$, and then obtains the feature quantities f_j $(1 \leq j \leq n + 1)$. k [bit] information for each feature quantity f_j is embedded, therefore, the total amount of embedded information is $k(n + 1)$[bit].

First, we explain how to embed k[bit] information into f_1. f_1 is the ratio of the pseudo radius in the center cut plane r_{n+1} to the axis length l. Convert the value of f_1 into normalized floating-point binary notation. Let $b_1, b_2, \ldots$ be the binary notation of the significand of f_1. b_1 is the first bit of a non-zero binary significand and is always 1. When k bit is embedded from the s-th most significant bit, modified significand $b'_1, b'_2, \ldots$ are obtained by the following steps:

1) $b'_1, b'_2, \ldots, b'_{s-1}$ are not changed, $(b'_1 = b_1, b'_2 = b_2, \ldots b'_{s-1} = b_{s-1})$.
2) $b'_s, b'_{s+1}, \ldots, b'_{s+k-1}$ are assigned to k bits to be embedded.
3) b'_{s+k} is assigned to 1 and the succeeding bits $b'_{s+k+1}, b'_{s+k+2}, \ldots$ are assigned to 0s .

In the last step, $b'_{s+k}, b'_{s+k+1}, \ldots$ are assigned to $1000\cdots$. The purpose of this step is to assign the modified value at the median of the interval in which the s bits in embedded position become $b'_s, b'_{s+1}, \ldots, b'_{s+k-1}$. This procedure is shown in Fig. 3. In Fig. 3, the embedded bits are assumed to be "111". Replacing the significand $b_1, b_2, \ldots$ by $b'_1, b'_2, \ldots$,

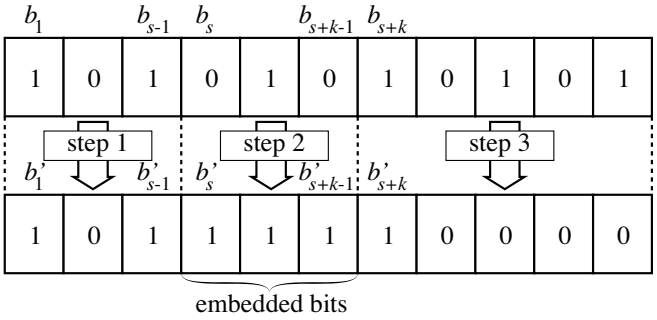


Fig. 3: Embedding into the significand

f'_1 that is the modified value of f_1 is obtained. Then A calculates $r'_1 = l f'_1$ and distorts the 3D object to make the pseudo radius in the center cut plane be r'_1.

Similarly, the rest of the information is embedded by modifying $f_2, f_3, \ldots, f_{n+1}$. These are the feature quantities of other cut planes. Only the maximum value of pseudo radii of cut planes that are symmetric about the center plane are used; embedding into the cut plane with a larger pseudo radius is enough. But in the case where embedding changes the plane with a larger pseudo radius, information must be embedded into the other plane too.

A makes 3D data in which $k(n + 1)$ bit information is embedded in this way and makes a 3D object by 3D printing.

2.3 Extraction

Next, we explain how B extracts information. Extraction is basically done by performing the embedding procedure in reverse. B observes the printed object and determines the pseudo rotation axis according to definition 1. B chooses a coordinate system and measures the axis length l. B

considers the $2n+1$ cut planes and measures the pseudo radius on each plane. B calculates the feature quantities and converts them into normalized floating-point binary notation. B obtains embedded bits by reading bits from s-th to the $s+k-1$-th position of the binary significand of each feature quantity.

2.4 Parameters and trade-off

Choice of parameters, the number of slice planes, $2n+1$, the bit position to start embedding, s, and the number of bits to embed into each plane, k, is important in terms of practical requirements. Choice of these parameters involves trade-offs among the degree of distortion of an object, the amount of information embedded, the probability of extraction failure, and robustness against distortion by attackers.

We summarize the mutual effects of these requirements.

Small degree of distortion is desirable

A small number of slice planes $2n+1$ or a large number of bit positions to start embedding s are required. But the smaller $2n+1$, the smaller the amount of information to be embedded. If s is large, then b'_{s+k-1}, the last bit position required to extract embedded information becomes a less significant bit. In this case we reduce the probability of successful extraction and robustness against distortion, or the value of k, the amount of information to be embedded.

Large amount of information to be embedded is desirable

A large number of slice planes $2n+1$ or, a small number of s and a large number of k are required. But the larger $2n+1$, the higher the probability of extraction failure. If s is small, the degree of distortion becomes large. If k is large, b'_{s+k-1} becomes a less significant bit. This decreases the probability of successful extraction and robustness against a distortion attack.

Low probability of extraction failure is desirable

If $s+k-1$ is large, the contribution of the least significant embedded bit b'_{s+k-1} to the external shape of the 3D object is small, therefore, the probability of extraction failure becomes large. It is necessary to keep $s+k-1$ small and this means s and k must also be kept small. Small s causes major distortion of embedded objects and small k reduces the amount of information to be embedded.

Robustness against distortion by attackers is desirable

If $s+k-1$ is large, the embedded information can be easily removed by making a small modification to the shape. The required condition of this case is the same as the previous item. Enhancement of robustness against a distortion attack causes an increase in the distortion of the object or a reduction in the amount of embedded information.

3. Experiments

We select the widely used STL format for 3D modeling. For simplicity, we use data of chess piece (pawn) (Fig. 4) that are a solid of revolution as an object of embedding. Parameters used in embedding are shown in the table 1. In this case, the amount of information that is embedded into the 3D object is $k(n+1)=4$ [bit]. Distortion of 3D data is done in ad-hoc manner. We edited an STL file to exchange and add polygons in order to change the external shape into a shape with feature quantities $(f'_1, f'_2, \ldots, f'_{n+1})$.

