Content Protection
Project Introduction

2022학년도 2학기
Suk-Hwan Lee

Artificial Intelligence

Creating the Future

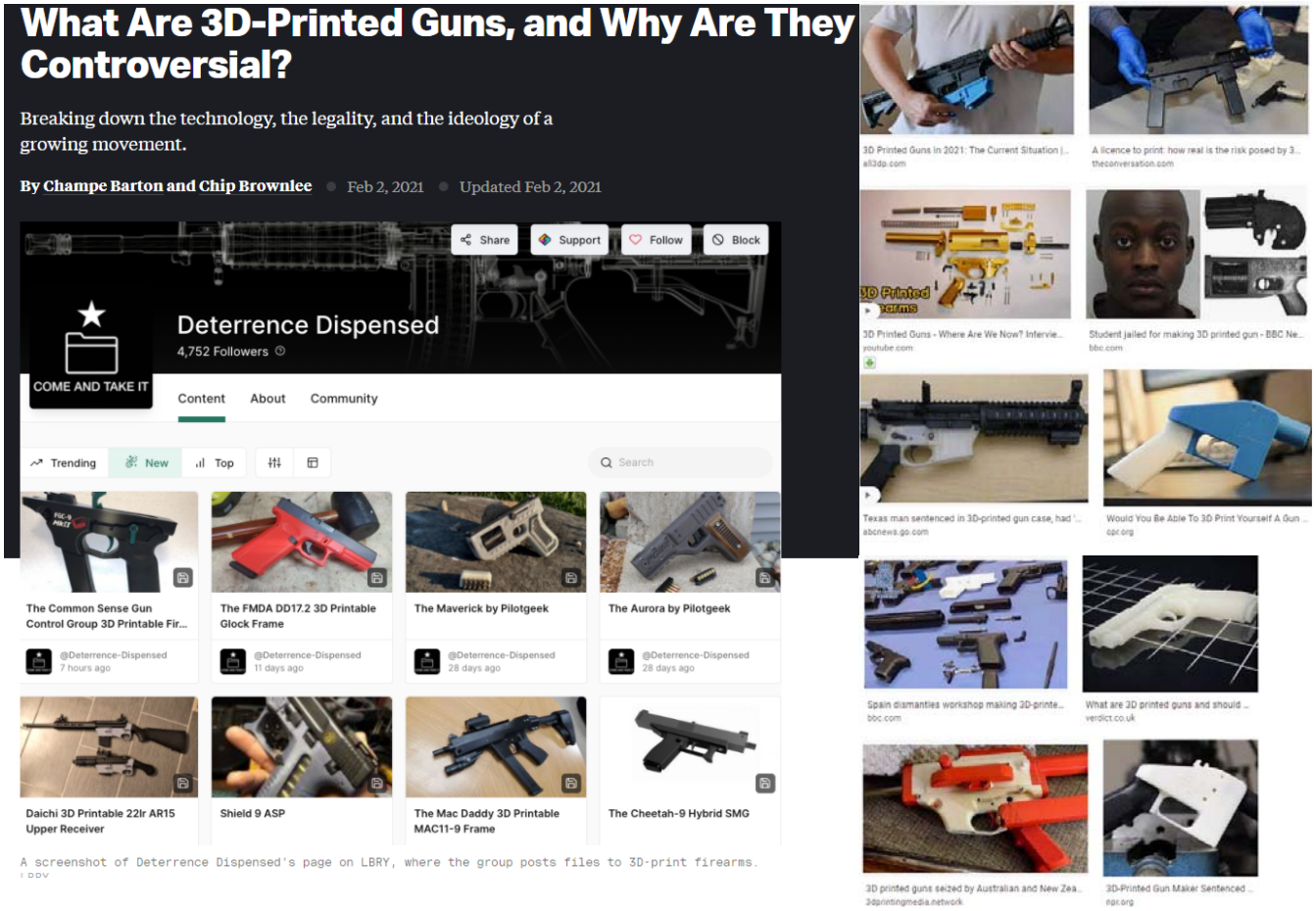
Dong-A University

Division of Computer Engineering &
Artificial Intelligence

1 Secure 3D Printing Informatics (2016~2019)

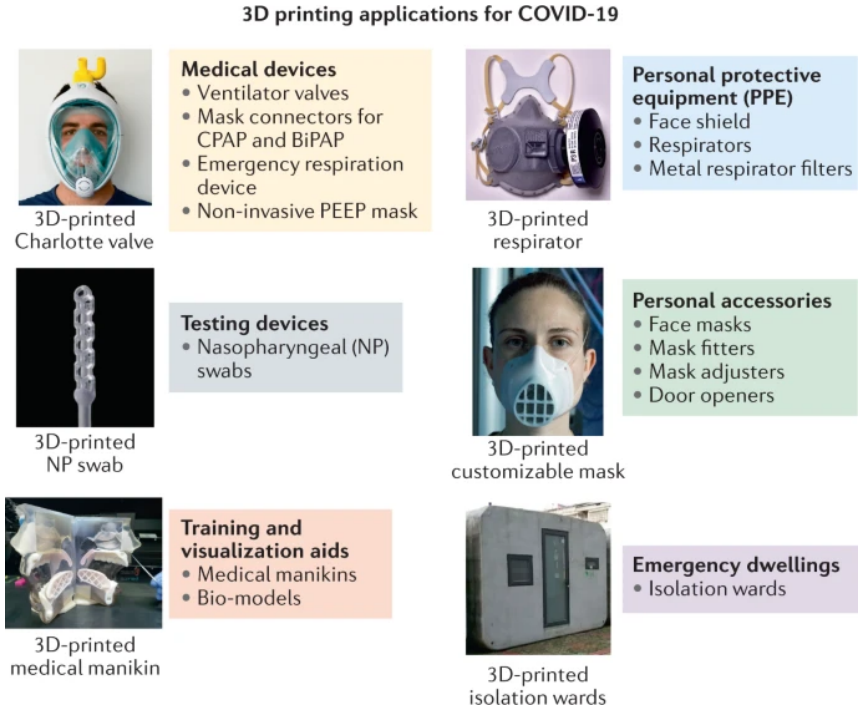
3D 프린팅 기술의 문제점

- 불법 총기 3D 프린터물



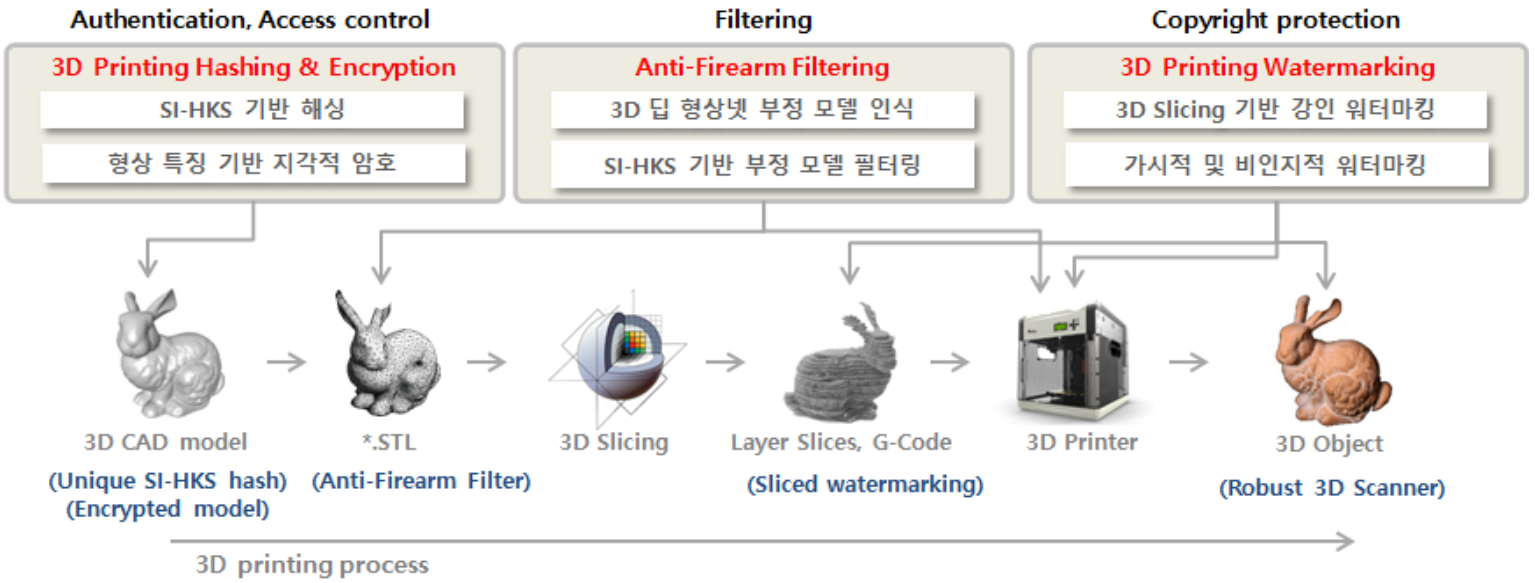
A screenshot of Deterrence Dispensed's page on LBRY, where the group posts files to 3D-print firearms.

