ISSN 2395-1621

Watermark Detection and Privacy Preserving Framework

[#1]Sonam Zurange, [#2]Kiran Mungsae, [#3]Dipika Deshmukh, [#4]Prof. Ayesha S.

[1]sonamzurange08@yahoo.com
[2]kiranmungase111@gmail.com

[#12345]Department of Information Technology,
Al-Ameen College of Engineering
Koregaon-Bhima,Tal-shirur Dist.Pune-412216.

ABSTRACT

Now a day's social Networks are more popular. In social sites privacy is a critical issue when the data owners outsource data storage or processing to a third party computing services, such as a server/cloud Users are using multiple applications for social media. Like, Users post their videos on the website and another user download that video do some changes in that video and again upload that video on their own name but it is the copyright. To overcome this problem, we propose a system in that when we/user upload the video that time video is divided in frames and from that frame give watermark on one frame and when that video is upload on website it detect watermark by DCT and register that watermark on particular users name so another user cannot upload same video on her/his name that means it gives copyright protection.

ARTICLE INFO

Article History

Received: 24th May 2016

Received in revised form :

24th May 2016

Accepted: 28th May 2016

Published online :

29th May 2016

Keywords: **Watermark detection, privacy preserving, Secure multiparty computation**

I. INTRODUCTION

Now day's Rapid growth of the Internet and social networks, made very easy for a user to collect a large amount of multimedia data from different sources without knowing the copyright information of those data. Data theft is the major issue for data owners when their data was outsourced in the public or private network. It increased in the field of photography and defensive system. For this as a greater result embedding process is carried out. Embedding a hidden stream of bits in a file is called Digital Watermarking. The file could be an image, audio, video or text. The specifications used for validating watermarking system are, Imperceptibility, Noise ratio and Capacity. An effective digital watermark should be perceptually invisible to prevent obstruction of the original image. Digital watermark should be statistically invisible to prevent detection from the illegal users and it should also be robust to many image manipulations, such as filtering, additive noise, and compression. Techniques have been proposed for a variety of applications, including ownership protection, authentication and access control. The cloud computing technologies are growing, and it is more economical for the data holders to shift data storage or signal processing computations to the cloud instead of purchasing hardware and software by themselves. Ideally the cloud will store the data and perform signal processing or data-mining in an encrypted domain in order to preserve the data privacy. Majorly two types of approaches are determined for secure watermark detection: asymmetric watermarking and zero-knowledge watermark detection. Watermarked copy are publicly available for the usage were the focus to be done only on the watermark pattern, while the privacy of the target media on which watermark detection is performed has received little attention. Performing privacy preserving storage and secure watermark detection can be done using the existing secure watermark detection technologies such as zero-knowledge proof protocols that transform the multimedia data to a public key encryption domain.

II. LITERATURE SURVEY

[1] In this paper, represents that various types of attacks in watermarking and solutions for qualifying the watermarking method are described.
In this paper implementation of basic digital watermarking methods in MATLAB, Fundamental methods in and hybrid domains are described. It also deals with various attacks in watermarking but it's just an initial stage.

[2] In this paper, explains about data privacy in the networks through Secure Multi-Party Computation allows parties with similar background to compute results upon their private data, minimizing the threat of disclosure.

This paper introduces encryption and decryption in embedding watermark through the key access. Quite a few protocols already exist where it has its way on TTP for several layers network in order to ensure privacy.

[3] In this paper, a general framework for robust nonlinear regression that leverages concepts from the field of compressive sensing to simultaneously detect outliers and determine optimally sparse representations of noisy data from arbitrary sets of basic functions.
Author replaces usage of Least Square regression which is not robust to violations. More techniques were introduced robust compressive sensing but all of the techniques does not have residual reduction except few of them.

[4]In this paper author demonstrated that it is possible to substantially decrease noise measurements without sacrificing robustness by leveraging more realistic signal models that go beyond simple sparsity and compressibility by including dependencies between values and locations of the signal coefficients.
This paper only considered the recovery of signals from models that can be geometrically described as a union of subspaces; and not for more complex geometries.

