American Journal of Pharmaceutics.
1(1):7-10, August 2019

Review paper

A Survey on Compressed Sensing Based Watermarking.

[1]G.Suneetha Devi, [2] Shaik Taz Mahaboob, [3] K.Siva Chandra.

[1]P.G.Scholar, Dept. of E.C.E., JNTUACEP, Pulivendula, Andhra Pradesh, India.
[2]Assistant Professor, Dept. of E.C.E., JNTUACEP, Pulivendula, Andhra Pradesh, India.
[3]Assistant Professor, Dept. of E.C.E., JNTUACEP, Pulivendula, Andhra Pradesh, India.

To cite this article: G.Suneetha Devi, Shaik Taz Mahaboob and K.Siva Chandra. A survey on compressed sensing based on water marking. American Journal of Nano Science and Technology, 1(1):7-10, May-June 2019

Email: suneethagavvala1@gmail.com

Received: 18th May 2019.| Revised: 28th May 2019.| Accepted: 10th June 2019.

Abstract: The main aim of this paper is to explain different watermarking techniques. It is a new technique for simultaneous data sampling and compression. A novel method has been proposed named, distributed compressed sensing for image using block measurements data fusion. Firstly, original image is divided into small blocks and each block is sampled independently using the same measurement operator, to obtain the smaller encoded sparser coefficients and stored measurements matrix and its vectors. Secondly, original image is reconstructed using the block measurements fusion and recovery transform. Finally, several numerical experiments demonstrate that our method has a much lower data storage and calculation cost as well as high quality of reconstruction when compared with other existing schemes. It is used in secret image sharing schemes to solve problems raised by the enlarged data. The paper focused on reduce the amount of data need to be processed and effectively shorten the execution time.

Keywords: DCT, image sharing, watermarking, compressed sensing, PSNR.

1. Introduction

Data hiding is a technique for embedding information into covers such as image, audio, and video files, which can be used for media notation, copyright protection, authentication, etc. The most data hiding approach is to embed messages into the cover media to generate the marked media. Digital watermarking techniques can be classified into two categories, spatial domain and frequency domain. The spatial domain watermarking embeds the watermark by Customize the intensity and the colour value of some selected pixels and in frequency domain watermark is embedded into frequency coefficients of the host image. In a spatial technique, we use Least Significant Bit modification (LSB). Frequency domain we use discrete cosine transform (DCT), Discrete Wavelet Transform (DWT) And Discrete Fourier transform (DFT) combination of DCT and DWT.

1.1. Discrete cosine transform

DCT transformation most popularly used transform and it is based on cosine functions **[1].** DCT plays a very important role for energy compaction property which is most important for image compression .The 2D discrete cosine transform (2D DCT) can be expressed by

$$D(i,j) = \frac{1}{\sqrt{2N}} c(i)c(j) \sum_{Y=0}^{N-1} \sum_{y=0}^{N-1} p(x,y) \cos\left(\frac{(2x+1)i\pi}{2N}\right) c\,os\left(\frac{(2y+1)j\pi}{2N}\right) \quad (1)$$

$$C(u) = \begin{Bmatrix} \frac{1}{\sqrt{N}} & if \quad u=0 \\ 1 & if \quad u=0 \end{Bmatrix} \quad (2)$$

1.2. Discrete wavelet transform

Discrete Wavelet Transform (DWT) of a signal x (n) is obtained by using Filter banks for wavelet transform **[2].** First, the data are passed through a low pass filter and has impulse response g (n) giving particular coefficients. Signal decomposition by using a high pass filter h (n), giving the more no of coefficients. The low pass filter gives approximate coefficient

$$y_{low}[k] = \sum_n x(n).g(2k-n) \quad (3)$$

$$y_{high}[k] = \sum_n x(n).h(2k-n) \quad (4)$$

LL	LH
HL	HH

Figure1.WaveletDecomposition Using Four Sub Bands wavelet transform decomposes an image in to four sub bands

