Journal of King Saud University – Computer and Information Sciences 31 (2019) 436–451

Contents lists available at ScienceDirect

Journal of King Saud University – Computer and Information Sciences

journal homepage: www.sciencedirect.com

A hybrid watermarking scheme with CS theory for security of multimedia data

Rohit Thanki [a,*], Vedvyas Dwivedi [a], Komal Borisagar [b]

[a] Faculty of Technology and Engineering, C. U. Shah University, Wadhwan City, Gujarat, India
[b] Atmiya Institute of Technology and Science, Rajkot, Gujarat, India

ARTICLE INFO

Article history:
Received 30 January 2017
Revised 29 April 2017
Accepted 12 May 2017
Available online 19 May 2017

Keywords:
Compressive sensing
Curvelet
Image
Multimedia
Video
Watermarking

ABSTRACT

A hybrid watermarking scheme for multimedia data such as digital image, digital video is proposed in this paper. The scheme utilizes various image processing transforms and Compressive Sensing (CS) to achieved fragility and security for multimedia data. The compressive sensing is applied on the singular value of wavelet coefficients of watermark image to get the CS measurements. These CS measurements are embedded with embedding factor into the hybrid coefficients (high frequency curvelet coefficients of DT coefficients) of the host medium. In the proposed scheme, host medium may be digital image or video. The generated watermarked data have different security layers such as four levels from CS such as knowledge of transform basis matrix, measurement matrix, orthogonal matrices, information of wavelet basis matrix and one level from watermarking such as embedding factor. The scheme offers fragility and security to multimedia data against various standard watermarking attacks such as signal processing attacks, geometric attacks, and compression attacks. This scheme can be provided high payload capacity and used for host multimedia authentication. A comparison of proposed scheme with existed schemes shows that the proposed scheme performed faster and better than existed schemes available in the literature.

1. Introduction

Nowadays, multimedia data such as images, videos, and texts are transferred over internet, mobile, and cloud. Many multimedia data are recreated and redistributed by imposter without any copyright. Also, the imposter can use copyright materials at any place in the world by using internet, mobile and cloud access. This is creating an issue of copyright protection and authentication for multimedia data when it is transferred over the internet, mobile, and cloud. The watermarking technique is one of solution for copyright authentication and protection for multimedia data (Langelaar et al., 2000).

The watermarking technique is divided into two types such as robust type watermarking and fragile type watermarking (Langelaar et al., 2000). The robust type watermarking is provided robustness against any attacks or manipulation. The meaning of robustness in watermarking is that extraction of watermark data is possible from watermarked data when watermarked data is corrupted or modified. This type of watermarking technique is used for copyright protection of multimedia data. The fragile type watermarking is provided fragility against any attacks or manipulation. The meaning of fragility in watermarking is that extraction of watermark data is not possible from watermarked data when watermarked data is corrupted or modified. This type of watermarking technique is used for copyright authentication of multimedia data.

The watermarking technique can be design in various domains such as spatial, transform, hybrid and sparse (Thanki and Kothari, 2016). The spatial domain techniques have less robust against any manipulation or attack (Langelaar et al., 2000; Thanki and Kothari, 2016). The transform domain techniques are far better than spatial domain techniques. So far robustness is concerned in spatial domain techniques. That is the reason why transform domain watermarking techniques are used to prefer for the security of multimedia data (Thanki and Kothari, 2016). But the transform domain techniques have limited payload capacity (Thakkar and Srivastava, 2016). The hybrid domain techniques are extending

* Corresponding author.
E-mail addresses: rohitthanki9@gmail.com (R. Thanki), vedvyasdwivediphd@gmail.com (V. Dwivedi), krborisagar@aits.edu.in (K. Borisagar).
Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.jksuci.2017.05.005
1319-1578/

version of transform domain techniques in which two or more than two image transforms are used (Kothari, 2013). The hybrid domain techniques are provided more imperceptibility to multimedia data compared to transform domain techniques. The spatial domain techniques, transform domain techniques, and hybrid domain techniques are mainly used for copyright protection of multimedia data. The sparse domain techniques are new techniques which are utilized compressive sensing theory with watermarking technique. These techniques are provided better authenticity and payload capacity compared to above three techniques. Any watermarking scheme has certain requirements such as robustness, perceptibility and payload capacity when it is designed for multimedia data. These three requirements have a trade-off triangle. This triangle is shown in Fig. 1. Fig. 1 shows that to achieve two of the three requirements, the third one should be traded off (Kothari, 2013). For example, to achieve high perceptibility and good payload capacity, one needs to throw out robustness requirement. So that, a hybrid domain based and sparse domain based watermarking scheme is proposed in this paper.

There are various watermarking schemes are proposed and presented by researchers for the security of multimedia data in last decades. The various spatial domain techniques for security of multimedia data are proposed using LSB substitution, correlation properties of different noise sequences for digital videos and images (Thanki and Kothari, 2016; Kothari, 2013; Ramalingam, 2011; Koz and Alatan, 2008; El-Gayyar, 2006; Chan and Cheng, 2004; Bangaleea and Rughooputh, 2002; Lee and Chen, 2000; Langelaar et al., 2000). These techniques are used for copyright authentication of multimedia data. But these techniques have less robust against various attacks. The various transform domain techniques are proposed by various researchers which overcomes the some limitation of spatial domain techniques (Gupta and Raval, 2012; Kamlakar et al., 2012; Essaouabi and Ibnelhaj, 2009; Preda and Vizireanu, 2007; Elbasi, 2007; Fan and Yanmei, 2006; Raval and Rege, 2003; Dajun et al., 2003; Serdean et al., 2002; Podilchuk and Delp, 2001; Arena et al., 2000; Hernandez et al., 2000; Cox et al., 1997). In these techniques, various image transform coefficients such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) are used for watermark embedding. These techniques are providing more robustness and less payload capacity compared to spatial domain techniques. These techniques are mostly robust techniques and used for copyright protection of multimedia data.

The various hybrid domain techniques are proposed by various researchers which utilizes two or more than two image transform coefficients (Kothari, 2013; Sridevi et al., 2010; Raghavendra and Chetan, 2009; Santhi and Thangavelu, 2009; Mostafa et al., 2009; Bhatnagar and Raman, 2009; Mansouri et al., 2009; Rajab et al., 2008; Dili and Mwangi, 2007; Huang and Guan, 2004; Ganic and Eskicioglu, 2004; Ejima and Miyazaki, 2000). In these techniques, various combination of image transforms such as DCT + DWT, DWT + SVD, DCT + DWT + SVD are used for watermark embedding. These techniques are achieved more robustness and imperceptibility compared to transform domain techniques and spatial domain techniques. The limitation of existed hybrid domain techniques is less payload capacity.