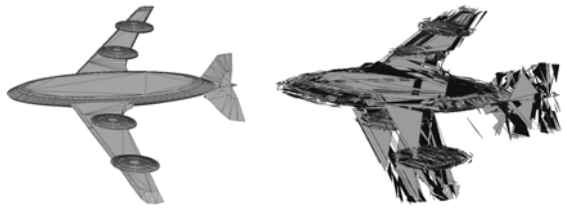
- 3D 프린터물 저작권



1 Secure 3D Printing Informatics (2016~2019)

3D 프린터의 부정 모델 필터링 및 보안 기술
(Illegal Model Filtering and Security for 3D Printer)



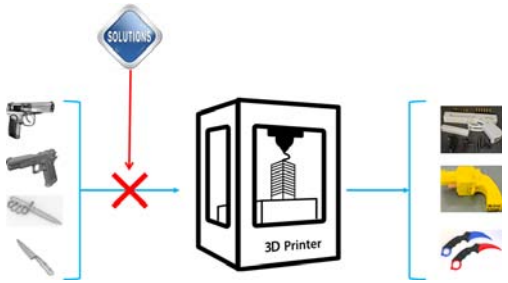


원 모델 가시적 암호화된 모델

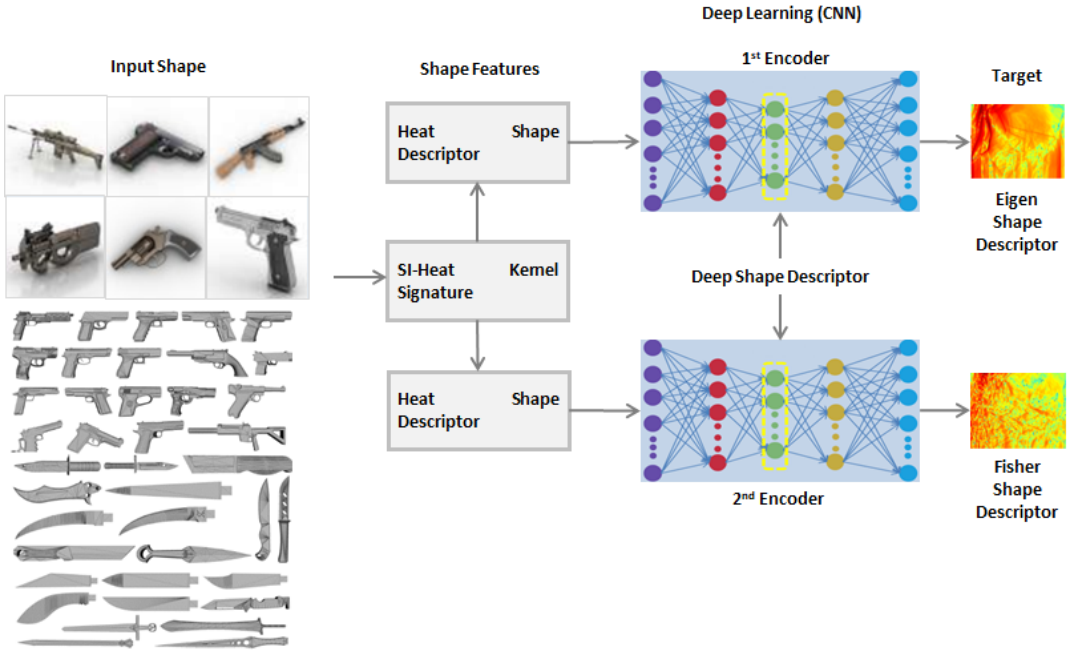
원 모델 워터마크된 프린트물 3D 스캐너 프린트물

1 Secure 3D Printing Informatics (2016~2019)

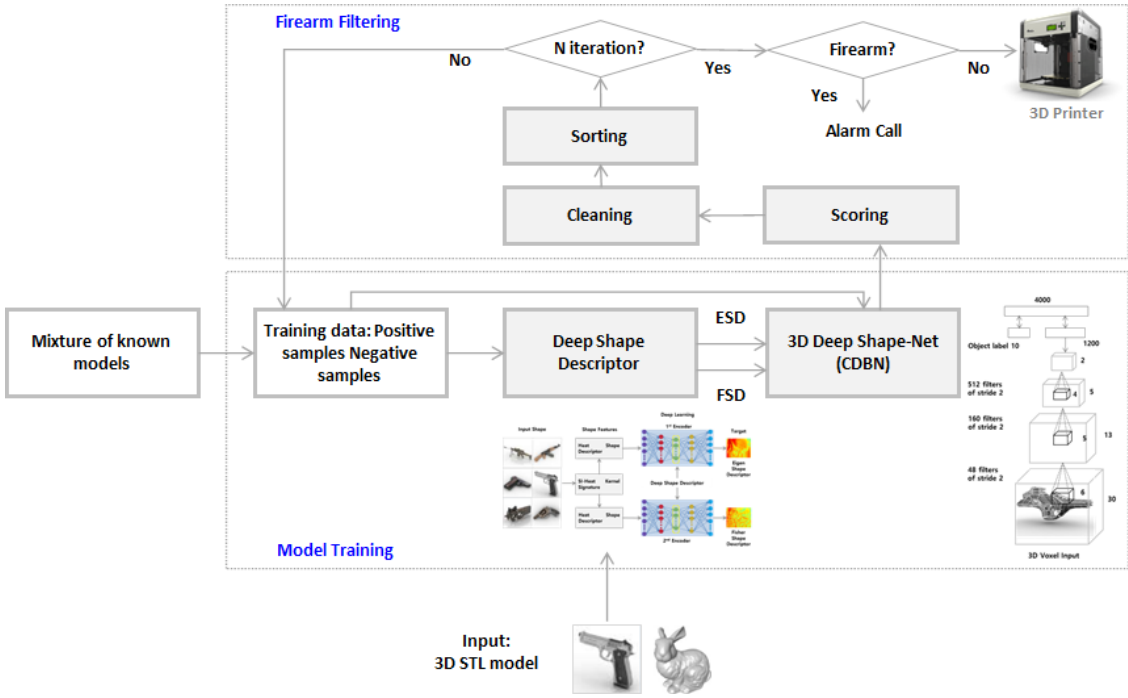
- 딥러닝 기반 불법 3D 프린터 도면 필터링



- 부정(불법무기) 모델에 대한 3D 딥 형상 기술자(Deep shape descriptor)



- 3D 딥-형상넷 기반 부정 프린터물 필터링



1 Secure 3D Printing Informatics (2016~2019)

➢ Anti-3D Weapon Model Detection Using CNN and D2 Shape Features

Open Access Article

Anti-3D Weapon Model Detection for Safe 3D Printing Based on Convolutional Neural Networks and D2 Shape Distribution

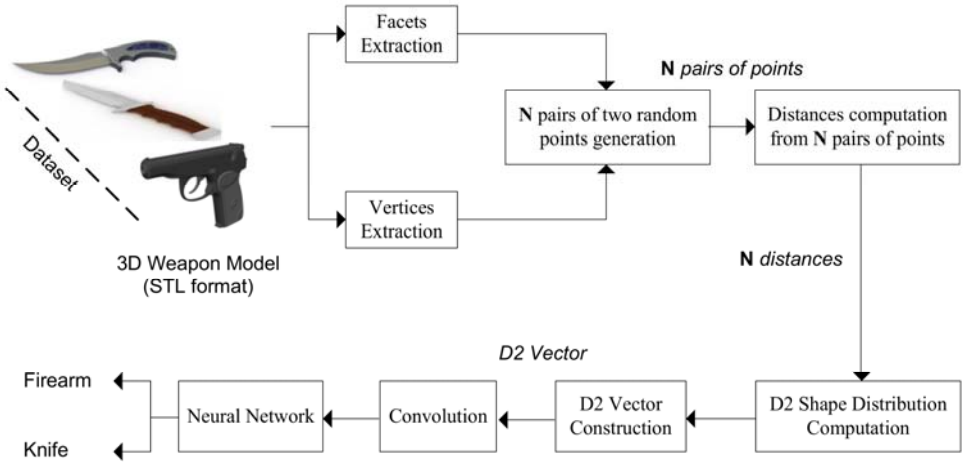
by Giao N. Pham [1], Suk-Hwan Lee [2], Oh-Heum Kwon [1] and Ki-Ryong Kwon [1,*]

[1] Department of IT Convergence & Application Engineering, Pukyong National University, Busan 608-737, Korea
[2] Department of Information Security, Tongmyong University, Busan 608-711, Korea
* Author to whom correspondence should be addressed.

