Copyright Protection for 3D Printing by Embedding Information Inside Real Fabricated Objects

Masahiro Suzuki[1], Piyarat Silapasuphakornwong[1], Kazutake Uehira[1], Hiroshi Unno[1] and Youichi Takashima[2]
[1]*Kanagawa Institute of Technology, 1030 Shimo-ogino, Atsugi, Japan*
[2]*Nippon Telegraph & Telephone Corp. Service Evolution Laboratories, 1-1 Hikarinooka, Yokosuka, Japan*

Keywords: Digital Fabrication, 3D Printer, Copyright Protection.

Abstract: This paper proposes a technique that can protect the copyrights of digital content for 3D printers. It embeds the information on copyrights inside real objects fabricated with 3D printers by forming a fine structure inside the objects as a watermark. Information on copyrights is included in the content before data are input into the 3D printer. This paper also presents a technique that can non-destructively read out information from inside real objects by using thermography. We conducted experiments where we structured fine cavities inside the objects by disposition, which expressed binary code depending on whether or not the code was at a designated position. The results obtained from the experiments demonstrated that binary code could be read out successfully when we used micro-cavities with a horizontal size of 2 x 2 mm, and character information using ASCCI code could be embedded and read out correctly. These results demonstrated the feasibility of the technique we propose.

1 INTRODUCTION

Digital fabrication technologies are attracting a great deal of attention because they offer the possibility of changing the system of manufacturing and logistics ((B. Berman, 2012), (B. Garrett, 2014)). Compact low-cost 3D printers have recently been produced and become easier for everyone to obtain. Their use is expected to become widespread by the general public. People are expected to have such digital fabrication equipment at home in the future, purchase the digital content of objects they want to produce from Web sites, and then download the content and manufacture objects at home with 3D printers instead of purchasing real objects from shops.

Although the final products are real objects in such cases, the digital data have value, not the real objects. Therefore, consumer pay for digital data and not real objects that are final products because once consumers obtain digital data, they can produce any number of final product themselves.

As businesses where consumers purchase digital data for 3D printers to produce real objects at home become more widespread, the problem of illegal copies of digital data will become serious because digital data are easy to copy. This problem did not exist when consumers purchased real objects from stores and it is exclusive to selling digital content for real objects produced by 3D printers. Copyrights for digital content and digital watermarking have been developed ((I. J. Cox et al., 1997), (M. D. Swanson et al., 1998), (M. Hartung et al., 1999)) as technologies to protect them. Moreover, digital watermarking for 3D content has also been developed ((P. R. Alface and B. Macq , 2007) (Q.S. Ai, et al., 2009)). However, conventional digital watermarking technologies cannot be applied to cases where real objects are produced from digital content by consumers because digital watermarking is only read out from digital content and after real objects are produced, it cannot be read out.

Here, we propose a technique that can protect the copyrights of digital content for homemade products using digital fabrication technologies such as those in 3D printers. It embeds information on copyrights inside real objects produced by 3D printers by using fine structures inside the objects that cannot be

Suzuki M., Silapasuphakornwong P., Uehira K., Unno H. and Takashima Y..
Copyright Protection for 3D Printing by Embedding Information Inside Real Fabricated Objects.
DOI: 10.5220/0005342401800185
In *Proceedings of the 10th International Conference on Computer Vision Theory and Applications* (VISAPP-2015), pages 180-185
ISBN: 978-989-758-091-8

observed from the outside. We also propose a technique that can non-destructively read out information from inside real objects using thermography. We conducted experiments to confirm the feasibility of the proposed technique. This paper also presents the results we obtained from the experiments.