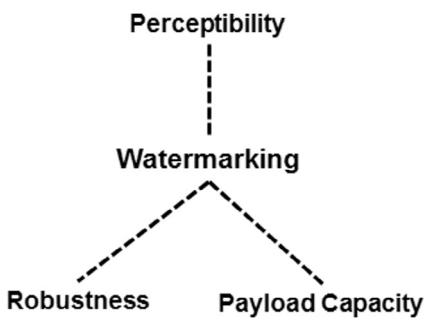

Fig. 1. Requirements of Digital Watermarking Technique.

Donoho and Candes have introduced new signal acquisition theory which is namely as Compressive Sensing (CS) theory (Donoho, 2006; Candes, 2006). This theory is breakthrough Shannon-Nyquist sampling technique. CS theory based watermarking techniques are known as sparse domain techniques because, in these techniques, sparse information of watermark is used. The various sparse domain techniques for security of multimedia data are proposed in last ten years (Yang et al., 2015; Liu et al., 2014; Orovik and Stankovic, 2013; Zang et al., 2013; Yamac et al., 2013; Tiesheng et al., 2013; Fakhr, 2012; Veena et al., 2012; Raval et al., 2011; Zhang et al., 2011; Tagliasacchi et al., 2009; Sheikh and Baraniuk, 2007). The CS theory based techniques have explored CS theory features such as data reduction and computational security. The CS theory based techniques are used for image tamper identification and authentication. The robust CS theory based techniques are proposed by Tiesheng et al. (2013), Fakhr (2012) and Veena et al. (2012) for multimedia data protection. Sheikh and Baraniuk proposed first sparse domain technique in 2007. The limitation of existed sparse domain techniques has less payload capacity.

After above discussion on review papers, it is cleared that most existed watermarking techniques are designed and implemented for copyright protection of multimedia data. There are fewer members of watermarking techniques are designed and implemented for copyright authentication of multimedia data. Also, the payload capacity of existed watermarking techniques is less. Thus, a hybrid CS theory based non-blind hybrid watermarking scheme is proposed which focuses on authentication of multimedia data and provided high payload capacity in this paper. The reason behind proposed this scheme is that most existed hybrid techniques have less payload capacity.

Literature also shows that existed transform domain techniques and existed sparse domain techniques are offered more robust with limited payload capacity (Thakkar and Srivastava, 2016; Kothari, 2013; Tiesheng et al., 2013; Raval et al., 2011; Mansouri et al., 2009; Raval and Rege, 2003). These existed techniques are provided security to multimedia data using the small size of watermark information with large execution time and less imperceptibility.

To overcome the drawbacks of existed transform domain techniques, existed hybrid domain techniques and existed sparse domain techniques, a hybrid watermarking scheme using DCT, DWT, SVD, and Curvelet transform with a combination of CS theory is proposed in this paper. In this scheme, the CS theory is applied on watermark image to generate CS measurements. The discrete wavelet transform (DWT) and singular value decomposition (SVD) is used for CS measurements. The high frequency curvelet coefficients of discrete cosine transform (DCT) coefficients of host image are modified according to sparse data of watermark image to generate watermarked image. In this proposed scheme, high frequency coefficients of host medium are chosen for achieved fragility of the algorithm. Because when watermarking attacks applied on watermarked image, then high frequency coefficients are mostly affected and became corrupted due to attacks (Raval and Rege, 2003). The reason behind using CS theory in proposed scheme is that this step is provide added one additional security layer in proposed watermarking scheme and provides security to watermark data before embedding. Also, in this proposed scheme, CS measurements of the watermark data is generated using two image processing transforms. While in existed sparse techniques, CS measurements of the watermark data is generated using single

image processing transforms. The main contribution of this proposed scheme is explored sparseness of various image processing transforms and used CS theory to provided high payload capacity with authenticity to multimedia data.

This proposed scheme offers good execution time and authentication to multimedia data. In this proposed scheme, Gaussian measurement matrix A is applied on the singular value of wavelet coefficients to get CS measurements. The proposed scheme is analyze using various host images with various frequency components. The orthogonal matching pursuit algorithm (Tropp and Gilbert, 2007) is used for reconstruction of watermark image from extracted CS measurements at detector size. This algorithm is selected because it has better computational time and easy to implemented.

The rest of paper is organized as follows: in Section 2, mathematics and information on compressive sensing theory, various transforms such as DCT, DWT, SVD and curvelet transform is presented. Section 3 gives information on the implementation of proposed scheme. The result and discussion for fragility and performance of proposed scheme for various watermarking attacks are given in Section 4. The application scenario of proposed scheme for the security of multimedia is presented in Section 5. Finally, the conclusion is given in Section 6.

2. Preliminaries

2.1. Compressive sensing (CS) theory

An image f can become sparse image when only a few non-zero elements are presented in the image. The image f can be converted into a sparse image by applying image transform basis matrix. The image has x non-zero coefficients (sparse coefficients) are represented as

$$x = \Psi \times f \times \Psi^{*} \tag{1}$$

where x is the sparse coefficients, Ψ is the transform basis matrix, Ψ^{*} is the inverse transform basis matrix.

The CS measurements of image using compressive sensing represented by using following equation

$$y = A \times x \tag{2}$$

where y is the CS measurements, A is known as measurement matrix.

To reconstruction of an image from CS measurements, various CS recovery algorithms are available in the literature (Donoho, 2006; Candes, 2006; Tropp and Gilbert, 2007). A greedy algorithm such as orthogonal matching pursuit (OMP) is used which is introduced and designed by Tropp and Gilbert (2007). It is used in this paper for the extraction of sparse coefficients from CS measurements. This algorithm is defined by three basic steps which are matching, orthogonal projection and residual update and recovering one non-zero sparse coefficient in each iteration. It can be mathematically explained using below equation:

$$x^{*} = \arg\min_{x} \|y - Ax\| \tag{3}$$

where x^{*} is extracted sparse coefficients which provide the extracted from the CS measurements y.

2.2. Various transforms

In this paper, various image processing transforms such as DCT, DWT, SVD and Curvelet transform are used for implementation of proposed scheme. The DCT and curvelet transform are used for watermark embedding whereas DWT and SVD are used for generation of sparse coefficients. The information of these transforms is given below.

2.2.1. Discrete cosine transform (DCT)

The discrete cosine transform decomposes the image into various frequency coefficients such as low frequency, mid-band frequency, and high frequency. The discrete cosine transform can apply various ways on the image such as block-wise process and without block-wise process. The DCT coefficients of the image using block-wise process and without block-wise are shown in Fig. 2.