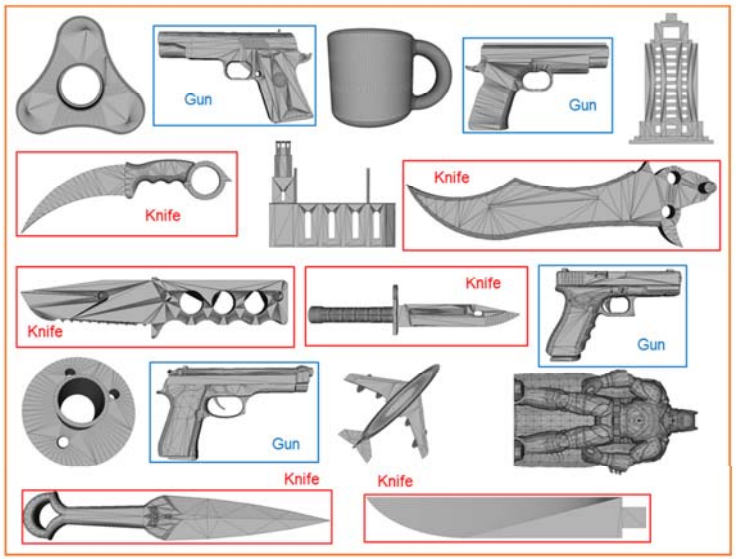
Symmetry **2018**, *10*(4), 90; https://doi.org/10.3390/sym10040090

Received: 28 February 2018 / Revised: 21 March 2018 / Accepted: 29 March 2018 / Published: 31 March 2018

(This article belongs to the Special Issue Information Technology and Its Applications 2018)



- Results of detection of the proposed algorithm.



Method No.	Used Features	Test Classes	Accuracy (%)
Thomas' method	Text, 2D sketch, D2 Shape	Chair, Elf, Table, Cannon, Bunked	62.54
Walter's method	Depth Image	Hammer, Mug, Airplane, Bottle, Car, Shoe	75.66
Osada's method	D2 Shape	Chair, Animal, Cup, Car, Sofa	66
Levi's method	Improved D2 Shape	Unknown (not shown)	Unknown
Our method	D2 Shape, improved CNNs	Firearm, Knife	98.03

1 Secure 3D Printing Informatics (2016~2019)

➢ 3D Perceptual Encryption for 3D Printing

Open Access Article

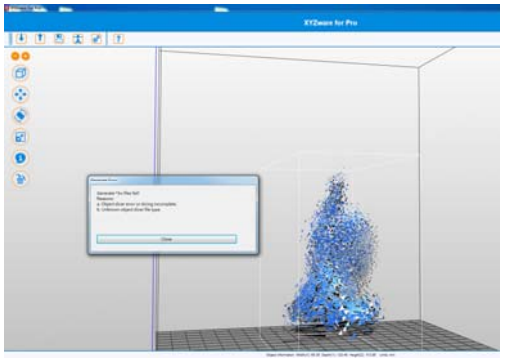
Two-Dimensional (2D) Slices Encryption-Based Security Solution for Three-Dimensional (3D) Printing Industry

by Giao N. Pham [1], Suk-Hwan Lee [2], Oh-Heum Kwon [1] and Ki-Ryong Kwon [1,*]

[1] Department of IT Convergence & Application Engineering, Pukyong National University, Busan 608-737, Korea
[2] Department of Information Security, Tongmyong University, Busan 608-711, Korea
* Author to whom correspondence should be addressed.

Electronics **2018**, 7(5), 64; https://doi.org/10.3390/electronics7050064

Received: 22 April 2018 / Revised: 30 April 2018 / Accepted: 2 May 2018 / Published: 7 May 2018



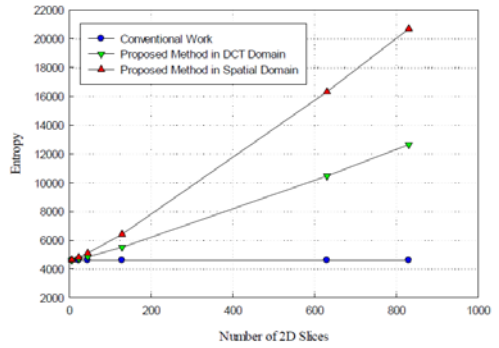


Figure 12. Entropy of the proposed methods according to the number of 2D slices.

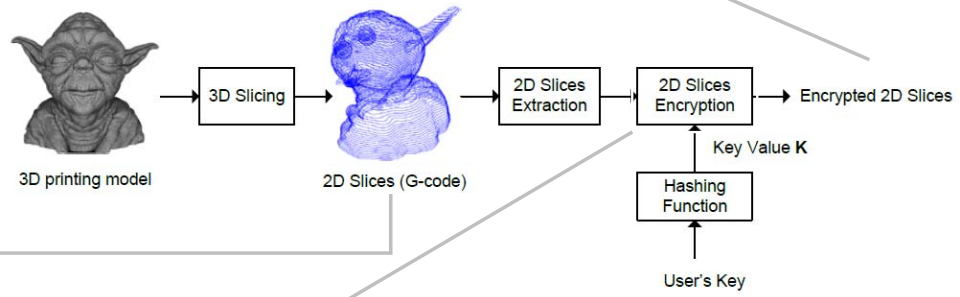


Figure 5. The proposed solution.

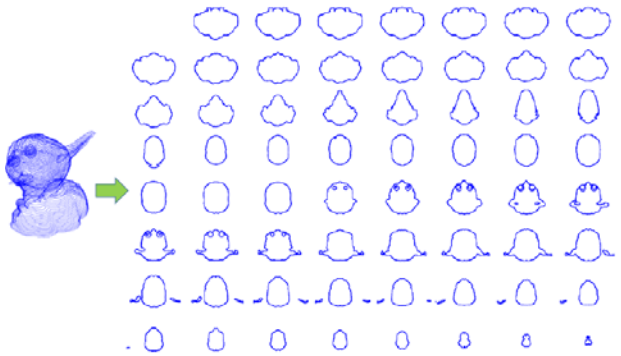


Figure 4. The 2D slices of a 3D printing model in 2D space.

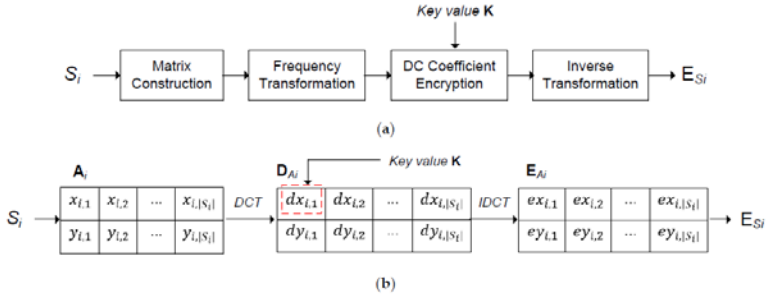


Figure 6. (a) Overview encryption method in the frequency domain, (b) The encryption process of 2D slices in Discrete Cosine Transform (DCT) domain.

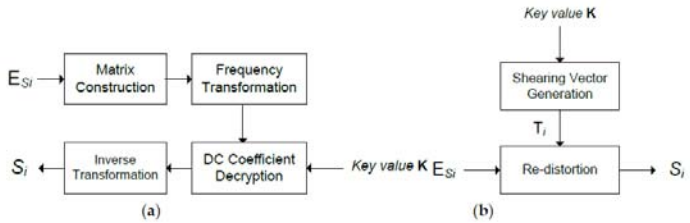


Figure 8. (a) Decryption in the frequency domain, and (b) Decryption in the spatial domain.

2 DNA Security (2011~2016)

Genetic code (DNA code)

Profound personal information

Protect intellectual properties

- Ensure the safety and security of procedures for collecting human genetic information

COMPUTING AND THE LAW

Protecting Bioinformatics as Intellectual Property

Brian M. Gaff, Ralph A. Loren, and Gareth Dickson
Edwards Wildman Palmer LLP

Although trade secrets and copyright provide some protection to bioinformatics tools, a carefully drafted patent can provide the broadest available protection in an increasingly competitive market.

