

커버 소스 불일치에 대한 이미지 스테그노그래피 일반화

오서연^{0*}, 김동수^{*}, 민지민^{*}, 장한열[†]

한밭대학교 컴퓨터공학과

{20211915, 20191766, 30231212}@edu.hanbat.ac.kr, hejang@hanbat.ac.kr

Steganalysis Learning Methods for Resolving Cover Source Mismatch Issues

요약

모바일 기기 보급으로 인해 스테가노그래피 도구의 활용성이 크게 향상됨에 따라 스테그노그래피 기술의 중요성이 높아지고 있다. 최근에는 커버를 생성하는 소스 이미지 생성 과정에서 파라미터 변화가 발생하는 경우 스테그노그래피 성능이 크게 저하되는 커버-소스 불일치 문제가 주목받고 있다. 본 논문에서는 다양한 소스 기기에서 취득한 이미지로 통합 데이터셋을 구축하여 커버-소스 불일치 문제에 효과적으로 대응한다. 또한, 커버와 스테고 이미지 간의 미세한 차이값을 효과적으로 탐지할 수 있도록 CNN 모델의 저수준 특징 추출부를 개선하고 대조 학습을 활용한다. 제안기법은 학습에 사용하지 않은 Galaxy Flip3와 iPhone12 기기에 대하여 베이스라인 모델 대비 평균 6.36% 탐지율 향상을 보였다.

1. 서론

스테가노그래피(steganography)는 이미지, 비디오, 오디오 등과 같은 다양한 매체에 정보를 비밀리에 삽입하는 기술로, 디지털 매체의 일상화와 함께 정보 보호 분야에서 중요한 방법 중 하나이다. 최근에는 스테가노그래피 모바일 도구 활용성이 크게 향상됨에 따라 스테그노그래피 기술도 중요해지고 있다. 스테그노그래피는 스테가노그래피를 통해 숨겨진 정보를 감지하고 분석함으로써 스테가노그래피의 부적절한 사용을 방지하고 보안을 강화하는 데 사용된다. 정보의 디지털화가 지속됨에 따라 스테그노그래피의 필요성은 더욱 커지고 있다.

스테가노그래피를 탐지하기 위해서는 메시지가 삽입된 스테고(stego) 이미지와 메시지가 삽입되지 않은 커버(cover) 이미지 사이의 미세한 차이를 구별해야 한다. 그림 1을 보면 커버와 스테고 이미지의 차이는 사람의 눈으로 거의 구별할 수 없다. 커버와 스테고 이미지에서 메시지가 삽입된 영역의 차이는 대부분 최하위 비트(least significant bit, LSB)에서 발생하기 때문에 픽셀 차이값은 1이고, 굉장히 미세한 패턴이다. 이미지의 통계적 특성을 주로 활용한 기존 스테그노그래피 방법들과 달리, 딥러닝을 활용한 스테그노그래피 방법은 더 복잡한 패턴과 관계를 학습할 수 있으며, 특히 컨볼루션 신경망(convolutional neural networks, CNN)은 고차원 데이터에 내재된 특징들을 추출하여 숨겨진 정보를 효과적으로 식별하는데 효과적이다.

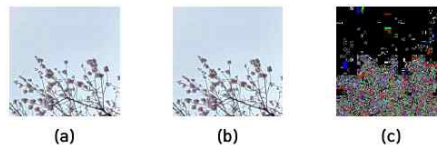


그림 1. (a) 커버, (b) 스테고, (c) 커버와 스테고 차이 이미지 예시

그러나 딥러닝 기반의 스테그노그래피 기법은 커버를 생성하는 소스 이미지 생성 과정에서 파라미터 변화가 발생하는 커버-소스 불일치(cover-source mismatch, CSM) 시에 탐지율이 크게 하락하는 제한점이 있다. CSM은 크게 이미지 획득과 이미지 처리 과정에서 발생한다. 이미지 획득 과정에서는 렌즈 종류, ISO, 노출 시간 등에서 파라미터 차이가 발생할 수 있고 이미지 처리 과정에서는 디노이징, 샤프닝, 절삭 등의 알고리즘의 파라미터 차이가 발생할 수 있다. 기존에 공개된 스테그노그래피 벤치마크의 경우 대부분 같은 기기와 같은 파라미터를 사용하여 소스 이미지를 생성하기 때문에 다른 소스 이미지 생성 과정으로 구축된 데이터셋에 대해서는 성능이 크게 하락하는 문제가 발생한다.

본 논문에서는 CSM 문제에 효과적으로 대응하기 위해 여러 종류의 모바일 기기에서 취득한 다양한 소스 환경의 통합 데이터셋을 구축하였다. 또한, 커버와 스테고 이미지 간의 미세한 차이값을 효과적으로 탐지할 수 있도록 CNN 모델의 저수준 특징 추출부를 개선하고 대조 학습을 활용하는 방법을 제안한다.