The DCT is mainly used in watermarking for convert image into its transform domain. The mostly watermarking algorithms based on DCT have used mid-frequency coefficients for achieved robustness. In this paper, all DCT coefficients of host image are used for achieved fragility because the low frequency and high frequency coefficients are mainly affected by watermarking attacks.

2.2.2. Discrete curvelet transform (DCuT)

The discrete curvelet transform (Candes et al., 2005) decomposes the image into various frequency cells such as low frequency cell and high frequency cell. This transform represents image into its sparse domain. There is two discrete transform are available such as frequency wrapping based and USFFT technique based. The frequency wrapping based discrete curvelet transform have less execution time and easy to implement compared to other curvelet transforms (Candes et al., 2005). The frequency wrapping based discrete curvelet transform is also known as fast discrete curvelet transform (FDCuT). For example, an image with a size of 256×256 pixels are decomposed using 5 scales and 16 angles shown in Fig. 3 (a). The low frequency coefficients are shown in the middle of the image. The Cartesian concentric coronas show the high frequency coefficients at different scales. The last coronae have high frequency coefficients which are equal to the size of the image. The high frequency curvelet coefficients of the image are shown in Fig. 3 (b).

In this paper, curvelet transform is applied to DCT coefficients of host image to get hybrid coefficients of the host image. Then high frequency curvelet transform is chosen for sparse data embedding because of these coefficients are affected by watermarking attacks. The size of these coefficients is equal to the size of the watermark image which is used for achieved 100% payload capacity. The high frequency curvelet coefficients of DCT coefficients of the image are shown in Fig. 4. It is cleared sees that these coefficients have no any visual information of host medium. So the visual information of host medium is not corrupted due to this approach.

2.2.3. Discrete wavelet transform (DWT) & singular value decomposition (SVD)

The discrete wavelet transform (DWT) decomposes the image into various frequency coefficients subbands. These coefficients are different than DCT coefficients. Nowadays, this transform is playing important roles in image processing applications such as image compression, compressive sensing, and watermarking. The DWT decomposed image in various frequency subbands such as approximation, horizontal, vertical and diagonal. The visual information of the image is laid on approximation wavelet subbands. These subbands have low frequency coefficients. Whereas other three subbands such as horizontal, vertical and diagonal have high frequency coefficients. These all wavelet subbands give sparsity property. When wavelet basis matrix with its inverse version is applied on the image then the image is converted into its wavelet coefficients are shown in Fig. 5.

The singular value decomposition is a linear algebra tool which decomposes the image into three different matrices such as singular value matrix, two orthogonal matrices. The singular value

(a) Without Block Wise Process (b) With Block Wise Process

Fig. 2. DCT Coefficients of Image.

(a) All Curvelet Coefficients (b) High Frequency Curvelet Coefficients

Fig. 3. Curvelet Coefficients of Image.

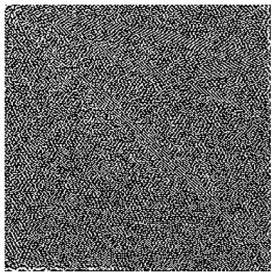

Fig. 4. High Frequency Curvelet Coefficients of DCT Coefficients of Image.

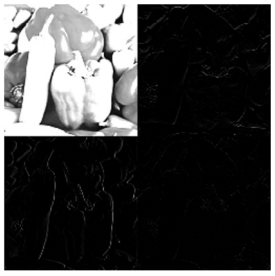

Fig. 5. Wavelet Coefficients of Image.

matrix has non-negative values and diagonally placed in the matrix. The singular value has sparsity and stable property which is suitable for sparse coefficients generation in CS. So singular value of image used for generation of sparse coefficients. When SVD is applied on the image is shown in Fig. 6.

In this paper, wavelet matrix is generated using wavelet matrix generation (Yan, 2009; Vidakovic, 1999) with equal size of watermark image. The various orthogonal wavelets such as Haar, bior6.8, and symlet are used for wavelet matrix generation. Then wavelet matrix with its inverse version is multiplied with watermark image to get sparse wavelet coefficients of watermark image which is shown in Fig. 7 (a). The SVD is applied on sparse wavelet coefficients of watermark image to the Singular matrix, U, V orthogonal matrices. The singular matrix values are used as sparse coefficients of watermark image for generation of CS measurements using compressive sensing theory which is shown in Fig. 7 (b). The reason behind chosen singular matrix is sparser than other two matrices which are shown in Fig. 6.

3. Proposed scheme

Today's world, data transferred from one place to other place using high speed of the internet. Therefore, watermarking techniques with having high computational time are not used for data protection. The many existed techniques have provided security to data using embedding factor or single security parameter. The data size of multimedia is also increasing day by day. Also, less watermarking techniques are available for multimedia data authentication. The CS theory based watermarking technique is mainly used for image tamper identification using standard logo or image. This technique is embedded CS measurements of the watermark in host image by the size of CS measurements is few bits or less than the size of the host image. The most of the existed hybrid watermarking techniques have less payload capacity for large watermark data embedding. Thus, the new watermarking scheme should have fast computational time, more payload capacity and authenticity.

So, in the proposed scheme, CS theory is used for increased fragility and providing the data authentication. The CS theory is used in proposed scheme for providing security to watermark multimedia data before embedding without any optimization techniques with increase execution time. In the proposed scheme, the curvelet transform is applied to DCT coefficients of host image to get hybrid coefficients of the host image. Then high frequency curvelet transform is chosen for sparse data embedding because of these coefficients are affected by watermarking attacks. The size of these

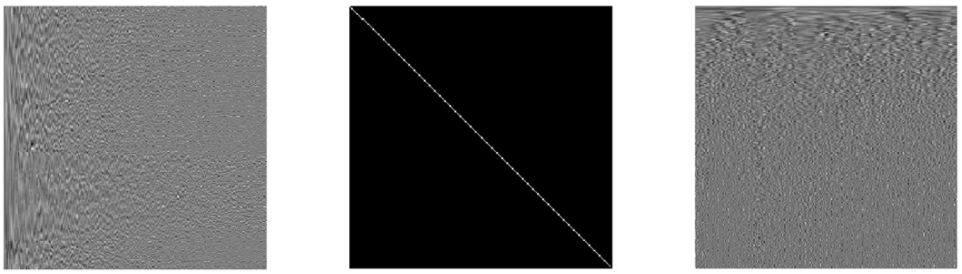

Fig. 6. SVD Matrices of Image: U Matrix (left), S Matrix (middle), V Matrix (right).

(a) **(b)**

Fig. 7. (a) Sparse Wavelet Coefficients of Watermark Image (b) Singular Matrix value of Wavelet Coefficients of Watermark Image.

coefficients is equal to the size of the sparse data of watermark image which is used for achieved 100% payload capacity.