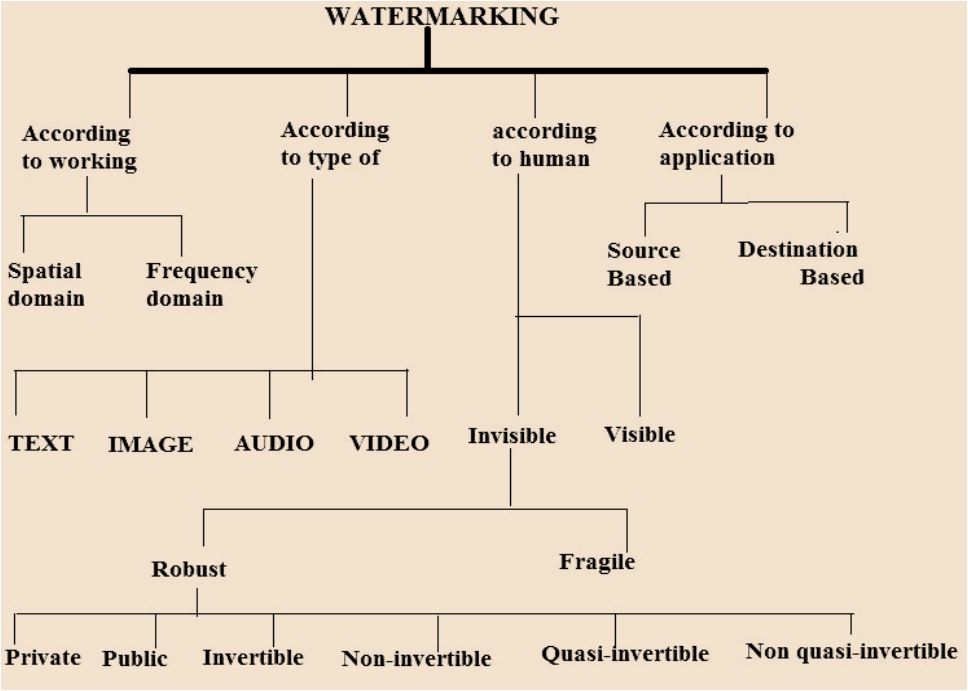

Figure – 2: Different water marking techniques

2. Watermarking applications

Before starting the talk on watermarking calculations we examine the applications. The fundamental utilizations of advanced watermarking are examined here.

2.1. Copyright Protection

Watermarking can be accustomed to securing redistribution of copyrighted material over the depended arrange like the Internet or shared (PP) systems. Content mindful systems (pp) could fuse watermarking advances to report or sift through copyrighted material from such systems.

2.2. Content Archiving

Watermarking can be utilized to embed advanced question identifier or serial number to help file computerized substance like pictures, sound or video. It can likewise be utilized for arranging and sorting out computerized substance. Ordinarily advanced substance is distinguished by their document names; be that as it may, this is an exceptionally delicate procedure as record names can be effectively changed. Henceforth installing the protest identifier inside the question itself lessens the likelihood of altering and subsequently can be viably utilized as a part of filing frameworks.

2.3. Meta-information Insertion

Meta-information alludes to the information that portrays information. Pictures can be named with its substance and can be utilized as a part of web crawlers. Sound documents can convey the verses or the name of the artist. Writers could utilize photos of an episode to embed the main story of the individual news. Therapeutic X-beams could store understanding records.

2.4. Communicate Monitoring

Communicate Monitoring alludes to the procedure of cross-confirming whether the substance that should be a supporter (on TV or Radio) has truly been telecaster or not. Watermarking can likewise be utilized for communicated observing. This has significant application is business and communicating where the substance who is publicizing needs to screen whether their notice was really telecaster at the correct time and for the right term.