<IEEE Computer Society, 2013>

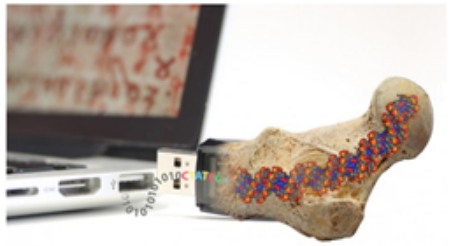
DNA Storage

- Consider a new biometric storage medium for storing huge amounts of data

COMPUTERS

DNA storage could preserve data for millions of years

By Dario Borghino 1 Comment
February 18, 2015



In the search for ways to store data permanently, ETH researchers have been inspired by fossils (Photo: Philipp Stössel/ETH Zurich)

<Gizmag, ETH Zurich, 2015>

DNA Cryptosystem

- New biological encryption

The Future of Data Security: DNA Cryptography and Cryptosystems

February 20, 2015 By Pierluigi Paganini

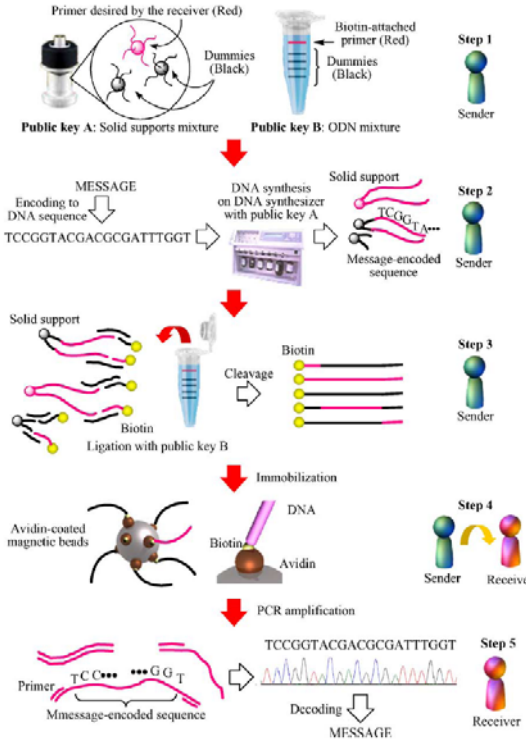
<Securityaffairs, wordpress, 2015>

Information hiding by steganography and watermarking using DNA/RNA sequences

2 DNA Security (2011~2016)

➢ DNA Cryptosystem

- Biological encryption and decryption based on **polymerase chain reaction (PCR)** or **DNA chips**
- Main security : **Restriction of biological techniques**
  - ➢ **PCR** for a sequence with the knowledge of the **correct two primer pairs**
  - ➢ **DNA chip** with the sequences present in **different spots** of DNA chip
- Recognized as a newly biological encryption in the future but the implementation difficulty



1) Encoding step

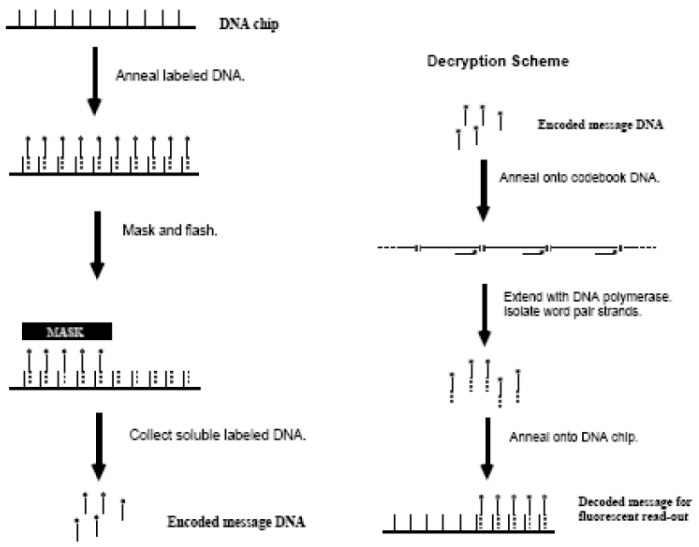
2) DNA synthesis step with key A containing forward primer

3) Ligation step with key B containing reverse primer

4) Immobilization step

5) PCR amplication step with primer

<Exchanging secret key, K. Tanaka et al. Biosystems, 2005 >



<DNA Chip based encryption/decryption, Kang Ning, 2009>

2 DNA Security (2011~2016)

➢ DNA Storage

- **M. Church et al (Havard Medical School), "Next-Generation Digital Information Storage in DNA," *Science*, Sept. 2012**
  - ➢ **Write 5.27 megabit book using DNA microchips (about 700 terabits per 1g)**
  - ➢ **Read the book using DNA sequencing**

- **N. Goldman et al (European Bioinformatics Institutue), "Towards practical, high-capacity, low-maintenance information storage," *Nature*, 2013**
  - ➢ **Improve DNA encoding scheme : 2.2 petabytes per 1g (store 468,000 DVDs)**

❖ **Requirements : High-capacity, Long-term storage, Low-maintenance**

❖ **General process**
  - ➢ **Translate words → binary code (0, 1) → strings DNA (nucleotide) bases {A,T(or U),C,G}**
  - ➢ **Error correction code or encode the information multiple times**

COMPUTING | OPINION

DNA: The Ultimate Data-Storage Solution

The double helix can archive a staggering amount of information in an almost inconceivably small volume

By Latchesar Ionkov, Bradley Settlemyer on May 28, 2021

Even better, DNA can archive a staggering amount of information in an almost inconceivably small volume. Consider this: humanity will generate an estimated 33 zettabytes of data by 2025—that's 3.3 followed by 22 zeroes. DNA storage can squeeze all that information into a ping-pong ball, with room to spare. The 74 million million bytes of information in the Library of Congress could be crammed into a DNA archive the size of a poppy seed—6,000 times over. Split the seed in half, and you could store all of Facebook's data.

<IEEE Spectrum "DNA Data Storage Just Got a Bit More Practical" 2015>

2 DNA Security (2011~2016)

➢ DNA Steganography

- Secret message communication in DNA sequences
- Useful for DNA storage or DNA signature and identification

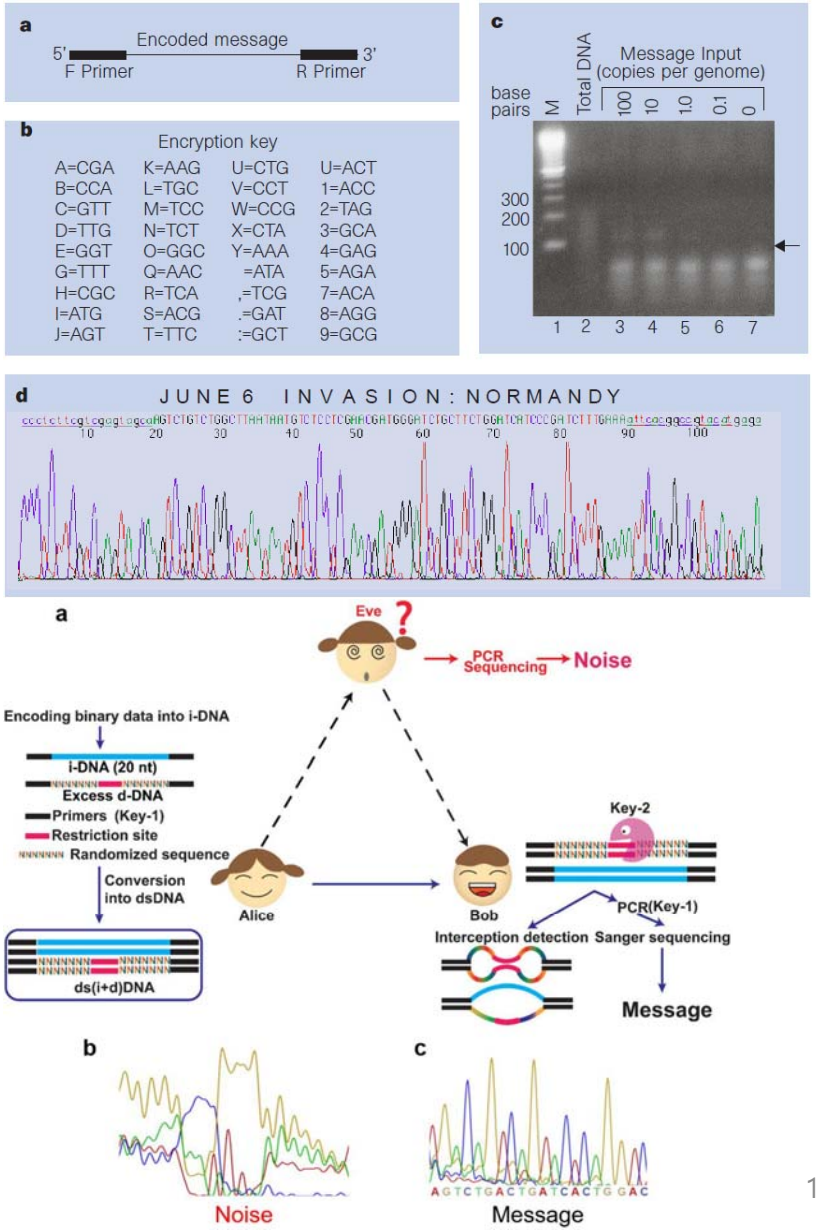
► **Not to recover DNA sequences/messages in the change of experimental conditions/ mutations**

First work : T. Clelland et al, "Hiding messages in DNA microdots," Nature, 1999.