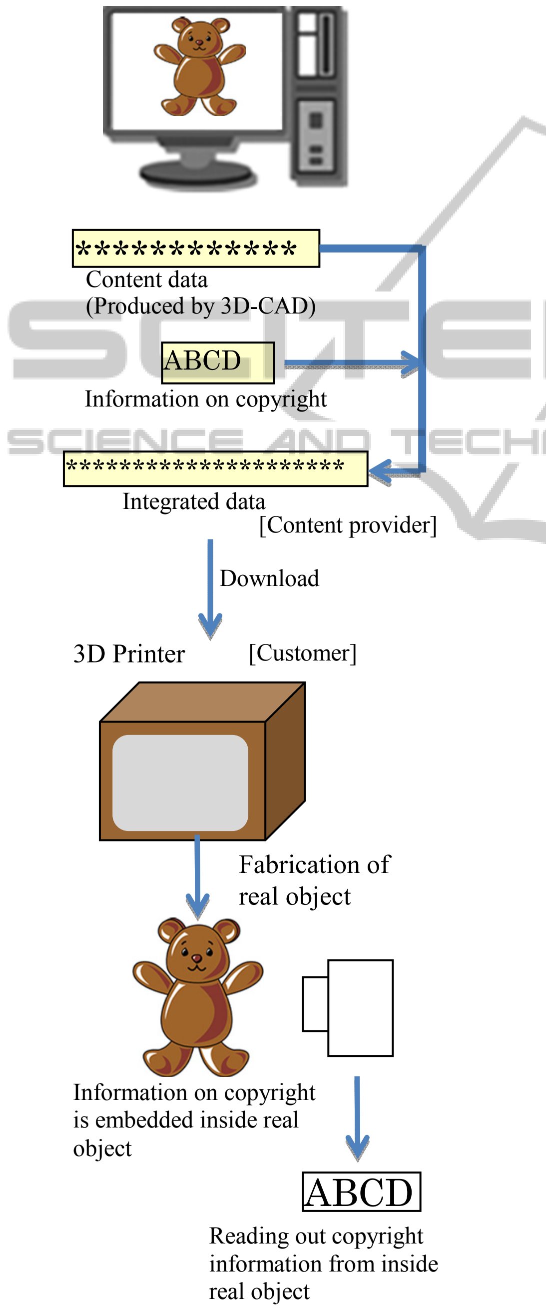


Figure 1: Basic concept underlying proposed technique.

2 PROPOSED TECHNIQUE

2.1 Basic Concept

Figure 1 outlines the basic concept underlying the technique we propose. After content data are produced using 3D-CAD or 3D-CG tools, the data for information on copyright are integrated with the content data by a content provider. A customer purchases the integrated data by downloading them and inputs them into a 3D printer to produce an object. The real object is basically formed using the content data; however, fine structures are simultaneously formed inside the real object during its fabrication. These structures express the information on copyright. The structures are non-destructively analyzed from the outside and information that the structures express is decoded, i.e., embedded information is read out.

Therefore, if the content provider finds a real object and is suspicious that it has been illegally produced, he/she can check this by using the method mentioned above. This has an effect of restraining illegal copies or production. The restraining effect we are expecting is the same as that of conventional digital watermarking. Here, illegal production means more products than those permitted for the content that is purchased, in addition to production using content that is illegally copied.

2.2 Embedding Information with Fine Structures inside Objects

The easiest and simplest way of expressing information is by using fine structures inside objects to form character shaped structures. However, this is also easy for people to observe who are trying to illegally produce objects. Another way is to form code that is encoded from character information. Figure 2 has a simple example of this method. An object produced by a 3D printer contains fine

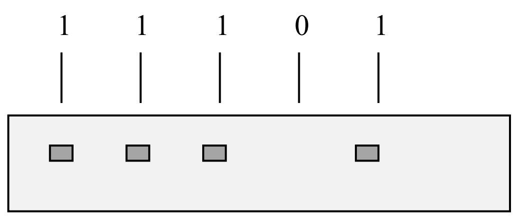


Figure 2: Example representation of binary code by using fine structure inside real object. Hatched areas are fine domains whose physical characteristics differ from other areas.

