

WATERMARKING

STEGANOGRAPHY

Erfan Bahmanyar – Elahe Nemati

TABLE OF CONTENTS

01

مقدمه

نگاهی جامع به واترمارکینگ

02

تاریخچه ای از پنهان سازی اطلاعات

تعاریف اولیه، شباهت ها و
تفاوت ها

03

واترمارک نامرعی

مفاهیم و اصطلاحات متداول
دیگر در واترمارکینگ

04

پارامترهای ارزیابی الگوریتم

الگوریتم های پیاده سازی
واترمارکینگ

05

ویژگی های قابل تعریف در واترمارک

06

محیط میزبان

انواع محیط های میزبان برای
واترمارکینگ

01

INTRODUCTION

مقدمه

مقدمه:

با توجه به گسترش روز افزون ارتباطات در دنیای امروز، ضرورت کنترل بهینه ارتباطات در محیط های گوناگون اداری، چندرسانه ای، فیزیکی، دیجیتالی و امنیتی بیش از پیش روشن میشود.

دانش هوش مصنوعی از زیرمجموعه های مهم در دانش کامپیوتر، دراین زمینه گامهای بلندی برداشته است. حفاظت از داده ها در مقابل کپی برداری و جعل اهمیت بالایی دارد به همین دلیل باید از راهکار هایی برای کنترل کپی کردن استفاده کرد. یکی از این نمونه کارها، استفاده از تکنیک واترمارکینگ است.

واترمارکینگ به معنای پنهان کردن داده ها در تصاویر است به نحوی که با چشم قابل تشخیص نباشد و فقط افراد مجاز قادر به استخراج این داده ها باشند.

به عبارتی دیگر میتوان چنین گفت که واترمارکینگ نسل جدیدی از پنهان سازی اطلاعات است.

از همین رو واترمارکینگ نیز بعنوان یک تکنیک در فرآیند استگانوگرافی، امروزه مورد توجه واقع شده است.



ارتباط واترمارکینگ و هوش مصنوعی :

در زمینه ی واترمارکینگ دانش هوش مصنوعی و زیرمجموعه ی پردازش تصویر بسیار به کار گرفته میشود.



02

A HISTORY OF HIDING INFORMATION:

تاریخچه ای از پنهان سازی اطلاعات :

تاریخچه ای از پنهان سازی اطلاعات :

در حدود 500 سال قبل از میلاد ، یهودیان از الفبای "آتاباش" که نوعی الفبای رمزوارونه است استفاده میکردند.

در سال 1870، در زمان محاصره شهر پاریس، برای رساندن نامه ها توسط کبوترهای نامه بر، از رمزگذاری اطلاعات استفاده میشد.

در جنگ جهانی دوم آلمانی ها روش "ریز نقطه" را برای رمزگذاری مکاتبات محرمانه خود ابداع کردند.

در جنگ آمریکا، نیروهای آمریکا و انگلستان هردو، از نوعی جوهر نامرعی برای رمزگذاری استفاده میکردند.

تعاریف اولیه، شباهت ها و تفاوت ها :

واترمارکینگ شاخه ای از فرآیند پنهان نگاری محسوب میشود که نخستین بار در سال 1996 معرفی شد.

واترمارکینگ به عنوان یک روش در حفاظت کپی رایت و جلوگیری از تکثیر غیر قانونی اطلاعات، روش مناسبی محسوب میشود.

تفاوت واترمارکینگ و پنهان نگاری در آن است که در پنهان نگاری تناسب موضوع و محتوا میان رمز و میزبان الزامی نیست.

محتوای رمز و میزبان میتواند کاملا مستقل از هم باشند. اما واترمارکینگ محتوای رمز و میزبان بایستی مرتبط باهم باشند.

03

**INVISIBLE
WATERMARK:**

واترمارک نامرعی:

واترمارک نامرعی :

نوعی از واترمارک است که اختصاصاً به منظور احراز هویت کاربر یا مالک یا حتی ایجاد قابلیت افزودن اطلاعات امنیتی یا مقابله با جعل اسناد و اوراق بهادار نظیر اسکناس و چک های بانکی و نظایر آن استفاده میشود.