Gene steganography
a) Prototypical secret-message
b) Encryption key for message
c) Gel analysis of products by PCR amplification with specific primers of microdots containing secret-message DNA strands
d) Sequence of the cloned product of PCR and Result of using encryption key to decode the message

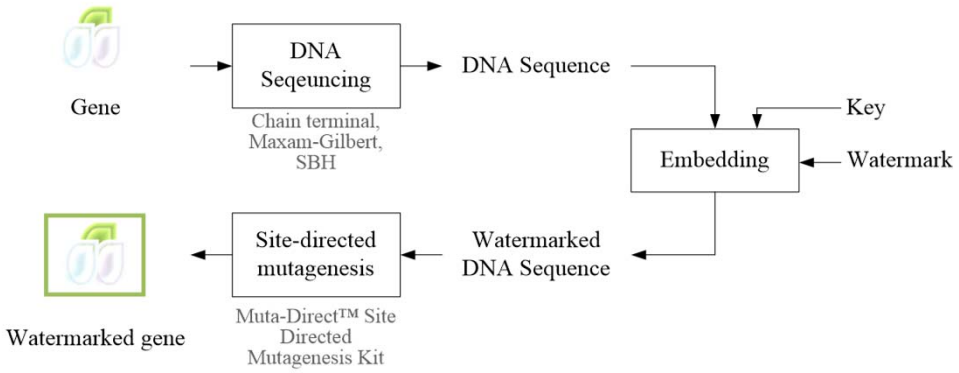
➢ DNA Watermarking

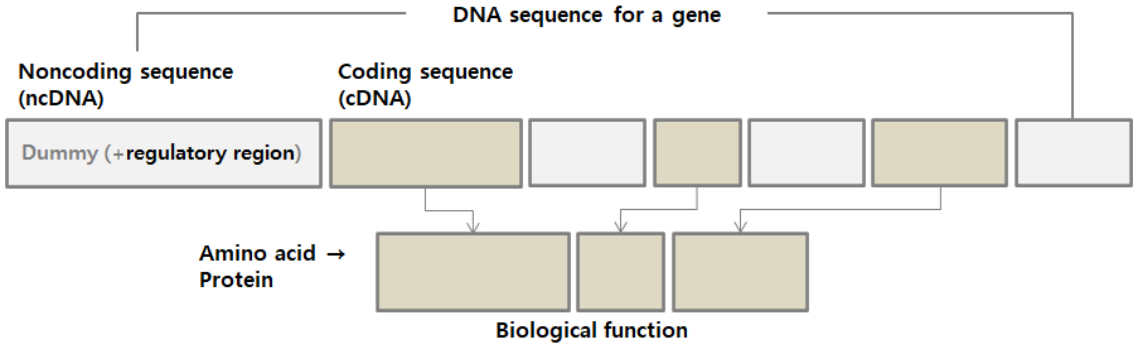
- Technique for protect the information within DNA sequence
- Applied for the copyright protection of GMO as well as the discrimination between wild type genome and artificial genome



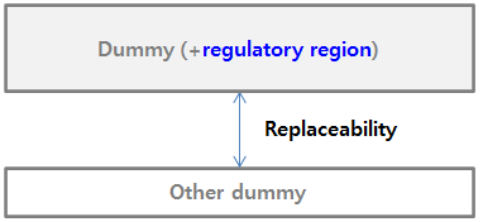
2 DNA Security (2011~2016)

- **General process of DNA Steganography & Watermarking**





Noncoding sequence : ncDNA



- **4 Nucleotide bases** based on algorithm
- High capacity → Steganography or Storage
- Main constraint : No false start codon

Coding sequence : cDNA

Amino acid preservation
No replaceability

- **64 codons** based on algorithm
- Low capacity → Watermarking
- Main constraint : Preserve protein (Amino acid)

- in vitro : 시험관 내 실험 (experimentation within test tube)
- in vivo : 생체 내 실험 (experimentation within living body)
- in silico : 컴퓨터 내 실험 기술 (experimentation within computer) - 바이오인포매틱스

※ in silico 기술 통하여 in vitro/in vivo 실험으로 입증

Coding sequence (cDNA) : Encode to protein
Non-coding sequence : Not encode to protein

- Recent time, non-coding is not dummy

↓

Target gene : Synthesized genome, Bacteria

2 DNA Security (2011~2016)

- **General process of DNA Steganography & Watermarking**

✓ Examples

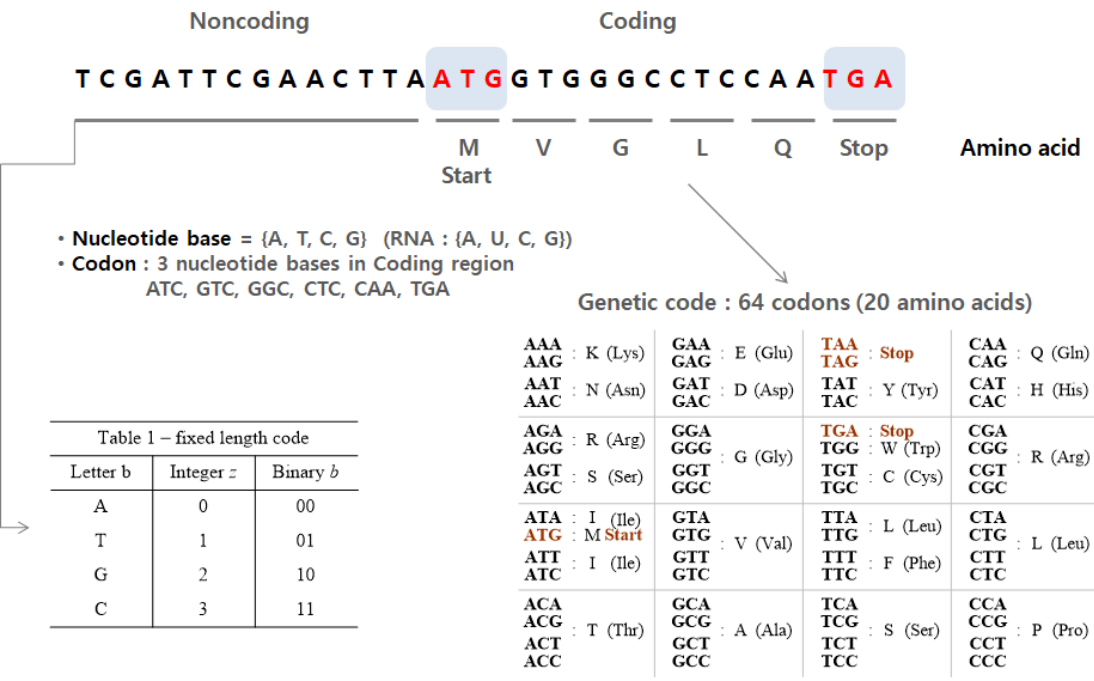


Table 1 – fixed length code

Letter b	Integer z	Binary b
A	0	00
T	1	01
G	2	10
C	3	11

✓ Requirements

- **Amino acid preservation** (Coding) : No change amino acids by the watermark
- **No false start codon** (Non-Coding) : Prevent to convert from non-coding to coding
- **Resistance** : Resist to spontaneous or induced mutations (point mutation, deletions, insertions)
- **Codon optimization** : CAI (codon adaptation index), GC content, etc
- **Security** : Very difficult to detect the watermark in DNA sequence without the key knowledge
- **Capacity** : Contain enough information for copyright
- **Others** : Message fidelity, Error tolerance, Easy delivery/interpretation

- **DNA Copyright Protection**

Information Sciences 273 (2014) 263–286

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

DWT based coding DNA watermarking for DNA copyright protection

Suk-Hwan Lee *,1

Department of Information Security, Tongmyong University, 535, Yongdang-dong, Namgu, Busan, Republic of Korea

ARTICLE INFO

Article history:
Received 13 November 2013
Received in revised form 21 February 2014
Accepted 9 March 2014
Available online 19 March 2014

Keywords:
DNA watermarking
DNA copyright protection
Coding DNA
Lifting based DWT
Genetic information security
Mutation resistance

ABSTRACT

DNA watermarking is a technique for copyright protection and ownership authentication of DNA sequences and ensures the security of private genetic information. This paper addresses issues regarding watermarking DNA coding sequences in the frequency domain that confer mutation resistance, amino acid conservation, and security. Multimedia watermarking is designed for robustness and invisibility mainly based on frequency domain representations. However, frequency domain watermarking for a coding DNA sequence is significantly constrained because the transformation and inverse transformation must be performed while completely conserving the amino acid sequence. In this paper, we present a coding DNA watermarking method in a lifting-based discrete wavelet transform (DWT) domain that focuses on the feasibility of frequency domain watermarking for DNA sequences. Our method divides a coding DNA sequence into a number of subsequences and allocates all codons in subsequences to a numerical code using the histogram ranks of the amino acids. Our method then calculates a set of DWT coefficients for subsequences of synonymous codons and finds a subsequence among them with DWT coefficients that are optimal for embedding watermark bits. Finally, our method substitutes this sequence for a subsequence of codons. To secure the watermark, our method generates the binary watermark based on nonlinear congruential – pseudorandom number generator (NC-PRNG) and randomly selects the embeddable position in the DWT domain of the subsequence. We experimentally verified that our method ensures not only amino acid conservation and security but also resists a point mutation rate of approximately 18.5% point mutations.