2. 관련 연구

2.1 CNN 기반의 스테그노그래피

최근 딥러닝 기반의 스테그노그래피 기술이 활발히 연구되고 있다. 딥러닝 모델은 높은 계산 능력과 복잡한 패턴을 학습할 수 있는 능력을 바탕으로, 전통적인 스테가노그래피 탐지 기법보

* 본 연구는 2024년 과학기술정보통신부 및 정보통신기획평가원의 SW중심대학사업의 연구결과로 수행되었음(2022-0-01068)

KCC 2024 발표논문 Index

Index 확인방법

<인덱스 예시> 26A-O1-9					
26	A	O	1	-	9
6.26(수)	오전(Am)	Oral	세션번호	-	발표순서

<인덱스 예시> 28P-P8.1-13					
28	P	P	8	-	13
6.28(금)	오후(Pm)	Poster	세션번호	-	보드번호

검색 논문 : 1 편

논문 번호	제 목	발표자	Index
99	커버 소스 불일치에 대한 이미지 스테그어날리시스 일반화	오서연	26A-P1.2-11

/ 1 pages

List number

<경진대회>

<https://sites.google.com/view/face-anti-spoofing-challenge/welcome/challengecvpr2024>.

<https://www.kaggle.com/competitions/hbnu-fake-audio-detection-competition/leaderboard>

Competition



Snapshot Spectral Imaging Face Anti-spoofing Challenge

Organized by THU-CVAILAB - Current server time: June 7, 2024, 12:28 p.m. UTC

First phase

Phase 1

Feb. 29, 2024, midnight UTC

End

Competition Ends

March 31, 2024, midnight UTC

[Learn the Details](#)

[Phases](#)

[Participate](#)

[Results](#)

Phase 1 Phase 2

Phase description

Development phase with result scoring

Max submissions per day: 5

Max submissions total: 100


[Download CSV](#)

RESULTS						
#	User	Entries	Date of Last Entry	ACER [%] ▲	APCER [%] ▲	BPCER [%] ▲
1	jho-yonsei	9	03/21/24	0.2060 (1)	0.4121 (1)	0.0000 (1)
2	jeu2250	17	03/21/24	0.6868 (2)	0.4121 (1)	0.9615 (3)
3	dongsukim	30	03/21/24	0.6868 (2)	0.4121 (1)	0.9615 (3)
4	minseok	19	03/22/24	0.8585 (3)	1.2363 (4)	0.4808 (2)
5	ZTT	6	03/21/24	0.9615 (4)	0.9615 (2)	0.9615 (3)
6	whyjlee	13	03/21/24	1.3049 (5)	1.6484 (6)	0.9615 (3)
7	Jimini	25	03/21/24	1.3393 (6)	1.2363 (4)	1.4423 (4)
8	ChenYifan	5	03/20/24	1.5110 (7)	1.0989 (3)	1.9231 (5)
9	yiyaoscb	17	03/17/24	2.0604 (8)	2.1978 (8)	1.9231 (5)
10	stella0831	48	03/23/24	2.1635 (9)	1.9231 (7)	2.4038 (6)
11	SeaRecluse	8	03/08/24	2.4382 (10)	1.5110 (5)	3.3654 (7)
12	sunghun	26	03/19/24	2.4725 (11)	1.0989 (3)	3.8462 (8)
13	yelan.lj	5	03/18/24	2.8846 (12)	5.7692 (12)	0.0000 (1)
14	hexianhua	11	03/20/24	3.6401 (13)	7.2802 (13)	0.0000 (1)
15	Bulbul	11	03/21/24	3.9835 (14)	3.1593 (9)	4.8077 (9)
16	ctyun-ai	11	03/21/24	4.7734 (15)	3.2967 (10)	6.2500 (10)
17	CTEL_AI	4	03/12/24	9.8901 (16)	3.4341 (11)	16.3462 (12)
18	THU-CVAILAB	1	02/29/24	11.0920 (17)	13.0495 (14)	9.1346 (11)
19	Wantongming	3	03/14/24	50.0000 (18)	100.0000 (15)	0.0000 (1)

제목	2024 소중한 SW·AI경진대회 최종 결과		
등록일	2024.06.03	조회수	111
작성자	SW중심대학사업단		

안녕하세요. 국립한밭대학교 SW중심대학사업단입니다.
2024 소중한 AI·SW경진대회 최종결과 안내드립니다.

부문	등수	팀명	우수팀 상금	비고
SW부문	1	대화가필요해	50만원	디지털 경진대회 참가
	2	도피티	40만원	
	3	MOBICOM	30만원	
AI부문	1	AiRLab	50만원	디지털 경진대회 참가
	2	DSDK	40만원	디지털 경진대회 참가
	3	AIMs	30만원	디지털 경진대회 참가
	4	EffAI Lab		디지털 경진대회 참가
	5	Sound Challenger		디지털 경진대회 참가
	6	타피오카 PEARL		디지털 경진대회 참가
	7	유채묵		디지털 경진대회 참가



HANEOL JANG · COMMUNITY PREDICTION COMPETITION · PRIVATE · 21 DAYS AGO

Late Submission

HBNU Fake audio detection competition

Fake audio detection competition at Hanbat National University

OverviewDataCodeModelsDiscussionLeaderboardRulesTeamSubmissions











Leaderboard

Raw DataRefresh

Search leaderboard

PublicPrivate

The private leaderboard is calculated with approximately 40% of the test data. This competition has completed. This leaderboard reflects the final standings.

#	△	Team	Members	Score	Entries	Last	Solution
1	—	AiRLab	    	0.9650	76	21d	
2	—	DSDK	    	0.9512	56	25d	