مفاهیم و اصطلاحات متداول دیگر :

: WATERMARK

به اطلاعات جاسازی شده در محیط میزبان، واترمارک گفته میشود.

: STEGOMEDIUM / HOST

به محیط و یا رسانه ای که واترمارک را در خود جاسازی میکند گفته میشود.

: STEGANOGRAM

به مجموعه ی محیط میزبان و واترمارک جاسازی شده در آن گفته میشود.

: STEGANOANALYSIS

به تجزیه و تحلیل استگانوگرام برای کشف و بازیابی واترمارک گفته میشود.

04

ALGORITHM EVALUATION

PARAMETERS:

پارامترهای ارزیابی الگوریتم:

پارامترهای ارزیابی الگوریتم :

نرم افزار هایی که برای ایجاد و کشف واترمارکینگ استفاده میشوند از الگوریتم های گوناگونی برای پیاده سازی واترمارک استفاده میکنند. در ارزیابی الگوریتم ها از پارامترهای زیر استفاده میشود :

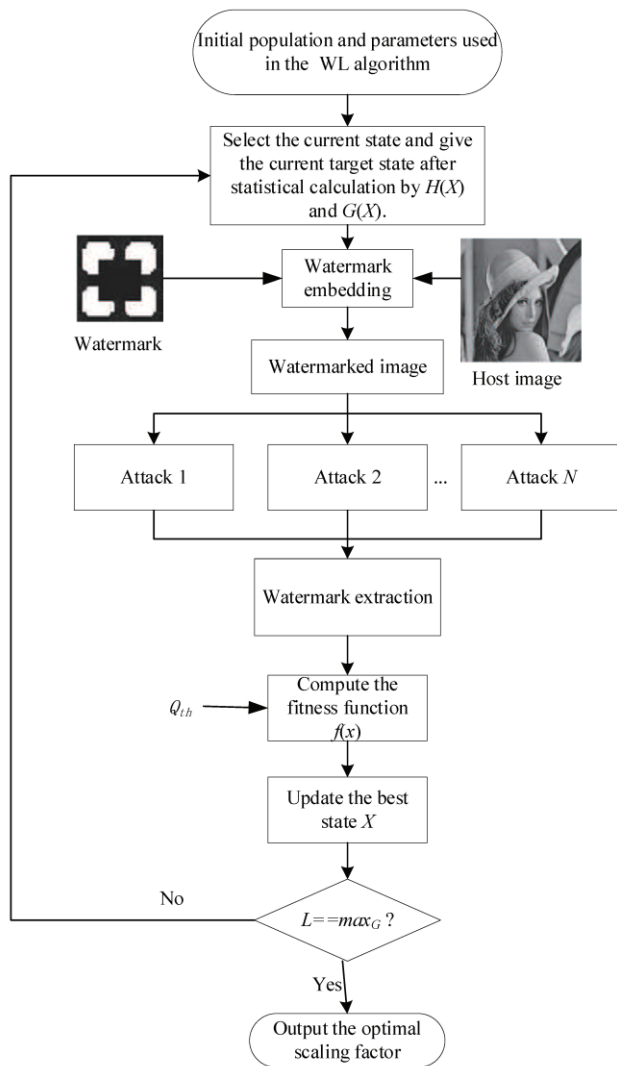
ROBUSTNESS : این پارامتر هرچقدر بالاتر باشد نشانه ی آن است که میزان تخریب و اثرپذیری واترمارک در اثر تغییرات در فایل میزبان کمتر است.

DATA RATE ظرفیت : پارامتری است که مشخص میکند که حداکثر حجم ممکن که میزبان برای واترمارک قادر است فراهم کند چقدر است.

IMPERCEPTIBILITY درجه مخفی سازی : این پارامتر مشخص میکند که حداکثر مجاز اثرگذاری واترمارک در فایل میزبان چقدر است.

SUITABILITY تناسب با فایل میزبان : این پارامتر مشخص میکند که واترمارک با توجه به حجم و محتوا و دیگر ویژگی های خود تا چه حد برای فایل میزبان مناسب است.

SECURITY امنیت : این پارامتر شبیه به درجه مخفی سازی است و تعیین میکند که فایل میزبان تا چه حد میزان وجود واترمارک را میتواند مخفی نگه دارد.