Fig. 4: Original pawn data

Table 1: Parameters used in experiments

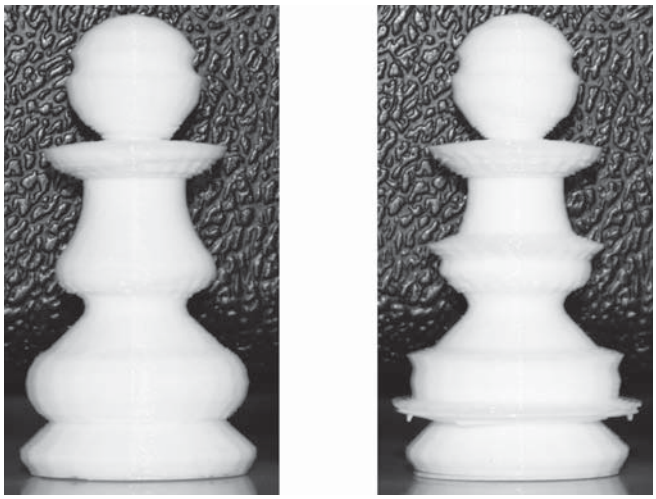
Description	parameter	value
The number of slice planes	$2n+1$	7
The bit position to start embedding	s	3
The number of bits to embed into each plane	k	1

3D printing was done using a Value 3D MagiX MH-500 (MUTOH INDUSTRIES, LTD), which is a low-cost FDM 3D printer. 3D objects that are distorted by embedded data are printed.

Extraction is done by measuring the photo image pixels of a printed object of an STL file that is distorted by embedding data.

4. Results

We printed the original 3D object and a distorted object in which 4bit data "1111" are embedded. The pictures of the objects are shown in Fig. 5. The left object labeled a. is the original 3D object and the right object labeled b. is the object in which information "1111" is embedded. The axis length l of the object a. in Fig. 5 measured using a Vernier micrometer was 63.0 [mm] and the axis length l of



a. output of original data

b. output of watermarked data

Fig. 5: Output of original data and output of watermarked data

the object b. was 63.1 [mm]. The reason for the difference in l is considered to be due to insufficient precision of FDM 3D printer.

The main purpose of this paper is to demonstrate that transmission of information using only a printed 3D object without any metadata is possible. We chose experiment parameters that guaranteed the correct extraction of information. Therefore, we chose relatively small s and k that are not suitable for practical use. We can see a marked difference between Fig. 5-a. and Fig. 5-b.

Extraction experiments were performed by 3 test subjects. Subjects took photographs and examined pixel images. They calculated feature quantities $(f'_1, f'_2, \dots f'_4)$ from the pixel distance of r_is and l. They converted $(f'_1, f'_2, \dots f'_4)$ into normalized floating-point binary notation and extracted the embedded bit from the third bit of each significand of the floating-point binary notation. All the test subjects succeeded in extracting the correct 4bit data "1111".

5. Conclusions and future work

We proposed a scheme that allowed information to be embedded into the external shape of objects. We conducted experiments in which information was embedded into a 3D object. We made watermarked objects by FDM 3D printing and extracted the embedded information by measuring pixel images of the objects. It was shown that transmission of information using only a printed 3D object without any metadata is possible. The proposed scheme has an advantage in that attackers cannot change the information embedded in the object without changing the external shape of the object. What adversaries want is to be able to copy the external shape; therefore, the proposed scheme is expected to be effective as a deterrent.

The main purpose of experiments described in this paper was to demonstrate that transmission of information without any metadata is possible. We selected parameters, the number of slice planes $(2n + 1)$, the bit position to start embedding (s), and the number of bits to embed into each plane (k) to be values that ensure the successful extraction of embedded information. Therefore, the amount of information embedded was small and the watermarked object had marked deformation. We are planning to conduct experiments to find the optimal parameters in terms of the trade-off among the degree of object distortion, the amount of information embedded, the probability of extraction failure, and robustness against distortion by attackers. Using large $2n + 1$ and k allows a large amount of information to be embedded but requires high precision for making and measuring the objects. Using small s reduces the deformation of watermarked objects. This also requires high precision when making and measuring objects.

We defined the feature quantities using maximum pseudo radii in two cut planes that are symmetric with respect to the center cut plane and consequently we used $n+1$ feature quantity values. By defining the direction of the pseudo rotation axis, for example, using the distribution of pseudo radii in cut planes, we can use $2n+1$ feature quantity values. Therefore we can embed $k(2n+1)$[bit] information instead of $k(n+1)$.

In the experiments in this paper, distortion of 3D data was done in an ad-hoc process where only required parts were distorted. Therefore, watermarked objects had artificial deformation. We are studying the process of deformation in which the rate of variability is changed smoothly to produce natural watermarked objects. Applying a technique of error-correcting code in the embedding process to obtain less notable deformation is a problem to be solved in the future.

References

[1] Ryutarou Ohbuchi, Hiroshi Masuda, and Masaki Aono, "Watermarking Three-Dimensional Polygonal Models Through Geometric and Topological Modifications," IEEE Journal on selected areas in communications, vol. 16, No.4, May 1998

[2] M. Suzuki, P. Silapasuphakornwong, K. Uehira, Y. Takashima, H. Unno, "Technique to Protect Copyright of Digital Data for 3-D Printing," 2015 Symposium on Cryptography and Information Security, 1B2-1, 2015 (in Japanese)