Security Based Data Transfer and Privacy Storage through Watermark Detection

Gowtham.T[1] Pradeep Kumar.G[2]

[1]PG Scholar, Applied Electronics, Nandha Engineering College, Anna University, Erode, India.
[2]Assistant Professor, Department of ECE, Nandha Engineering College, Anna University, Erode, India.

Abstract—Digital watermarking has been proposed as a technology to ensure copyright protection by embedding an imperceptible, yet detectable signal in visual multimedia content such as images or video. In every field key aspect is the security—Privacy is a critical issue when the data owners outsource data storage or processing to a third party computing service. Several attempts has been made for increasing the security related works and avoidance of data loss. Existing system had attain its solution up to its level where it can be further able to attain the parameter refinement. In this paper improvising factor been made on the successive compressive sensing reconstruction part and Peak Signal-to-Noise Ratio (PSNR).Another consideration factor is to increase (CS) rate through de-emphasize the effect of predictive variables that become uncorrelated with the measurement data which eliminates the need of (CS) reconstruction.

Keywords— Compressive sensing, Peak Signal To Noise Ratio, secure computing service, privacy preserving.

1. INTRODUCTION

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 been 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: Robustness (Against intentional attacks or unintentional ones such as compression), Imperceptibility, Noise ratio and Capacity[3,6,10]. 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[2,5]. Majorly two types of approaches are determined for secure watermark detection: asymmetric watermarking [2] and zero-knowledge watermark detection [5,7,11].

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 [5,7] that transform the multimedia data to a public key encryption domain.

2. RELATED WORKS

[1] In this paper, author represents various types of attacks in watermarking and solutions for qualifying the watermarking method are described.

Pros and cons:

In this paper implementation of basic digital watermarking methods in MATLAB , Fundamental methods in spatial, spectral, and hybrid domains are described. It also deals with various attack in watermarking but its just a initial stage.

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

Pros and cons:

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, author presents 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 basis functions.

Pros and cons:

In this paper, author replaces usage of Least Square (LS)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(M) 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.

Pros and cons:

In this paper author have only considered the recovery of signals from models that can be geometrically described as a union of subspaces; and not for more complex geometries (for example, high-dimensional polytopes, nonlinear manifolds.)

[5] In this paper, author presented watermarking scheme using Genetic Algorithm(GA).Genetic algorithms are a part of evolutionary computing, which is a rapidly growing area of artificial intelligence.*Pros and cons:*

In this paper GA has been applied to clusters of the image instead of the complete image so the processing speed is higher.This paper has poor response for data hiding capacity, using Multiple Optimization GA.

3. PROCEDURAL FLOW OF THE SYSTEM

The proposed framework has several subtasks where each has its specific operation, they are given below

- Watermark insertion and generation
- Embedding Process
- Watermark Extraction
- Decoding Process

3.1 Watermark insertion and generation

In the initial stage select the file which been going to watermarked and also the data that to be embedded in it. Later DWT of an image and the watermark pattern to be calculated which resembles like picture matrix.

Watermark insertion involves watermark generation and encoding process. Watermark Generation: Each owner has a unique watermark or an owner can also put different watermarks in different objects, the marking algorithm incorporates the watermark into the object. The verification algorithm authenticates the object determining both the owner and the integrity of the object. The watermark can be a logo picture, sometimes a binary picture, sometimes a ternary picture; it can be a bit stream or also an encrypted bit stream etc. The encryption may be in the form of a hash function or encryption using a secret key.

The watermark generation process varies with the owner. In the encoding process both the original data and the watermark data are passed through the encoding function. The payload signal and the original host signal now together occupy space, which was previously occupied only by the host signal. For this purpose either the original data is compressed or redundancy in digital content is explored to make space for the payload.