For extraction of the watermark from watermarked data from watermarked image, there are various security keys are required. These security keys such as embedding factor, sampling factor, the measurement matrix, wavelet basis matrix and orthogonal matrices U, V are required in proposed extraction process. These security keys are provided security to multimedia data in various stages in proposed scheme. The required of these keys are make proposed scheme little be complicated but provide excellent security to multimedia data. Because imposter is required five keys to extract watermark data which very difficult to get compared to one or two keys. But the security of security keys is very important at storage of computer, server or cloud.

For the security of these keys can be provided using various data encryption algorithms such as Digital Encryption Standard (DES), Riverst Shamir Adleman (RSA), etc. These all keys are numeric values which are represented in bytes. The overall size of all keys is few kB which can be storage in any computer system, server or cloud. This is very small amount data consideration of modern times of computer and server which have very high storage capacity for data storage.

The block of diagram of proposed scheme is shown in Fig. 8. In this section, the watermark embedding procedure and watermark extraction procedure of proposed scheme are described.

3.1. Watermark embedding procedure

The watermark image w is transformed into the sparse domain using orthogonal transform basis matrixΨ. The CS measurements y of watermark biometric image is generated using compressive sensing (CS) with measurement matrix. The CS measurements y of watermark image is embedded into the high frequency curvelet coefficients of DCT coefficients of the host image, which is used to provide a different level of security. Fig. 9 shows the block diagram for the proposed embedding procedure and the mathematical steps for watermark embedding are given below.

- Apply wavelet basis matrix with its inverse version is multiplied with the watermark image w to get the wavelet coefficients.

$$x = \Psi \times w \times \Psi^{*} \tag{4}$$

In above equation, x is wavelet coefficients of the watermark image, Ψ is the wavelet basis matrix and Ψ^{*} is the wavelet basis matrix.

- Apply the singular value decomposition on wavelet coefficients of the watermark image to get the singular matrix, two orthogonal matrices. The singular matrix value of wavelet coefficients is chosen as sparse coefficients.

$$[U, S, V] = svd(x) \tag{5}$$

In above equation, S is the singular value of wavelet coefficients of watermark image.

- Apply measurement matrix A (which is Gaussian in nature) on the singular value of wavelet coefficients of watermark image which is giving the CS measurements y.

$$y = A \times x \tag{6}$$

In above equation, y is the CS measurements, A is the measurement matrix.

- Apply downsampling procedure with sampling factor on CS measurements of watermark image which is giving the sparse data of watermark image wSparse.

$$W_{Sparse} = \beta \times y \tag{7}$$

In above equation, β is the sampling factor; W_{Sparse} is sparse data of watermark image.

- Apply discrete cosine transform (DCT) on the host image H, to get the DCT coefficients. Apply frequency wrapping based fast discrete curvelet transform on DCT coefficients to get its curvelet coefficients values C. Then high frequency curvelet coefficients are chosen for watermark embedding.

$$D = dct(H) \tag{8}$$

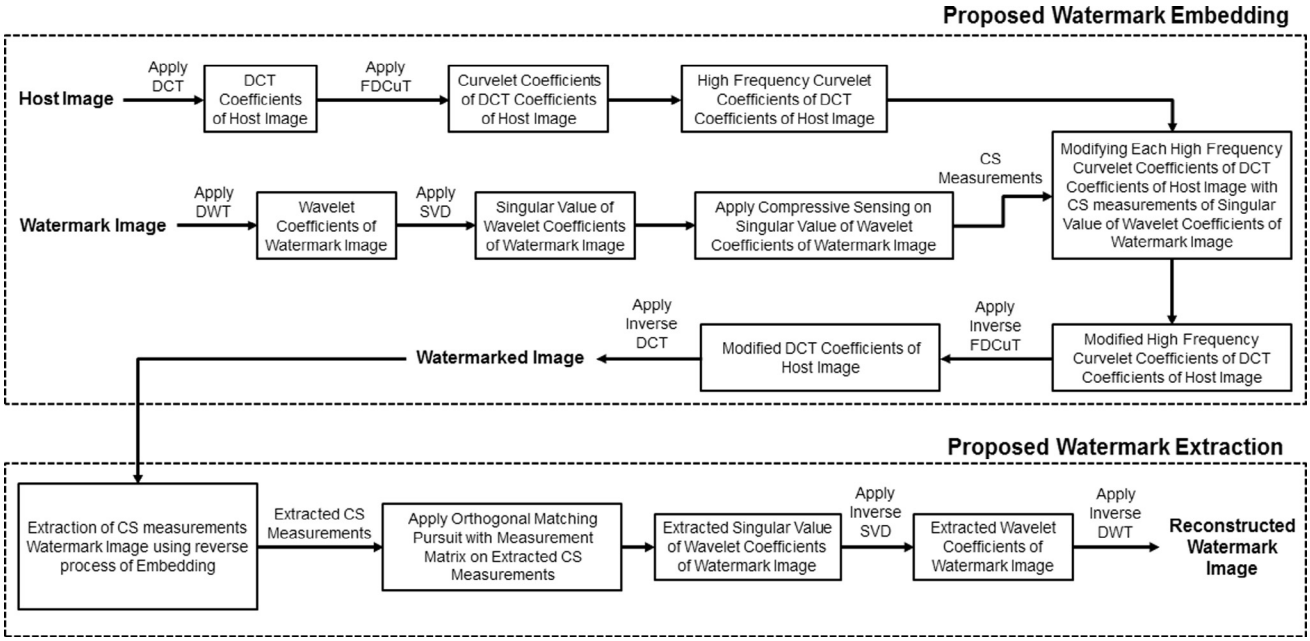

Fig. 8. Block Diagram of Proposed Scheme.

$$C = FDCuT(D) \tag{9}$$

In above equation, D is DCT coefficients of the host image; C is curvelet coefficients of DCT coefficients of the host image.

- The high frequency curvelet coefficients of host image are modified with sparse data of watermark image to embed the watermark data into the host image.

$$C^*_{High\_Frequency\_Ceofficients} = C_{High\_Frequency\_Coefficients} * (1 + k \times W_{Sparse}) \tag{10}$$

In above equation, $C*$ is modified curvelet coefficients of DCT coefficients of the host image, k is embedding factor.

- Apply inverse frequency wrapping based fast discrete curvelet transform to get the modified DCT coefficients of the host image.
- Apply inverse discrete cosine transform (IDCT) on modified DCT coefficients to get the watermarked image, $H*$.

3.2. Watermark extraction procedure

For extraction of the watermark from watermarked image, embedding factor, sampling factor, the measurement matrix, wavelet basis matrix, and orthogonal matrices U, V are required. The OMP algorithm is used to the extraction of singular value of wavelet coefficients from the CS measurements values. Fig. 10 shows the block diagram for the proposed extraction procedure and the mathematical steps for watermark extraction are given below.