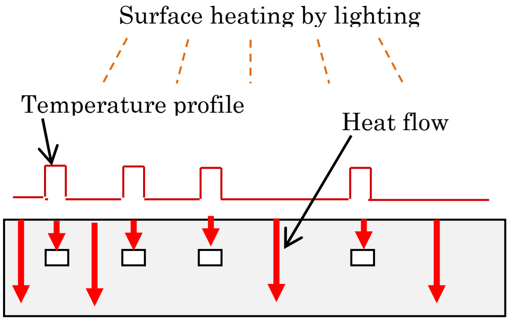


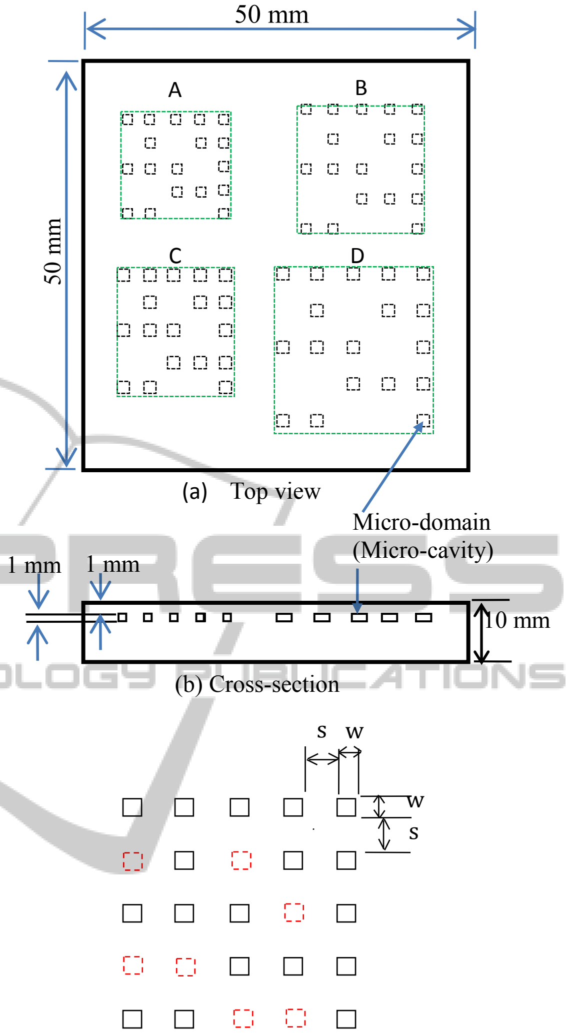
Figure 3: Example representation of binary code by structuring fine domain inside real object.

domains whose physical characteristics such as optical, acoustic, or heat conduction differ from the body of the object. The disposition of the fine domain expresses this information. Although there are various ways of expressing information due to the disposition of the fine domain, one example is where binary data, “1” or “0”, are expressed due to the existence or non-existence of the fine domain in a designated position, as shown in Fig. 2. Therefore, we can expect to read out these embedded binary data using X-rays or ultrasonic waves if we know the disposition of the fine domain from the outside of the real object by utilizing the difference in physical characteristics between the fine domain and the body material of the object.

We formed small cavities as fine domains in this study to structure the inside of a real object and embed information on copyright in it. Since there was no material in the cavities, their physical characteristics were different from those of other areas where material was filling up.

2.3 Reading out Information

We propose a method of thermography to read out embedded information. Figure 3 outlines the principles behind reading out binary code using thermography. First, the temperature of the surface of the object rises by heating. This results in heat conduction from the surface to the inside of the object. However, heat conduction is blocked by small cavities because their heat conductivity is very low. This causes the temperature of the surface area under the cavities to increase and such areas become slightly higher than the other areas, as shown in Fig. 3. Therefore, if we obtain the temperature profile of the surface of the object using thermography, we expect to know the disposition of the fine domain, i.e., it enables us to read out the binary data embedded in the real object.



	W	S
Group A	1	1
B	1	2
C	2	1
D	2	2

(mm)

(c) Possible positions of cavity and size parameters. Dashed lines indicate positions where there are no cavities

Figure 4: Sample used in experiment (Sample 1).

3 EXPERIMENTS

We evaluated the feasibility of this method that used thermography to analyze the distribution of fine cavities and read out character information by decoding binary code. Figure 4 has an example of the sample (Sample 1) we used in an experiment.

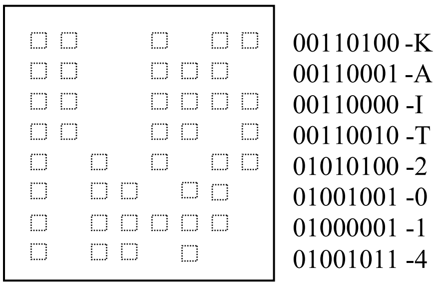


Figure 5: Sample used in experiment (Sample 2).