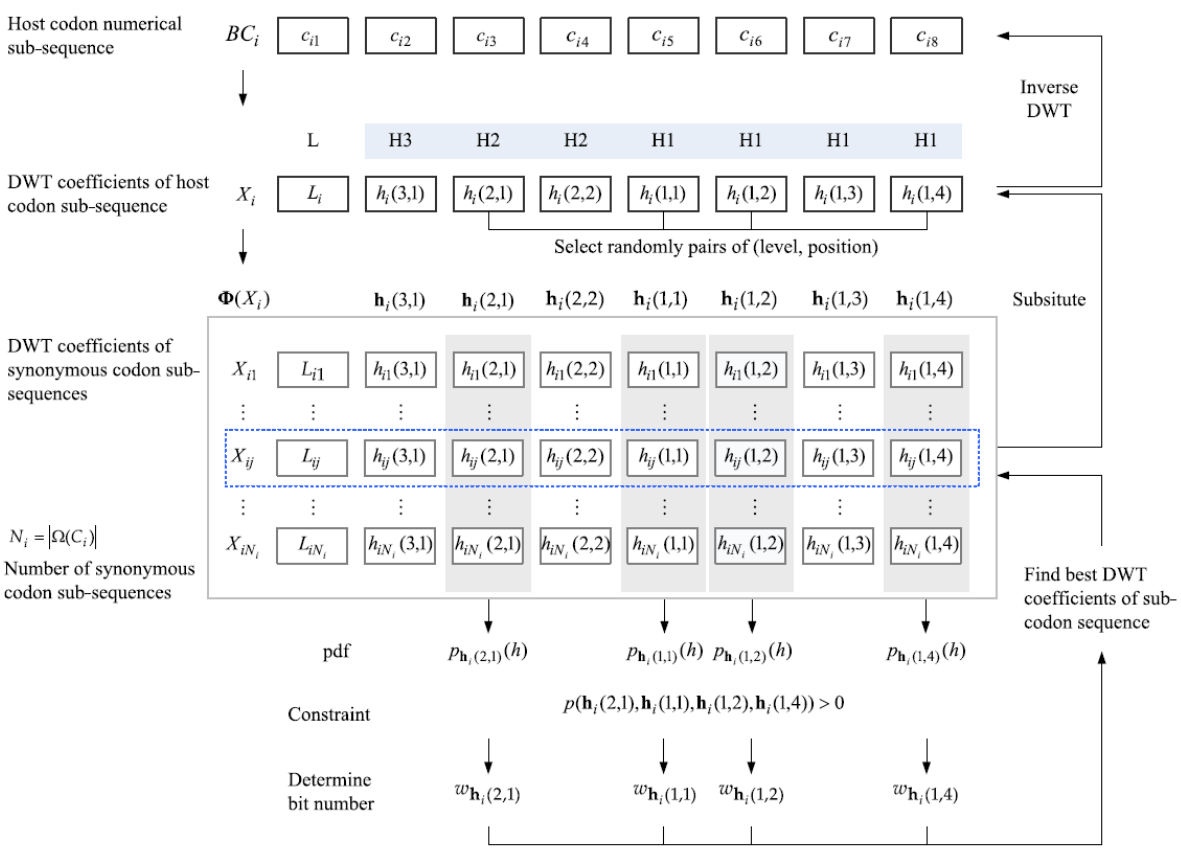


Fig. 7. Embedding process for a numerical codon subsequence BC_i, in $N_B = 8$ and $M = 4$.

Table 4
Watermark capacities and change rates of nucleotide bases ($n = 5$ in WDH(n) for Heider's DNA-Crypt algorithm [39], $R = 3$ for Liss's method. [58], 5 repeated times of Haughton's BioCode pcDNA with watermark codes [36]).

GeneBank accession	Gene	Watermark capacity (bit/codon)				Base change rate (%)			
		Proposed	Heider	Liss + Repetition	Haughton + Repetition	Proposed	Heider	Liss + epetition	Haughton + Repetition
JQ670900	bg1	0.172	0.142	0.119	0.180	20.31	7.03	8.20	11.21
JQ439993	mgpB	0.188	0.164	0.129	0.194	20.39	10.51	13.22	16.22
NM001179490	CCT2	0.21	0.193	0.16	0.223	21.90	11.80	17.74	20.74
L34837	FET4	0.164	0.169	0.141	0.199	20.43	10.84	12.29	15.29
NM000520	HEXA	0.213	0.196	0.164	0.226	23.08	12.83	14.71	17.71
NM001145	ANG	0.216	0.189	0.155	0.219	21.17	12.61	19.14	18.14
BC111374	TUBB6	0.162	0.183	0.151	0.213	17.85	11.24	13.17	16.17
BC094877	ACTG2	0.161	0.18	0.151	0.210	18.65	11.58	11.67	14.67
BC094878	ARL2BP	0.150	0.156	0.13	0.186	17.21	9.59	16.56	15.52
BC140809	ANKRD20A2	0.164	0.157	0.131	0.187	21.18	9.88	14.58	17.58
Average		0.180	0.173	0.143	0.204	20.21	10.79	14.13	16.32

Table 5
CAI and GC content of host DNA and watermarked DNA sequences.

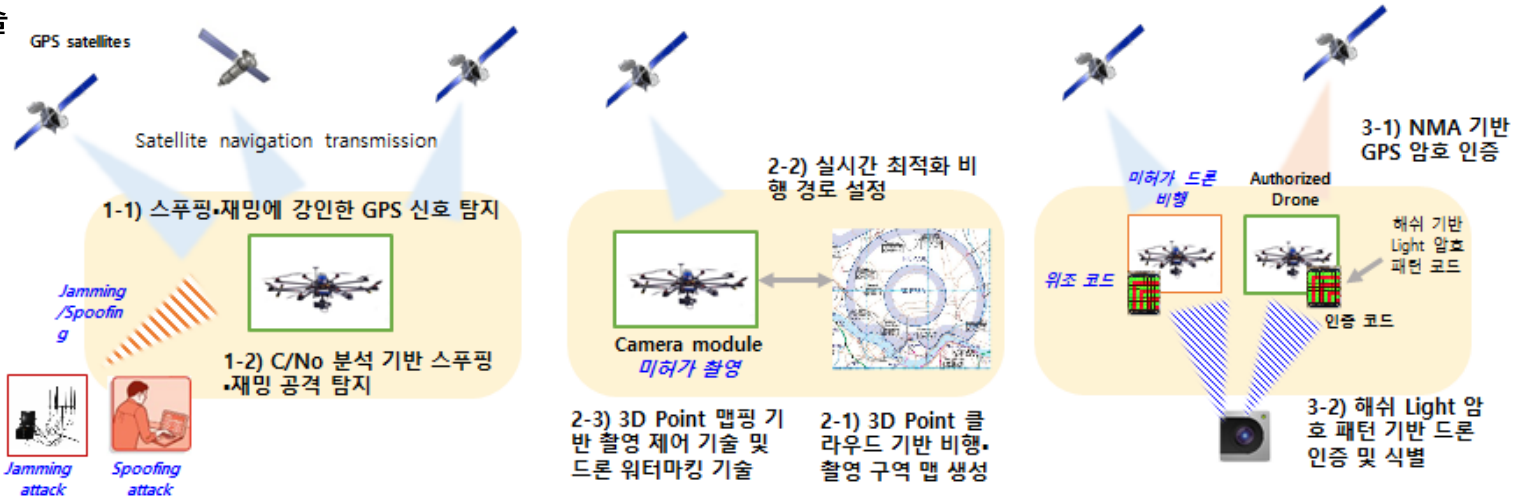
GeneBank accession	CAI					GC content (%)				
	Host	Proposed	Heider	Liss + Repetition	Haughton + Repetition	Host	Proposed	Heider	Liss + Repetition	Haughton + Repetition
JQ670900	0.825	0.769	0.758	0.799	0.825	46.05	43.93	44.13	44.70	46.05
JQ439993	0.918	0.914	0.912	0.932	0.918	35.16	37.50	33.20	34.37	35.16
NM001179490	0.812	0.802	0.796	0.828	0.812	43.62	42.11	46.52	46.90	43.62
L34837	0.766	0.814	0.821	0.809	0.766	40.32	39.18	43.64	38.93	40.32
NM000520	0.833	0.810	0.804	0.854	0.833	52.14	54.90	53.58	54.72	52.14
NM001145	0.878	0.874	0.841	0.889	0.878	51.57	52.25	50.90	48.42	51.57
BC111374	0.732	0.767	0.754	0.796	0.732	58.93	58.92	53.72	60.04	58.93
BC094877	0.785	0.789	0.799	0.850	0.785	52.52	52.51	48.89	55.44	52.52
BC094878	0.869	0.879	0.863	0.904	0.869	47.06	46.19	46.18	46.40	47.06
BC140809	0.790	0.834	0.837	0.871	0.790	39.98	36.45	40.82	38.07	39.98
Average	0.821	0.825	0.818	0.853	0.821	46.73	46.40	46.15	46.79	46.73