- Apply discrete cosine transform (DCT) on the Watermarked image $H*$, to get the modified DCT coefficients. Apply frequency wrapping based fast discrete curvelet transform on DCT coefficients to get its modified curvelet coefficients values $C*$. Then get modified high frequency curvelet coefficients which are used for watermark embedding.
- Extract sparse data of watermark image using modified high frequency curvelet coefficients and embedding factor (security key 1) as

$$W_{Extracted} = \left\{ \frac{C^*_{High\_Frequency\_Coefficients}}{C_{High\_Frequency\_Coefficients}} - 1 \right\} \Big/ k \tag{11}$$

In above equation, $W_{Extracted}$ is sparse data of watermark image.

- Apply upsampling procedure with sampling factor (security key 2) on sparse data to get CS measurements of watermark image.

$$y_{Extracted} = \frac{W_{Extracted}}{\beta} \tag{12}$$

In above equation, $y_{Extracted}$ is CS measurements of watermark image.

- The measurement matrix A which is used as security key 3 and recovered the singular value of watermark image with the help of OMP algorithm.

$$S^*_w = OMP(y_{Extracted}, A) \tag{13}$$

- Further apply inverse SVD on the singular value of watermark image with original orthogonal matrices U, V which is used as security key 4 to get wavelet coefficients x of watermark image.

$$x^*_{Extracted} = U_w S^*_w V'_w \tag{14}$$

In above equation, $x*_{Extracted}$ is extracted sparse coefficients of the watermark image.

- Finally, apply inverse wavelet basis matrix (security key 5) with its original version is multiplied with the extracted wavelet coefficients to get reconstructed watermark image $w*$.

$$w^* = \Psi^* \times x^*_{Extracted} \times \Psi \tag{15}$$

After extracting watermark image, watermark data authentication performed. For host multimedia data authentication, below two hypotheses is formed.

H_0: A host multimedia data is authenticated i.e.$SSIM(\omega, \omega^*) > \tau$

H_1: A host multimedia data is unauthenticated i.e.$SSIM(\omega, \omega^*) > \tau$

In above equation τ is a predefined threshold, SSIM is Structural Similarity Index Measures (Wang and Bovik, 2004) which is found similarity between watermark data.

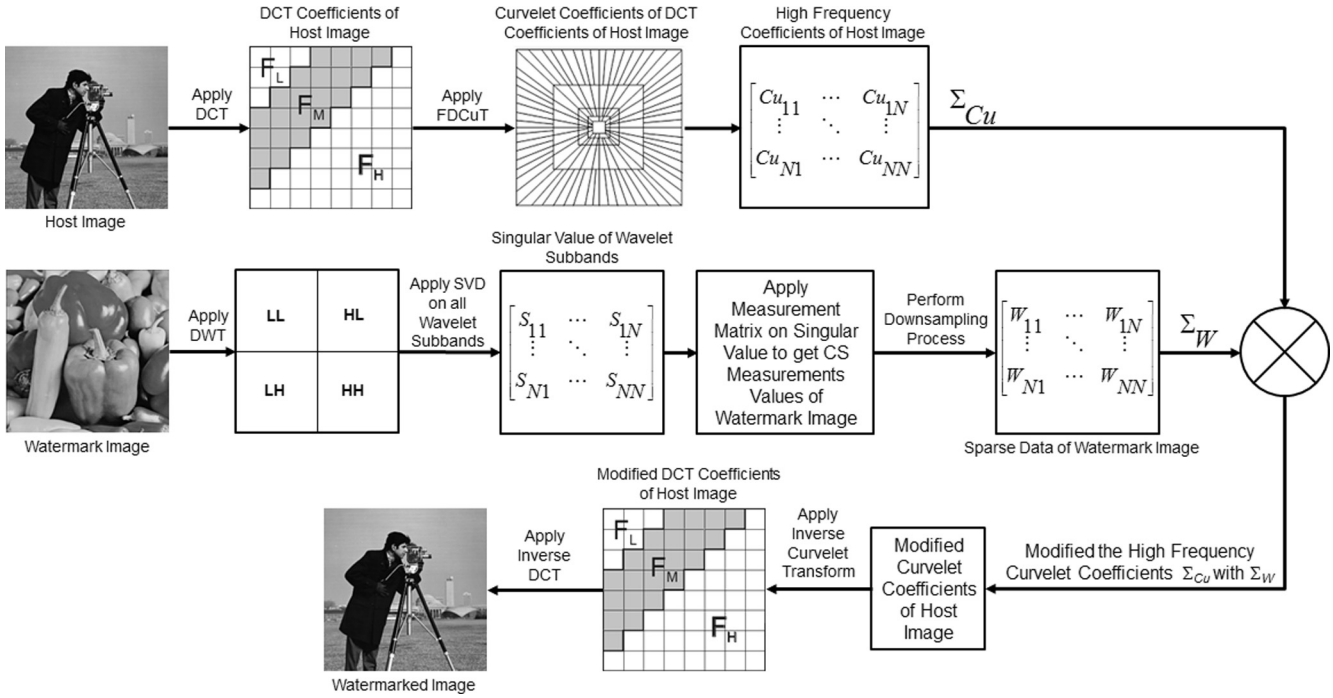

Fig. 9. Block Diagram of Proposed Watermark Embedding Procedure.