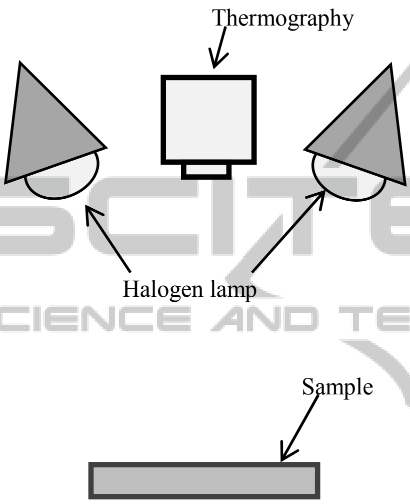


Figure 6: Configuration for experiment.

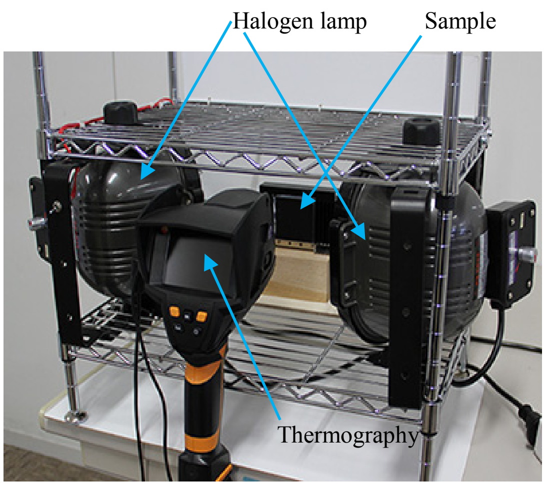


Figure 7: Photograph of experimental system.

We produced it with a stereolithographic 3D printer and polylactide (PLA) resin was used as the material for the sample, which was 5 x 5 x 1 cm. The sizes of the cavities and spaces between them were changed as experimental parameters, as listed in Fig. 4 (c). They were formed at positions at a depth of 1 mm from the surface.

We also prepared a sample in which the character information was embedded by disposition of the cavities which expressed the American Standard Code for Information Interchange (ASCII) code for the characters (Sample 2). Figure 5 has an example of Sample 2. The size parameters were the same as those for Group D of Sample 1. Although Figure 5 only shows the top view, the vertical sizes of the sample and the cavities are also the same as those of Sample 1. We assigned “0” to positions where there were cavities and “1” where there were no cavities. The disposition of these cavities expressed ASCCI code for eight characters – KAIT2014.

Figure 6 illustrates the experimental system. We used two 500-W halogen lamps to heat the object surface. The lamps were placed at a distance of 10 cm from the sample. Thermography that had a resolution of 160 x120 pixels was used to capture a thermal image on the surface of an object. The temperature resolution of thermography was 0.1 degree. Figure 7 has a photograph of the experimental system.

We read out the arrangement of cavities as follows. Since we knew the possible positions of cavities in advance, we checked whether there were cavities or not at all possible positions by comparing the temperature of the surface area above possible positions and that of peripheral areas where there were no cavities, i.e., we determined this depending on if the difference in temperature was larger than a threshold value or not.

4 RESULTS AND DISCUSSION

Figure 8 has an image captured with thermography for Sample 1. This image was one captured 10 s after heating started. It can be seen from Fig. 8 that the temperature of the surface area above the cavities is higher than that of the other areas regardless of the space length between adjacent cavities. Figure 9 has the results for determining the existence of cavities at possible positions for the 2 x 2 mm cavities. It can be seen that it is possible to correctly determine cavities for all the positions.

We can only see slight differences in temperature for the surface area above cavities that are 1 x 1mm. These differences were too small to enable the embedded information to be read out correctly. The reason we could not see the difference in temperature for 1 x 1 mm cavities was because heat

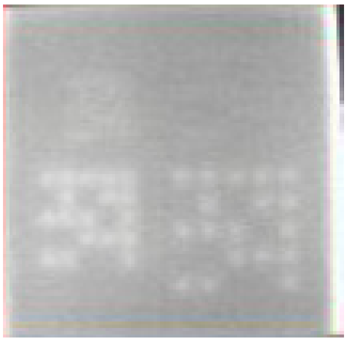


Figure 8: Image captured with thermography for Sample 1.