05

DEFINABLE FEATURES IN WATERMARK:

ویژگی های قابل تعریف در واترمارک :

ویژگی های قابل تعریف در واترمارک :

SYMMETRIC : از کلید های یکسان برای جاسازی و بازیابی چند واترمارک استفاده میشود.

ASYMMETRIC : از کلیدهای متمایز برای جاسازی و بازیابی چند واترمارک استفاده میشود.

STEGANOGRAPHIC : به تکنیکی اشاره میکند که در آن کاربران از وجود واترمارک بی اطلاع هستند، این شیوه در تشخیص اثر انگشت استفاده میشود.

NON-STEGANOGRAPHIC : به تکنیکی اشاره میکند که در آن کاربران از وجود واترمارک آگاهی دارند. این روش در ردیابی استفاده های غیر مجاز کاربرد دارند.

ROBUST : تغییر محتوای فایل میزبان به واترمارک خدشه ای وارد نمیکند.

FRAGILE : تغییر محتوای فایل میزبان به واترمارک صدمه میزند یا حتی از بین میبرد آن را.

VISIBLE : واترمارک به وسیله حس بینایی یا شنوایی انسان قابل تشخیص است.

TRANSPARENT / BLIND : واترمارک توسط سیستم بینایی یا شنوایی انسان قابل تشخیص نیست.

PUBLIC : کاربران مجاز به شناسایی و بازیابی واترمارک هستند.

PRIVATE : کاربران اجازه شناسایی و بازیابی واترمارک را ندارند.

06

HOST

ENVIRONMENT:

محیط میزبان:

محیط میزبان :

محیط و رسانه های گوناگونی میتوانند میزبان واترمارک باشند.

محیط میزبان میتواند از نوع رسانه های دیجیتالی یا غیر از آن باشند.

برخی از محیط های متداول عبارت اند از :

عکس - فیلم - رسانه صوتی - رسانه متنی - فایل سرآیند - نرم افزار - سخت افزار - فایل سیستم - دیسک - ژنوم و ...

ملموس ترین و ابتدایی ترین صورت واترمارک دیجیتالی و سنتی، مخفی سازی یک پیغام یا طرح هندسی در یک تصویر ساکن است. نرم افزارهای واترمارک کردن تصاویر امروزه به راحتی قابل تهیه و استفاده است.

واترمارک صوتی و تصویری هردو بر خطا پذیری سیستم شنوایی و بینایی انسان استوار است.

واترمارک متنی نیز میتواند توسط نرم افزار های واژه پرداز تهیه شود. از این واترمارک میتوان برای رمز کردن فایل های موجود در اینترنت استفاده کرد.

اساسا این نوع HTML واترمارک بر سه گونه معنایی، دستوری، یا فضای آزاد تقسیم بندی میگردد.

نمونه ای که در ذیل آورده میشود در تقسیم بندی ها ((NULL CIPHER)) یا رمز پوچ شناخته میشود :

متن میزبان :

**FISHING FRESHWATER BENDS AND SALTWATER COATS REWARDS
ANYONE , FEELING STRESSED RESOURCEFUL ANGLERS USUALLY FING
MASTERFUL LEAPERS FUN AND ADMIT SWORDFISH RANK
OVERWHELMING ANYDAY.**

با کنار هم گذاشتن حروف سوم کلمات، پیغام رمز نمایان میشود :

SEND LAWYERS , GUNS AND MONEY

کاربردهای عملی واترمارکینگ:

Copyright protection – Copy
Protection – Tracking / Product
Serialization –

Tamper proofing – Monitoring –
Concealed communication –

Filtering / Classification – Asset /
Content Management – Rights
management – Remote triggering –
Linking / E-Commerce



استفاده از واترمارکینگ در ایران:

فرآیند چاپ اسکناس احتمالا متداول
ترین و قدیمی ترین استفاده واترمارک
در ایران میباشد. در حالی که در کشور
ما واترمارک میتواند در ارگانهای نظامی
و انتظامی یا مراکز پزشکی با صرف
هزینه ای قابل قبول به کار گرفته شود.
واترمارک همچنین میتواند به اجرا
شدن قوانین مصوب کشوری در مورد
کپی رایت در جهت حفاظت از مالکیت
معنوی کمک کند.



THE END

پایان