3 Drone Security (2017~2019)

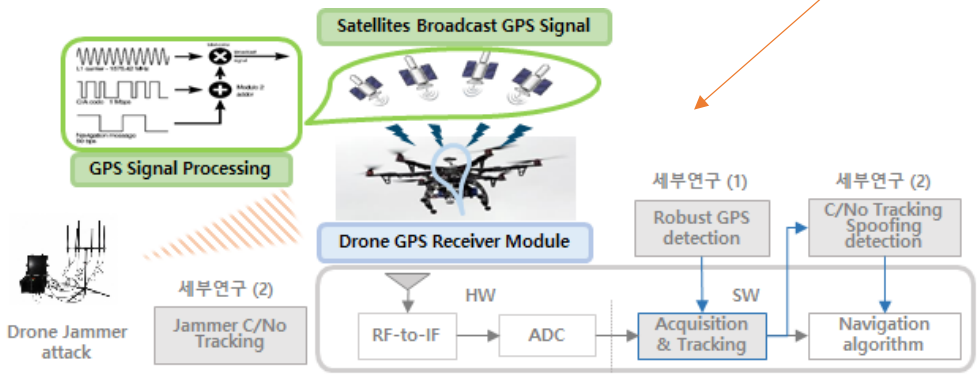
불법 비행·촬영 방지 위한 신뢰있는 드론 보안 기술 연구
(Trust Drone Security Technique for Illegal Flight·Photographing Prevention)

➢ 불법 비행.촬영 방지위한 드론 보안 및 인증 기술

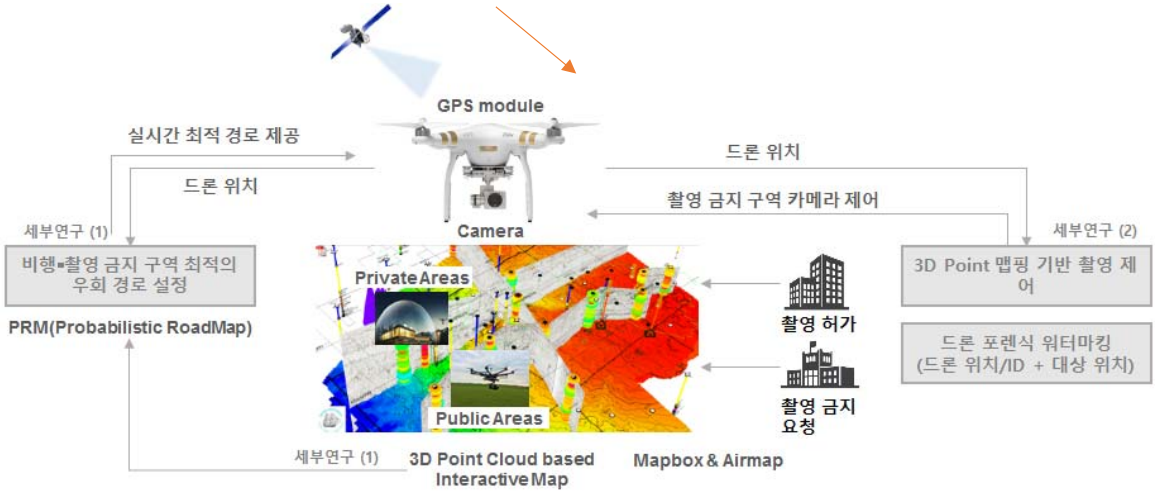
- 강인한 GPS 신호 검출
- C/No 기반 공격 탐지 기반 GPS 스푸핑. 재밍 방지 기술,
- 불법 비행.촬영 방지위한 드론 비행.촬영 제어 및 워터마킹 기술
- Light 암호 패턴 기반 드론 보안 인증 및 식별 기술



1. 드론 스푸핑·재밍 방지 기술



2. 드론 불법 비행·촬영 방지 기술

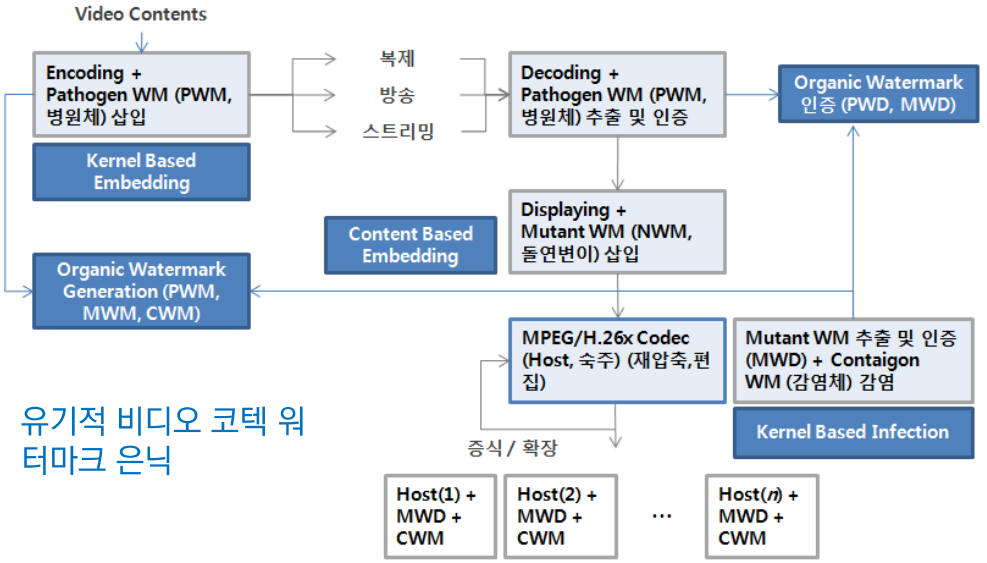


3. 드론 보안 인증 및 식별 기술

3 Video Watermarking (2011~2013)

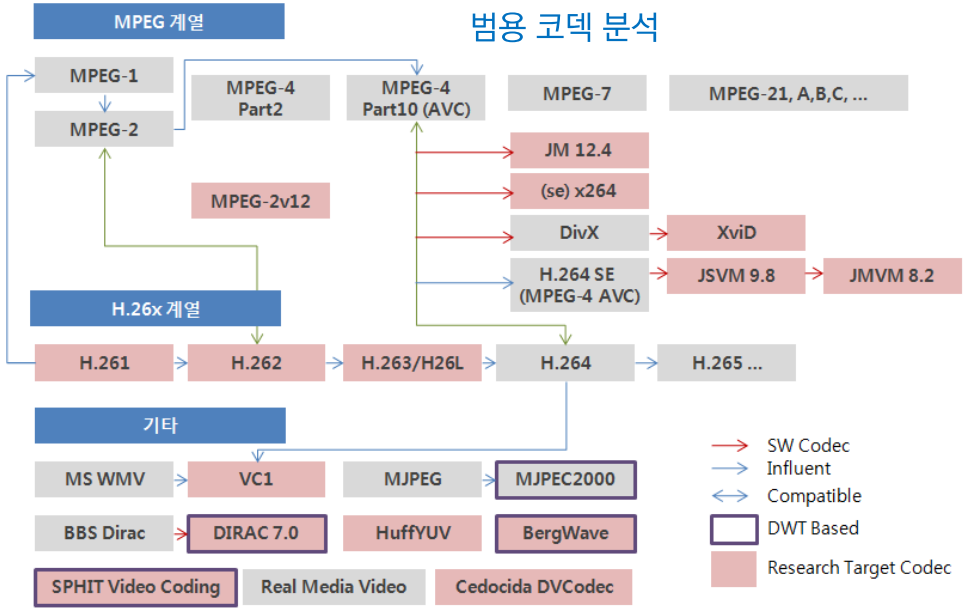
➢ 비디오 영상 관리를 위한 생물학적 유기체 기반 워터마킹 개발

- 생물학적 유기체의 성질과 전염성 바이러스 특징 기반의 유기적 워터마킹 이론을 모델링 개발
- 유기적 전염성 워터마크 생성 및 관리 기법 개발
- 유기적 워터마크 및 전염성 바이러스 감염 모델링 기반으로 숙주 비디오 코덱 상의 유기적 워터마크 감염 기법과 인증 관리 기법 개발
- 생물학과 워터마킹 개념이 결합된 새로운 이론을 제시하고, 범용 비디오 코덱에 적용함으로써 살아있는 유기적인 속성을 가지는 비디오 콘텐츠의 인증, 검색 및 저작권 관리 시스템을 개발