3.2Embedding Process

It provides the action of mixer where it has various algorithms for embedding process. These are commonly divided into three categories (1)

- Watermarking in Spatial Domain
- Watermarking in Spectral Domain
- Watermarking in Hybrid Domain

There are several transforms that brings an image into frequency domain. Among most common of those, we can mention are: Discrete Cosines Transform (DCT) and Fast Fourier Transform (FFT). In frequency domain, coefficients are slightly modified. This will make some unnoticeable changes in the whole image and makes it more robust to attack compared to what we have in spatial methods. Coefficients are modified according to the stream bits of the message using to the equation

$C_{AW} = C_A(1 + \alpha \cdot (Wi))$

In which C_{AW} is the watermarked coefficient, C_A is the original one, α represents watermarking strength (e.g. 0.3), and Wi is the corresponding bit of the message data. Embedding can be done to obtain higher PSNR values (higher fidelity) and higher NCC values (better robustness to attacks)[10].

3.3 Watermark Extraction

Extraction is achieved in twosteps[1]. First the watermark is extracted in the decoding process and then the authenticity is established in the comparing process. After the embedding process through key providence now the extraction of the image takes place. Inverse action of image scan been done and obtain IDCT of an image. The decoding process can be itself performed in two different ways. In one process the presence of the original unwatermarked data is required and other where blind decoding is possible. A decoder function takes the test data (the test data can be a watermarked or un-watermarked and possibly corrupted) whose ownership is to be determined and recovers the payload.

3.4Data Admin(Holder)

DH (e.g., media agencies), when it collects a large volume of multimedia data from the Internet and stores their encrypted versions in the CLD, it wants to make sure those multimedia can be edited and republished legally.

3.5 Watermark Owner Module

Watermark owners (WOs) are also the content providers who distribute their watermarked content (the watermark embedding is performed by WO before the contents are published). WOs always want to know if their contents are legally used and republished.

4 Compressive Sensing

The compressive sensing theory asserts that when a signal can be represented by small number of nonzero coefficients, it can be perfectly recovered after being transformed by a limited number of incoherent, non-adaptive linear measurements. Most of the literature of compressive sensing has focused on improving the speed and accuracy of compressive sensing reconstruction take some initial steps towards a more general framework called compressive signal processing (CSP), which shows fundamental signal processing problems such as detection, classification, estimation, and filtering can be solved in the compressive sensing domain.

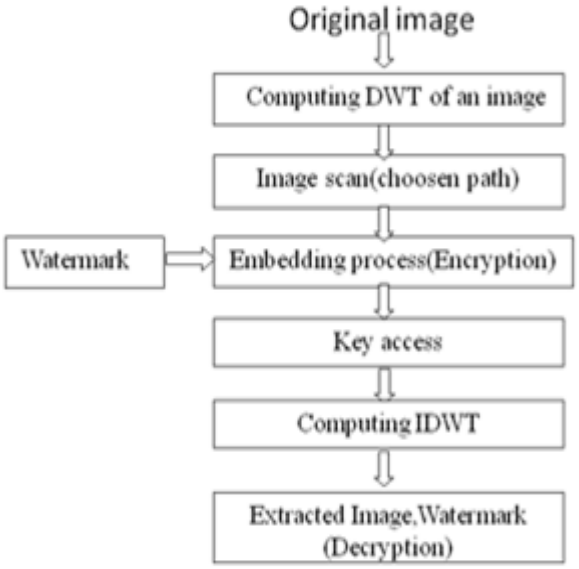


Figure.1Architecture of the proposed framework

DCT of the image been obtained using the formula

FDCT

$$v(k,l) = \alpha(k)\cdot\alpha(l)\sum_{m=0}^{N-1}\sum_{n=0}^{N-1} u(m,n)\cdot\cos\left[\frac{(2m+1)k\pi}{2N}\right]\cos\left[\frac{(2n+1)l\pi}{2N}\right]$$

where k, l = 0, 1, ... N-1.