III. PROPOSED SYSTEM

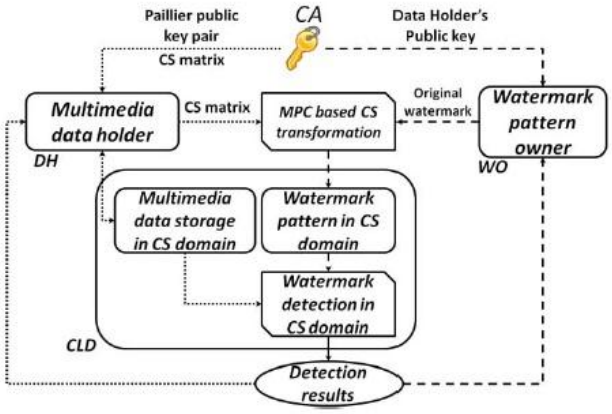


Fig 1. System architecture

Traditional secure watermark detection techniques are designed to convince a verifier whether or not a watermark is embedded without disclosing the watermark pattern so that an un trusted verifier cannot remove the watermark from the watermark protected copy In this paper, we propose a compressive sensing based privacy preserving watermark detection framework that leverages secure multiparty computation and the cloud. It has been shown that many signal processing algorithms performed in the CS domain have very close performance as performed in the original domain .Using random matrix transformation for privacy preserving data-mining has also been proposed, which proposed a random projection data perturbation approach for privacy preserving collaborative data-mining. The proposed a secure image retrieval system through random projection and have proven that the proposed random projection domain multimedia retrieval system is secure under the Cipher text Only Attack model (COA) and the semi-honest model . Furthermore that CS transformation can achieve computationally secure encryption. These works indicate that signal processing or data-mining in the CS domain is feasible and is computationally secure under certain conditions. In our framework, the target image/multimedia data is possessed by the image holder only. A compressive sensing matrix is issued by a certificate authority (CA) server to the image holder. The image holder transforms the DCT coefficients of the image data to a compressive sensing domain before outsources it to the cloud. For secure watermark detection, the watermark is transformed to the same compressive sensing domain using a secure multiparty computation (MPC) protocol and then sent to the cloud. The cloud only has the data in the compressive sensing domain. Without the compressive sensing matrix, the cloud cannot reveal the original multimedia data and the watermark pattern. The cloud will perform watermark detection in the compressive sensing domain. The image data in the compressive sensing domain can be stored in the cloud and reused for detection of watermark from many other watermark owners.

Mathematical Model

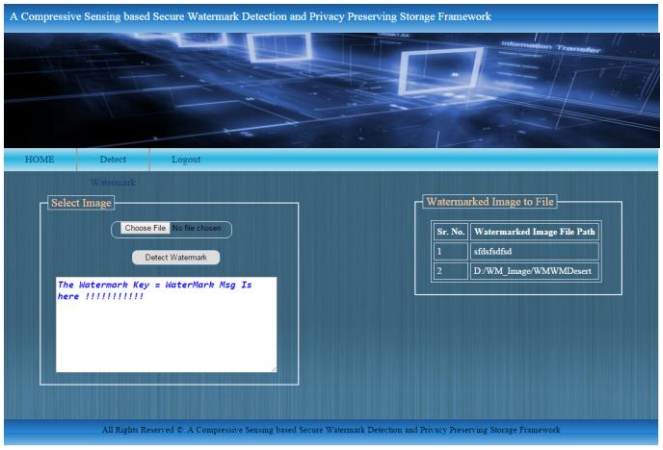
Let 'S' be the "Colored Image"
S= {…….}
Set S is divided into 3 modules
S= {S1, S2, S3}
S1= Communication module
S2= security Module
S3=GUI Module

Identify the inputs.
For S1
Inputs = {X1}
X1= Request for User
Identify the output for S1.
Outputs = {Y1}
Y1= Provide a service
Identify the inputs.

For S2
Inputs = {X2, X3}
Set Theory
X2= User login
X3=Authentication
Identify the output for S2.
Outputs = {Y2, Y3}
Y2= Download authorized data
Y3=Download decoy document
Identify the inputs.

For S3
Inputs = {X4}
X4= Client communicate with server
Identify the output for S3.
Outputs = {Y4}
Y4= Give the corresponding java classes for JSP file.

IV. RESULT



V. CONCLUSION

This system proposes a compressive sensing based secure signal processing framework that enables simultaneous secure watermark detection and privacy preserving storage. Our framework is secure under the semi-honest adversary model to protect the private data.

ACKNOWLEDGMENT

First and foremost our sincerest gratitude to our college, Al-Ameen College of Engineering and our department of Information Technology which has provided the support and equipment we needed to complete our work. We extend my hearty gratitude to our guide, Prof. Ayesha S., who has supported us throughout our research with their patience and knowledge.

REFERENCES

1. “Digital Watermarking Using MATLAB” ,Pooya Monshizadeh Naini University of Tehran, Iran,2009.

2. “A Secure Multi-Party Computation Protocol for Malicious Computation Prevention for preserving privacy during Data Mining”,Dr. Durgesh Kumar Mishra, International Journal of Computer Science and Information Security, Vol. 3, 2009

3. “A General Framework for Robust Compressive Sensing Based Nonlinear Regression”,Brian Moore, Manhattan, Kansas 66506, USA,2009.

4. “Model-Based Compressive Sensing”,Richard G. Baraniuk,Rice university,2009.

5. “Secure Multiparty Computation and Secret Sharing An Information Theoretic Approach”,Ronald Cramer,May 11, 2013.

6. “Study and Implementation of Watermarking Algorithms”,Alekhika Mohanty,Rourkela, India .April 2006.

7. “Watermark Detection Schemes with High Security” ,Liu Yongliang, Institute of Computing Technology, China,(ITCC’05).

8. “Steganography And Digital Watermarking”, Jonathan Cummins, The University of Birmingham,2004.

9. “Digital Watermark Detection in Visual Multimedia Content”,Peter Meerwald, University of Salzburg,2010.

10.”Practical challenges for digital watermarking applications”, Ravi.K.Sharma,USA,2002.