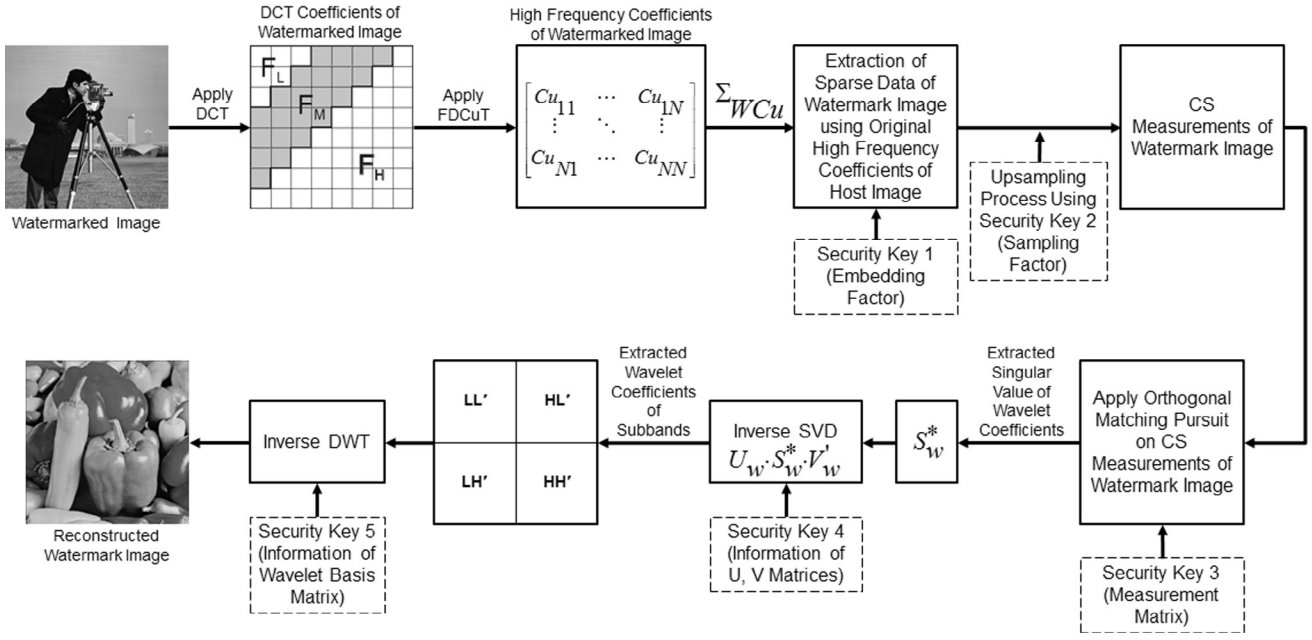

Fig. 10. Block Diagram of Proposed Watermark Extraction Procedure.

3.3. Watermarking attacks

The watermarking attacks are used for checking performance and comparison of different watermarking techniques. Therefore, in this paper, standard watermarking attacks (Voloshynovskiy et al., 2001) are used. These attacks are divided into various types such as removal attacks, geometric attacks, cryptographic attacks and protocol attacks. The watermarking attacks such as noise addition filter attack, compression, and geometric attacks are applied on watermarked image. In this paper, corrupted or modified watermarked data by attacks is checked for ownership authentication by the user using various security keys. If watermarked data is successful authenticate if watermarked data is not corrupted or modified by watermarking attacks.

4. Results and discussion

The testing of proposed scheme using various multimedia data such as different images and video with quality measures are discussed in this section. The various test images and video are discussed in Section 4.1. The quality measures such as PSNR; SSIM

for proposed scheme is discussed in Section 4.2. The effect of watermarking attacks on the authenticity of proposed scheme is discussed in Section 4.3. The effect of various wavelet packets on perceptual quality and performance of proposed scheme is discussed in Section 4.4. The performance analysis of proposed scheme for video is discussed in Section 4.5. The comparison of proposed scheme with existed schemes is discussed in Section 4.6.

4.1. Test images and video

The performance of any watermarking scheme varies with different types of images. Therefore, in this paper, two different types of host images such as cameraman image which has low frequency coefficients and lady image which has high frequency coefficients are used. In Fig. 11, cameraman host image and lady host image have a size of 256×256 pixels. The watermark peppers image and watermark mandrill image has a size of 256×256 pixels. The watermark peppers image with different host images shows the performance of proposed scheme. The performance of proposed scheme is carried out for different embedding factor. The analysis of proposed scheme is carried out for various watermarking attacks such as JPEG compression with various quality factor; noise addition such as Gaussian noise, Salt and Pepper noise and speckle noise; filter attacks such as Mean, median, sharpen and Gaussian low pass filter; geometric attacks such as histogram equalization, rotation and cropping.

This proposed scheme is also implemented and analyzed for digital video. In Fig. 12, news reader video which has low frequency coefficients is taken as host video. This video contains 15 frames with a size of 256×256 pixels. The performance analysis of proposed scheme for digital video is discussed in Section 4.5.

4.2. Quality measures

The perceptual quality of watermarked image is measured by Peak Signal to Noise Ratio (PSNR) (Langelaar et al., 2000) and the mathematical equation of PSNR is given in below

$$PSNR = 10\log_{10}\frac{255^2}{MSE} \tag{16}$$

In above equation, MSE is defined as mean square error and given by

$$MSE = \frac{1}{M \times N}\sum_{x=1}^{M}\sum_{y=1}^{N}\{I(x,y) - I^*(x,y)\}^2 \tag{17}$$

In above equation, I and I^* is original host image and watermarked image respectively.

The MSE is measured in general scale while PSNR is measured in logarithmic scale. The high value of PSNR is indicated more imperceptibility of watermarking scheme. The structural similarity index measures (SSIM) are used to measure the similarity between original watermark image and reconstructed watermark image. The mathematic equation for SSIM is given in below

$$SSIM(w, w^*) = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N} w(x,y) \times w^*(x,y)}{\sqrt{\sum_{x=1}^{M}\sum_{y=1}^{N} w^2(x,y)} \times \sqrt{\sum_{x=1}^{M}\sum_{y=1}^{N} w^{*2}(x,y)}} \tag{18}$$

In above equation, w is original watermark image and w^* is reconstructed watermark image.

The SSIM value lies in 0 to 1. When SSIM value is 1 then it is indicated the reconstructed watermark image is exactly similar to the original watermark image. But SSIM value is 0 then it is indicated that the reconstructed watermark image is not similar to the original watermark image.

4.3. Authenticity of proposed scheme under various watermarking attacks

In the proposed scheme, CS measurements are generated using the singular value of wavelet coefficients of watermark image. In this proposed scheme, the wavelet coefficients of watermark image are generated using different wavelet packets. These CS measurements are embedded into high frequency curvelet coefficients of DCT coefficients of the host image. Fig. 13 shows the watermarked