2.5. Alter Detection

The computerized substance can be recognized for altering by inserting delicate watermarks. In the event that the delicate watermark is devastated or debased, it showed the nearness of altering and henceforth the computerized content can't be trusted. Alter recognition is critical for a few applications that include profoundly delicate information like satellite symbolism or therapeutic symbolism. Alter recognition is additionally helpful in an official courtroom where computerized pictures could be utilized as a measurable apparatus to demonstrate whether the picture is altered or not.

2.6. Advanced Fingerprinting

Advanced Fingerprinting is a method used to identify the proprietor of the computerized content. Fingerprints are one of a kind to the proprietor of the advanced substance. Henceforth a solitary computerized question can have distinctive fingerprints since they have a place with various clients.

3. Hiding techniques

3.1. Steganography and Cryptography

Fadhil Salman et al (2010) had used an idea to hide a text in an image file in such a way that precludes, as much as possible, any suspicion of the hidden text. For this authors had used the combined feature of steganography and cryptography. The proposed system depends upon DCT Quantization through steganography process. Authors use two levels of security: the RSA algorithm and the digital signature. Finally, the image is stored in a JPEG format. In this case, the secret message will be looked at as plaintext with digital signature while the cover is a coloured image. The proposed system can be distinct as asymmetric key Steganography **[3].**

3.2. Steganography Using LSB Technique and Pseudo-Random

Devi, Kshetrimayum Jenita (2013) had proposed a technique that is based on image steganography .this technique was a combination of Least Significant Bits (LSB) techniques and pseudo-random encoding technique and used to enhance the security of the communication of images. In the LSB approach, the Least Significant Bits (LSB) of the cover image with the Bits of the messages to be hidden without destroying the property of the cover image significantly. In the Pseudo-Random technique, Pseudo-Random Number Generator uses random-key as a seed during the embedding process. While embedding messages inside the cover image both the techniques use a stego-key this stego-key reduces the chance of getting attacked by the attacker **[4].**

3.3. Visual secret sharing scheme for multiple secrets without pixel expansion

Lin, T.L et al. presented multiple secrets-sharing schemes with no pixel expansion in 2010. They presented two secrets in which there is no pixel expansion. Also, it does not need a codebook to encode the secret images. It was observed that the pixel expansion was 4 times less as compared to the earlier schemes after applying aspect ratio constraints. Through the separation and disguising processes, two shares where meaningless images individually. They did not disclose any data of the secret images. Therefore, the security rule of VSS schemes is obeyed. For recovering the secret, both shares were overlapped and HVS was able to identify the recovered image. This scheme resolved the serious pixel expansion problem. Authors also carried out a new study that differs from the former schemes **[5].**

3.4. Reversible Data hiding

Z. Ni, Y. Shi, N. Ansari, and S. Wei, **[6]** have proposed a system that performs the Reversible Data hiding by using the histogram shift operation for RDH. In this system used the spare space for embedding the data by shifting the bins of grayscale values. The embedding capacity measured by the use of a number of pixels in peak point. This system has some benefits such as it is simple and has constant PSNR ratio, capacity is high and distortion is very low. This system has some disadvantages such as more time consuming while searching the image number of times.

3.5. Symmetric Key Cryptographic Technique

Paul, Manas, and Jyotsna Kumar Mandal (2013) proposed a technique based on symmetric key cryptographic on session bit level .and this method is known as Spiral Matrix Based Bit Orientation Technique (SMBBOT). SMBBOT consider the binary bit stream as an input plain text. This stream is divided into conveniently sized blocks with variable lengths stream for the duration of encryption. Bits of these blocks are taken from MSB to LSB to fit into a square matrix. This square matrix breaks into 2x2 sub-matrices. To form the encrypted binary string. Bits are taken column-wise from all 2x2 sub-matrices from this encrypted binary string cipher text is generated. The cipher text is considered as binary bit string for decryption process. After taking the bits from the square matrix the decrypted binary string is formed and following the reverse concept of Spiral Matrix. The decrypted binary form is used to regenerate plain text **[7].**