IDCT

$$u(m,n) = \sum_{k=0}^{N-1}\sum_{l=0}^{N-1} \alpha(k)\cdot\alpha(l)\cdot v(k,l)\cdot\cos\left[\frac{(2m+1)k\pi}{2N}\right]\cos\left[\frac{(2n+1)l\pi}{2N}\right]$$

where m, n = 0, ... N-1

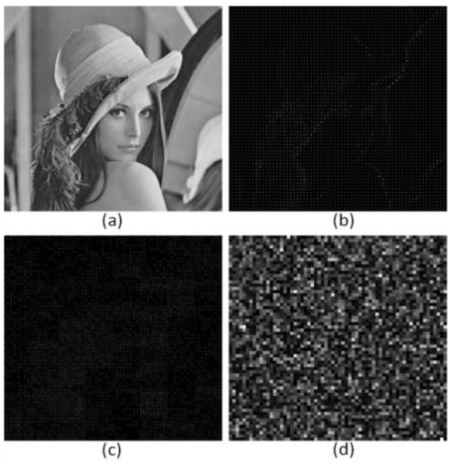


Figure.2(a)Original image; (b)Image in 8×8 DCT domain; (c)DCT coefficient after CS transformation; (d)Image reconstruction with the wrong CS matrix. (CS rate 1.0 is chosen here, similar effects are observed under other CS rates).

In existing system DCT coefficient of each piece of the image will form a vector and be transformed to a CS domain with the same CS rate but using different CS matrices[11].

For privacy preserving storage, since the DCT coefficients are not perfectly sparse, the CS reconstruction will introduce distortion to there constructed image, especially when CS rate is low. In order to have a good quality image after the CS reconstruction, the CS rate needs to be high. In the existing system experimental result shows that the PSNR(Peak Signal-to-Noise Ratio) is around 65 after the CS transformation/reconstruction process when the CS rate is 0.8. Even when the CS rate is set to 1.0, the CS reconstruction algorithm (Orthogonal Matching Pursuit) still introduces distortion as we can see the PSNR is around 45. However, it should be noted that when the CS rate equals1.0,theoriginal DCT coefficient can be recovered perfectly given the inverse of the CS matrix, in which case CS reconstruction is not necessary.

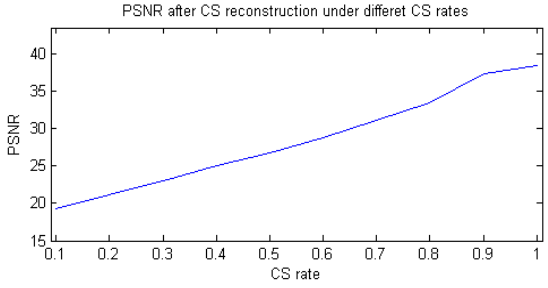


Figure.3CS reconstruction distortion when AC coefficients are transformed to the CS domain.

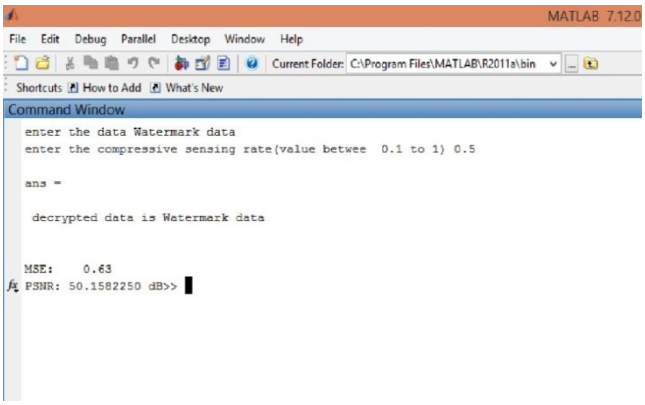


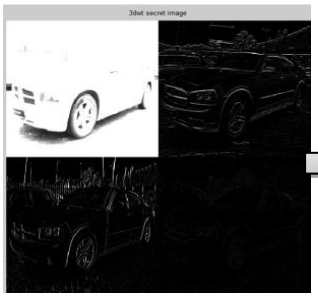
Figure. 4Calculation of PSNR and MSE value through simulation