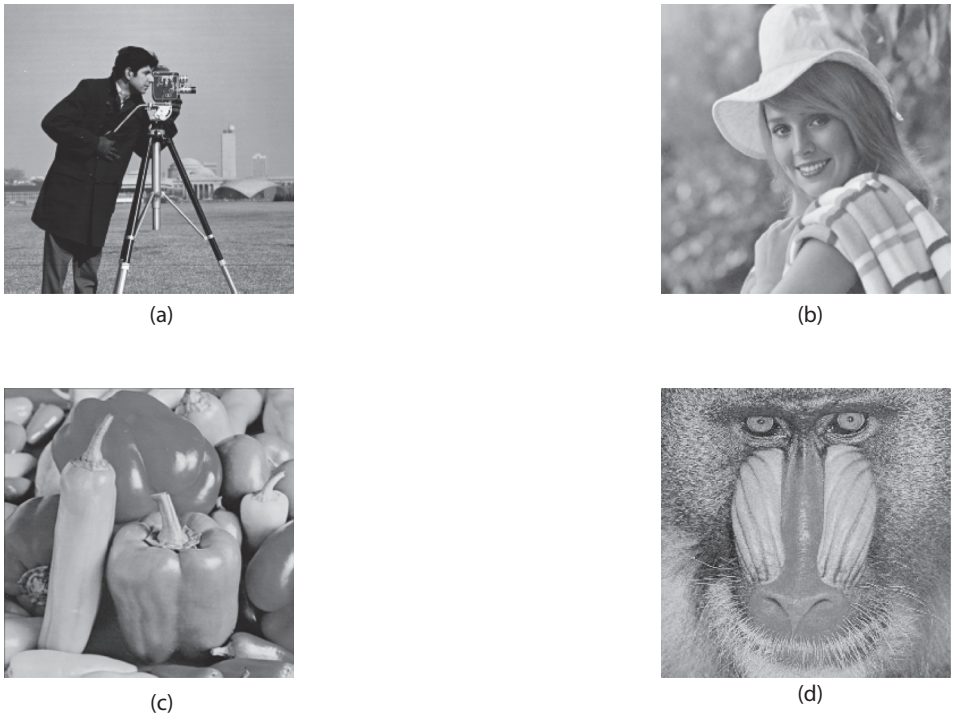

Fig. 11. Host Images (a) cameraman, (b) lady and Watermark Image (c) peppers (d) mandrill.

Fig. 12. Test Video, News Reader Video which has low frequency coefficients.

(a) Watermarked Cameraman Host Image (b) Reconstructed Peppers Watermark Image

(a) Watermarked Lady Host Image (b) Reconstructed Peppers Watermark Image

Figure 13. Results of Proposed Scheme without Watermarking Attack

Fig. 13. Results of Proposed Scheme without Watermarking Attack.

image and reconstructed watermark image without application of watermarking attacks on watermarked image using embedding factor 0.02 and Sym8 wavelet.

The PSNR values and SSIM values for proposed scheme without watermarking attacks is 47.19 dB, 40.51 dB and 1.00, 1.00 for cameraman host image and lady host image respectively. The sampling factor value β is set 0.0001 for generated all watermarked image with attacks and without attacks. For authentication decision of host multimedia data, the predefined threshold τ value is set 0.90. The value of sampling factor β and predefined threshold τ can be decided by the user as per his or her requirements.

To check the fragility of proposed watermarking scheme and authentication of host multimedia data, various watermarking attacks are applied on watermarked image. The various water-

marking attacks such as JPEG compression with different quality factor, Gaussian noise, speckle noise, salt & pepper noise, mean filter with different filter mask, median filter with different filter masks, Gaussian low pass filter with different filter masks, sharpening attack, histogram equalization and geometric attach such as rotation attack, cropping attack is applied on watermarked image. The JPEG compression is mainly used when data is transmission over a medium. This technique is used in various applications such as data compression, video compression, and telemedicine. The JPEG compression standard is applied on the image when it is transferred to medium. When JPEG compression is applied to the image then it removes high frequency coefficients of the image. So in this paper, JPEG compression with different quality factor is applied on watermarked image and tries to the reconstruction of watermark image after application of JPEG compression. Table 1 shows the performance of proposed scheme under JPEG compression attack with different quality factors. Table 2 shows the performance of proposed scheme under noise addition attacks such as Gaussian noise, salt & pepper noise, and speckle noise.

Table 3 to 5 shows the performance of proposed scheme under various filters attack such as median filter, mean and Gaussian low pass filter with a different size of filter masks. Table 6 shows the performance of proposed scheme under various attacks such as sharpening, histogram equalization, geometrical attacks like rotation and cropping.

The analysis of proposed scheme under various watermarking attacks for different embedding factors for cameraman host image and lady host image is shown in Table 2 and 6. The results show that SSIM values for reconstructed watermark image are near to zero under all watermarking attack. The SSIM values are less than a predefined threshold τ value 0.90 when watermarking attacks is applied on watermarked image. When any attack or manipulation is applied on watermarked image than the extraction of watermark image is not possible based on mentioned SSIM values in Table 1 to 6. This is indicated that this proposed scheme has fragile in nature.

Table 1
The performance of proposed scheme for digital video with various watermarking attacks in term of SSIM values for reconstructed watermark.

Embedding factor	JPEG Compression Attack				Decision about Host Image Authentication
	Q = 20	Q = 40	Q = 60	Q = 80	
Cameraman Host Image					
0.02	0.00004	0.00003	0.00001	0.00002	Unauthenticated
0.03	0.00021	0.00004	0.00006	0.00001	Unauthenticated
0.04	0.00010	0.00036	0.00019	0.00004	Unauthenticated
0.05	0.00025	0.00004	0.00055	0.00014	Unauthenticated
Lady Host Image					
0.02	0.00093	0.00070	0.00001	0.00013	Unauthenticated
0.03	0.00071	0.00055	0.00076	0.00410	Unauthenticated
0.04	0.00490	0.00044	0.00046	0.00220	Unauthenticated
0.05	0.00067	0.00063	0.00085	0.00300	Unauthenticated

Table 2
Comparison of Proposed Scheme with Existed Schemes.

Embedding factor	Noise Addition Attack			Decision about Host Image Authentication
	Gaussian Noise (Variance = 0.001)	Salt & Pepper Noise (Variance = 0.005)	Speckle Noise (Variance = 0.004)	
Cameraman Host Image				
0.02	0.00009	0.00008	0.00035	Unauthenticated
0.03	0.00002	0.00004	0.00014	Unauthenticated
0.04	0.00010	0.00004	0.00009	Unauthenticated
0.05	0.00041	0.00007	0.00006	Unauthenticated
Lady Host Image				
0.02	0.00043	0.00014	0.00049	Unauthenticated
0.03	0.00012	0.00039	0.00001	Unauthenticated
0.04	0.00110	0.00021	0.00005	Unauthenticated
0.05	0.00210	0.00010	0.00030	Unauthenticated

Table 3
The performance of proposed scheme for different embedding factor with JPEG compression attack in term of SSIM values for reconstructed watermark.

Embedding factor	Median Filter Attack			Decision about Host Image Authentication
	Mask Size = 3×3	Mask Size = 5×5	Mask Size = 7×7	
Cameraman Host Image				
0.02	0.00004	0.00083	0.00006	Unauthenticated
0.03	0.00051	0.00040	0.00010	Unauthenticated
0.04	0.00000	0.00042	0.00011	Unauthenticated
0.05	0.00027	0.00006	0.00005	Unauthenticated
Lady Host Image				
0.02	0.00025	0.00055	0.00034	Unauthenticated
0.03	0.00027	0.00012	0.00022	Unauthenticated
0.04	0.00023	0.00032	0.00072	Unauthenticated
0.05	0.00008	0.00021	0.00024	Unauthenticated

Table 4
The performance of proposed scheme for different embedding factor with noise addition attack in term of SSIM values for reconstructed watermark.