Table-1: Review Summary

S.no	Author	Method used	Highlights
1	Fadhil Salman et.al[1]	RSA algorithm	Secret image will be looked as plain text with digital signature while the cover is a color image
2	Devi, kshetrimayum jenita (2013)	Pseudo-Random encoding technique	stego key reduces the chance of getting attacked by the attacker
3	Lin T. L et al.	Without pixel expansion	HVS was able to identify the recovered image
4	Z. Ni, Y. shi, N. Ansari	Reversible data hiding	Constant PSNR ratio, capacity is high and distortion is very low
5	Paul, manas, and Jyotsnakumar mandal (2013)	Spiral matrix based bit orientation technique	Decrypted binary form is used to regenerate plain text

4. Conclusions

On analyzing different types of techniques and their approaches towards different segments of the image by increasing the capacity of embedded in a secret image. We find that this method effectively reduces the data volume that needs to be processed, cuts execution time of image sharing and restoring algorithm and alleviates transmission burden and storage overhead. In order to further improve the visual quality of the reconstructed image, we will study how to get the more sparse linear representation of the image signal and improve the performance of the reconstruction algorithm.

References

1. G.Richard, Baraniuk, E.Candes and Robert Nowak. Compressive sampling. IEEE signal processing magazine, 3:12-13, 2008.
2. Zhenghua Zou, Xinji Liu and Shu-Tao Xia. A comparative study of wavelets and adaptively learned dictionary in the compressive image sensing. IEEE11th International Conference on signal processing, 2:302-309,2002.
3. Abed, Fadhil Salman and Nada Abdul Aziz Mustafa. A Proposed Technique for Information Hiding Based on DCT. Int. J. Adv. Comp. Techn,2(5):140-152,2010.
4. Devi, Kshetrimayum Jenita. A Secure Image Steganography Using LSB Technique and Pseudo Random Encoding Technique. Ph.D. Thesis, National Institute of Technology, Rourkela, 2013.
5. Lin, Tsung-Lieh. A novel visual secret sharing scheme for multiple secrets without pixel expansion. Expert systems with applications, 37(12):7858-7869,2010.
6. Z.Ni,Y.Shi.Y,N.Ansari and S.Wei. Reversible data hiding. IEEE Trans.Circuits Syst. Video Technol., 16(3):354– 362, Mar.2006.
7. Paul, Manas and Jyotsna Kumar Mandal. A Novel Symmetric Key Cryptographic Technique at Bit Level Based on Spiral Matrix Concept. arXiv preprint, 1305-1314,2013.
8. C.C.Thien and J.C.Lin. An image-sharing method with user-friendly shadow images. IEEE Transactions on Circuits and Systems for Video Technology, 13(12):1161 -1169,2003.
9. C.C.Lin and Tsai Who. Secret image sharing with steganography and authentication. Journal of Systems and Software, 73(3):405-414, 2014.
10. C.N.Yang, T.S.Chen, Yu KH and C.C.Wang. Improvements in image sharing with steganography and authentication: Journal of Systems and Software, 80(7):I070-1076,2007.
11. P.Y.Lin, J.S.Lee and C.C.Chang. Distortion-free secret image sharing mechanism using the modulus operator. Pattern Recognition Letters, 42(5):886-895,2009.
12. P.Y.Lin and C.S.Chan. Invertible secret image sharing with steganography. Pattern Recognition Letters, 31(13):1887-1893,2010.
13. C.C.Thien and J.C.Lin. Secret image sharing. Computers & Graphics, 26(5):765 - 770, 2002.
14. Zhou Qinglei and Guo Rui. Efficient and scrambling-free secret image sharing method. computer engineering, 36(9):126-128,2010.
15. R.J.Wang and C.H.Suo. Secret image sharing with smaller shadows. Pattern Recognition Letters, 27(6):551-555,2010.
16. J.B.Feng, H.C.Wu, C.S.Tsai and Y.P.Chu. A new multi-secret image sharing scheme using Lagrange's interpolation. The Journal of Systems and Software, 76(3):327-339,2005.