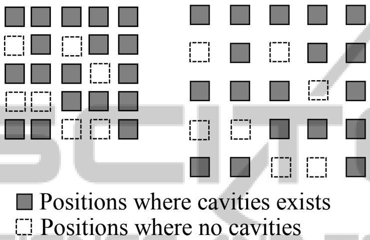


Figure 9: Results for existence of fine cavities for Sample 1.

not only diffused straight down, but diffused in all directions depending on the temperature gradient. However, we still have the possibility of detecting cavities to enhance the resolution of the temperature of the thermal image of the object surface.

Figure 10 has an image captured with thermography for Sample 2. Figure 11 has the results to determine the existence of cavities at possible positions and it also reveals the characters decoded from the ASCCI code. It can be seen from Figs. 10 and 11 that embedded character information (KAIT2014) can be read out correctly. These results demonstrate the feasibility of our proposed technique.

5 CONCLUSIONS

We proposed a technique that could protect the copyright of digital content for digital fabrication technologies such as 3D printers. It embeds information on copyrights inside real objects produced by 3D printers by using fine structures inside objects. We also proposed a technique that can non-destructively read out information from inside real objects using thermography. We conducted experiments where we used fine cavities to express binary information depending on whether it existed or not at designated positions. The results

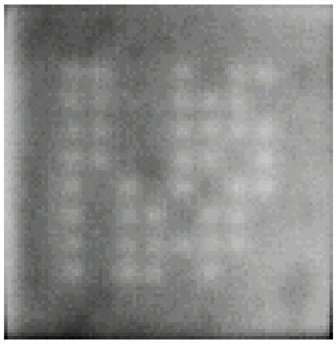


Figure 10: Image captured with thermography for Sample 2.

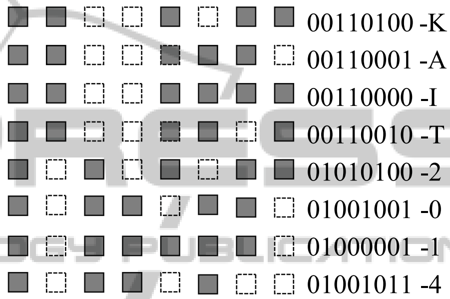


Figure 11: Results for existence of fine cavities for Sample 1.

from the experiments demonstrated that binary code could be read out successfully when we used fine cavities with a horizontal size of 2 x 2 mm and character information using ASCCI code could be embedded and read out correctly. These results demonstrate the feasibility of the technique we propose.

We intend to test materials other than PLA resin in future work; especially material that has high heat conductivity. We will also try to make embedded information more invisible both as digital content data and in real objects.

REFERENCES

B. Berman, 2012. 3-D printing: The new industrial revolution. Business Horizons*,* 55 (2): 155–162.

B. Garrett, 2014. 3D Printing: New Economic Paradigms and Strategic Shifts. Global Policy, 5(1): 70–75.

I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, 1997. Secure spread spectrum watermarking for multimedia, *IEEE Trans. Image Process*., 6 (12): 1673–1687.

M. D. Swanson, M. D. Swanson, M. Kobayashi, and A.H. Tewfik, 1998. Multimedia data-embedding and watermarking technologies, *Proc. IEEE*, 86 (6): 1064–1087.

M. Hartung and M. Kutter, 1999. Multimedia watermarking techniques, *Proc. IEEE*, 87 (7): 1079–1107.

P. R. Alface and B. Macq , 2007. From 3D Mesh Data Hiding to 3D Shape Blind and Robust Watermarking: A Survey, Transactions on Data Hiding and Multimedia Security II: Lecture Notes in Computer Science, 4499: 91–115.

Q.S. Ai, Q. Liu, Z.D. Zhou, L. Yang, and S.Q. Xie, 2009. A new digital watermarking scheme for 3D triangular mesh models, Signal Processing, 89 (11): 2159–2170.