5.EXPERIMENTAL RESULTS

PARAMETERS	VALUES
Protocol	Multi Party Computation(MPC)
Algorithm	DWT
Image Size	1024 x 1024
Character Length	Upto 100
Key	Public or Private

TABLE 1:Simulation Parameters

In proposing system instead of using DCT we would like to develop system with the usage of DWT for the image coefficients were it been segregated into various image blocks.



HH (High High)	LH (Low High)
HL (High Low)	LL (Low Low)

Figure. 5Energy segments of the processed image

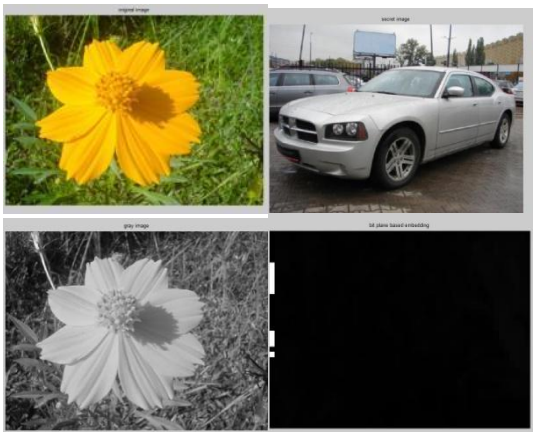


Figure. 6a).Original image b).Secret image c).Gray scale of original image d.)Bit plane slicing of secret image

In the above image work been carried out with DWT process through spatial domain and frequency domain. Fig(6.b)shows the gray scale of the original image in that color of the image been transformed to gray value and Fig(6.d)shows the bit plane slicing of secret image.(In this figure shown is 6-bit plane slicing).

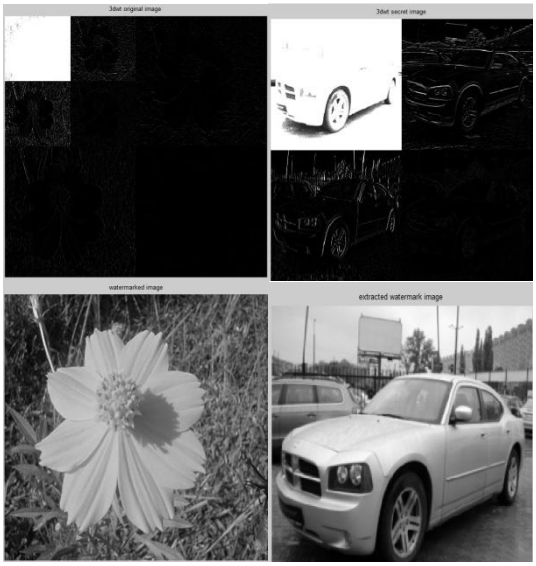


Figure. 7a).DWT of original image(3 bit plane) b).DWT of secret image(3 bit plane) c).Watermarked image d).Extracted watermark image

6.CONCLUSION

The main aim of the project is to improve the security of the data where user prefers to obtain it. Further analysis being carried out to increase CS rate through DWT process. Increase in CS rate reduces the reconstruction of the image where image would be recovered perfectly with the image coefficients.

In this paper considering existing system parameters as the guideline, work been takes place for improving the

performance of the system with the available methods and algorithms.

ACKNOWLEDGEMENT

The authors would like to thank the anonymous reviewers for their constructive comments that greatly improved the quality of this paper.

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.

11. "A Compressive Sensing based Secure Watermark Detection and Privacy Preserving Storage Framework", *Qia Wang, Wenjun Zeng*,ieee transactions on image processing, vol. 23, no. 3, march 2014.