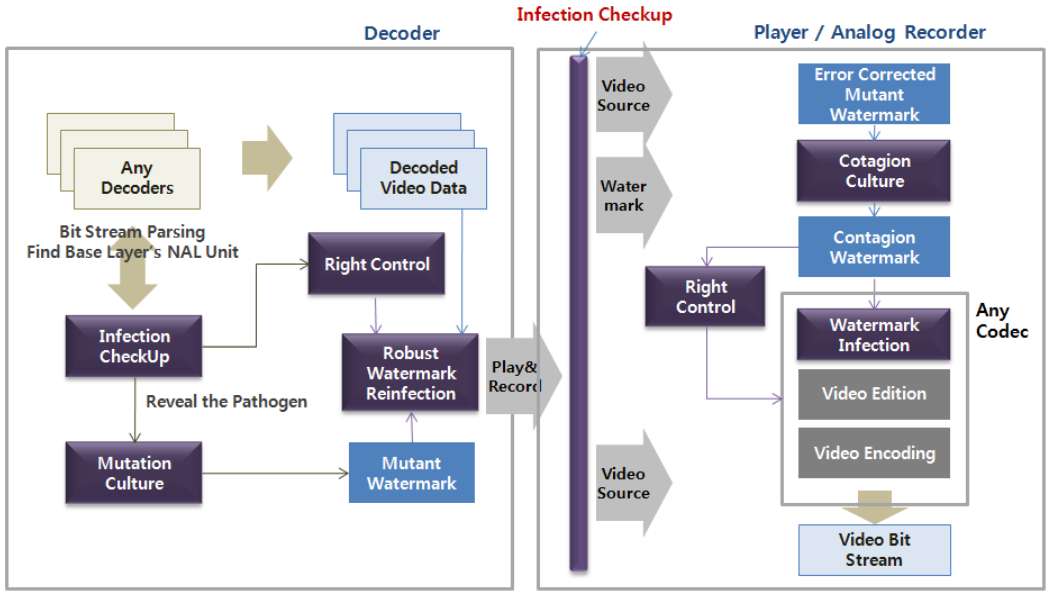


유기적 비디오 코텍 워터마크 은닉

범용 코덱 분석



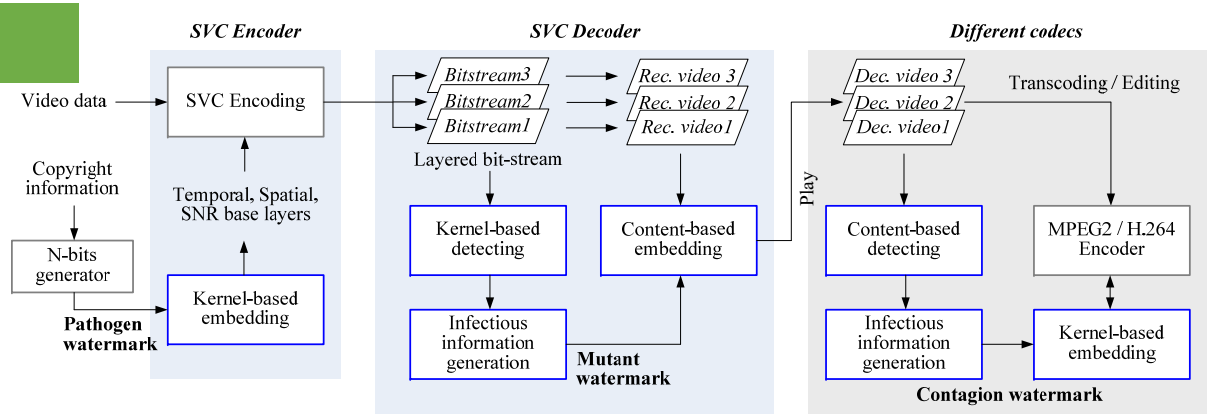
복호기 및 비디오 편집 과정에서 워터마크 신뢰 및 권한제어신호 검증 및 은닉



3 Video Watermarking (2011~2013)

➢ 비디오 영상 관리를 위한 생물학적 유기체 기반 워터마킹 개발

- H.264 SE/MPEG-4 SVC codecs
- H.264/MPEG-2 codecs



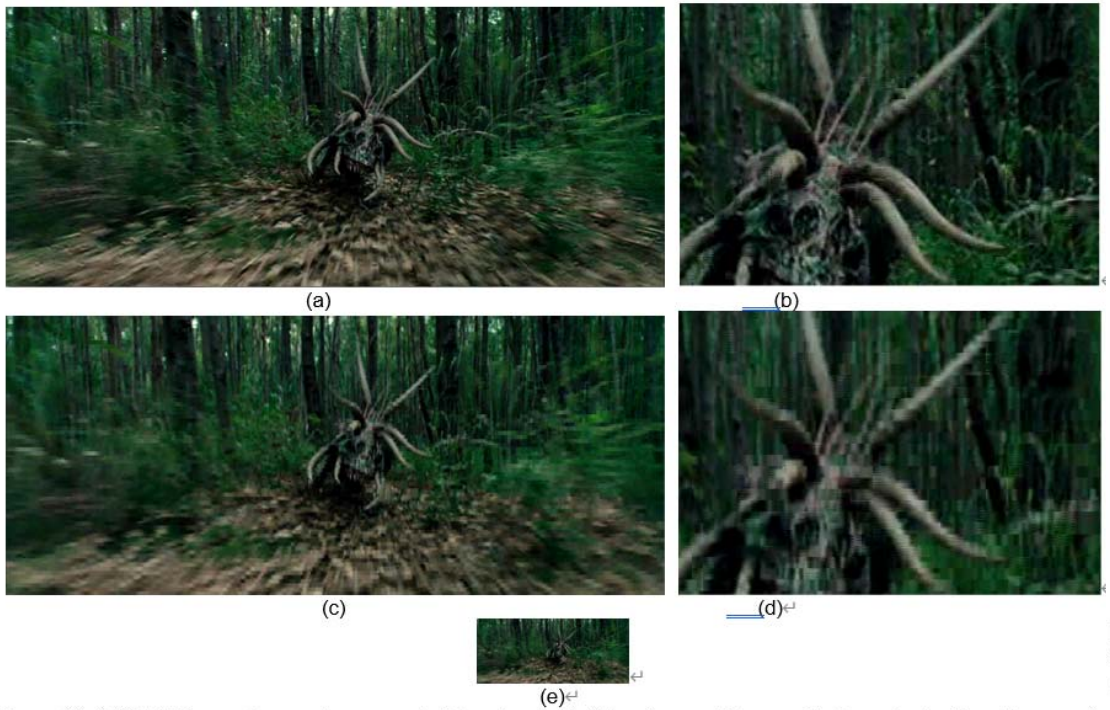


Figure 10. (a)(b) A frame of normal recovered video stream, (c)(d) a frame of low quality in expired video stream or in unauthorized codec, and (e) a frame of low quality and low resolution in expired video stream or in unauthorized codec. ((a),(c),(e) 30% scaled version of original resolution, (b)(d) Magnified version of any region)

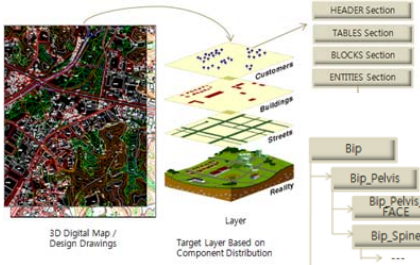
Figure 9. Any frame of (a),(b) normal recovered video after K-EM and K-DM and (c),(d) recovered video with the blocking artifacts because of recovery error by re-hiding of the random watermark. ((a),(c) : 30% scaled version of original resolution, (b),(d) : Magnified version of any region)

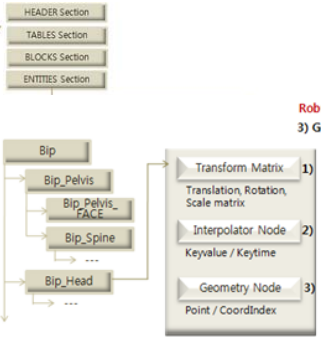
3 Perceptual Hashing (2009~2011)

➢ **3D 콘텐츠의 복사 검출 및 인증을 위한 3D 해싱 기술**

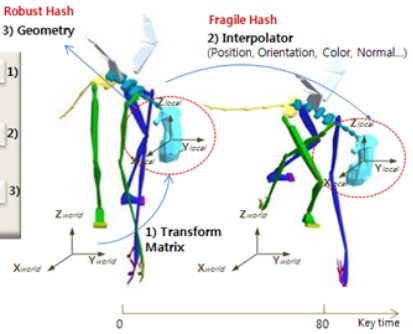
- 3D 콘텐츠의 기본 모델인 3D 폴리곤 모델, 3D 애니메이션 모델 및 3D 벡터데이터 모델에 적용이 가능한 3D 해싱 기술을 개발
- 각 모델 구조에 따른 3D 특징벡터 추출, 특징벡터의 양자화 과정 및 3차 Reed-Muller 또는 Wyner-Ziv에 의한 해쉬 비트열 생성 기술
- 3D 콘텐츠의 공격 및 변형 유형 모델링 기술과 이들 공격에 대한 강인성 및 연약성을 모두 가지는 3D 해쉬 생성 기술과 3D 해싱 기술의 보안성 및 강인성 평가 체계

- 벡터 데이터





- 메쉬 모델



3D Contents Hashing System for Authentication and Copy Detection