Embedding factor	Mean Filter Attack			Decision about Host Image Authentication
	Mask Size = 3×3	Mask Size = 5×5	Mask Size = 7×7	
Cameraman Host Image				
0.02	0.00034	0.00069	0.00016	Unauthenticated
0.03	0.00380	0.00015	0.00280	Unauthenticated
0.04	0.00009	0.00001	0.00018	Unauthenticated
0.05	0.00630	0.00013	0.00110	Unauthenticated
Lady Host Image				
0.02	0.00005	0.00130	0.00045	Unauthenticated
0.03	0.00190	0.00012	0.00100	Unauthenticated
0.04	0.01420	0.00720	0.00030	Unauthenticated
0.05	0.00033	0.00130	0.00000	Unauthenticated

Table 5
The performance of proposed scheme for different embedding factor with median filter attack with different filter masks in term of SSIM values for reconstructed watermark.

Embedding factor	Gaussian Low Pass Filter Attack			Decision about Host Image Authentication
	Mask Size = 3×3	Mask Size = 5×5	Mask Size = 7×7	
Cameraman Host Image				
0.02	0.00034	0.00002	0.00003	Unauthenticated
0.03	0.00006	0.00028	0.00071	Unauthenticated
0.04	0.00001	0.00003	0.00001	Unauthenticated
0.05	0.00200	0.00041	0.00005	Unauthenticated
Lady Host Image				
0.02	0.00025	0.00005	0.00044	Unauthenticated
0.03	0.00049	0.02880	0.00058	Unauthenticated
0.04	0.00120	0.00730	0.00035	Unauthenticated
0.05	0.00280	0.01170	0.00120	Unauthenticated

Table 6
The performance of proposed scheme for different embedding factor with mean filter attack with different filter masks in term of SSIM values for reconstructed watermark.

Embedding factor	Sharpening	Histogram Equalization	Rotation (90°)	Cropping (10%)	Decision about Host Image Authentication
Cameraman Host Image					
0.02	0.00009	0.00024	0.00012	0.00006	Unauthenticated
0.03	0.00055	0.00012	0.00004	0.00076	Unauthenticated
0.04	0.00004	0.00009	0.00005	0.00005	Unauthenticated
0.05	0.00037	0.00016	0.00007	0.00089	Unauthenticated
Lady Host Image					
0.02	0.00330	0.00000	0.00400	0.00160	Unauthenticated
0.03	0.00002	0.00014	0.00062	0.00089	Unauthenticated
0.04	0.00020	0.00025	0.00290	0.00013	Unauthenticated
0.05	0.00016	0.00025	0.00160	0.00006	Unauthenticated

This proposed scheme can be used for copyright ownership or authentication for any digital image.

4.4. Perceptual quality and performance of proposed scheme for various wavelet packets

In this proposed scheme, the wavelet transform is used for generation of sparse coefficients of watermark image. The sparse coefficients of watermark image are generated using various wavelet packets such as symmetric wavelet, asymmetric wavelet, orthogonal wavelet and bi-orthogonal wavelet. The three wavelet such as Haar, Bior 6.8 and Sym8 are used for generation of sparse coefficients of watermark image in this proposed scheme. The Haar wavelet is basic wavelet, simplest, asymmetric and orthogonal as well as bi-orthogonal in nature. The Bior6.8 wavelet is bi-orthogonal in nature and symmetric wavelet. The Sym8 wavelet is new wavelet, near symmetric and orthogonal as well as bi-orthogonal in nature. The quality of watermarked image for above three wavelet packets are given in Table 7 without application of any watermarking attacks. The PSNR values are obtained for both host images. The results show that the value of PSNR is more than 30 dB which is accepted by HVS property of watermarking scheme. The analysis shows that this proposed scheme can be work equally for all types of wavelet packets.

Table 7
The performance of proposed scheme for different embedding factor with Gaussian low pass filter attack with different filter masks in term of SSIM values for reconstructed watermark.

Embedding factor	Various Wavelet Packets		
	Haar	Bior6.8	Sym8
Cameraman Host Image			
0.02	49.42	44.12	47.19
0.03	44.37	41.88	42.78
0.04	38.36	37.92	35.03
0.05	35.99	32.98	32.14
Lady Host Image			
0.02	38.73	38.48	40.51
0.03	36.44	35.31	36.68
0.04	33.49	33.10	35.74
0.05	30.27	31.25	31.85

4.5. Performance analysis of proposed scheme for video

The performance analysis of proposed scheme for digital video is discussed in this section. For the implementation of proposed scheme for video, the first digital video is broken out into various frames. Then watermark image is embedding into individual video frames using proposed watermark embedding procedure to generated individual watermarked frames. Then these watermarked frames are combined to get watermarked video. The results of proposed for digital video shows in Figs. 14 and 15.

The watermarked video frames are generated using embedding factor 0.02 and sampling factor 0.0001. The Sym8 wavelet is used for generation of wavelet coefficients of watermark image. The results show the perceptual quality of watermarked video frames is greater than 30 dB with SSIM value of 0.998 for extracted watermark image without application of watermarking attacks. For performance analysis of proposed scheme for video, take one watermarked video frame in which watermark image is embedded. Then various watermarking attacks is applied on this watermarked video frame and try to get watermark image from corrupted or modified watermarked video frame. The SSIM values for reconstructed watermark image when watermarked video frame is corrupted by the attack are summarized in Table 8.

The analysis of proposed scheme under various watermarking attacks for different embedding factors for a digital video frame is shown in Table 8. The results show that SSIM values for reconstructed watermark image are near to zero under all watermarking attack. The SSIM values are less than a predefined threshold τ value 0.90 when watermarking attacks is applied on watermarked video frame. When any attack or manipulation is applied on watermarked video than the extraction of watermark image is not possible based on mentioned SSIM values in Table 8. This is indicated that this proposed scheme can be used for copyright ownership or authentication for any digital video.

4.6. Comparison of proposed scheme with existed scheme

Nowadays, the execution time and payload capacity of the watermarking scheme are important parameters. The watermarking scheme is designed for various applications for multimedia data protection, big data protection when these data transferred over the high-speed internet. So in this paper, a fast watermarking scheme with high payload capacity and authenticity to multimedia is presented. The execution time of scheme is divided into watermark preparation time, watermark embedding time, watermark extraction time and watermark reconstruction time. The comparison of proposed scheme with existed schemes with various parameters is given in Table 9.

The proposed scheme can be used for authentication of any type of multimedia data such as image and video while Thakkar scheme is used for digital image protection, Kothari Scheme, Liu scheme and Nguyen scheme is used H.264 video standard based video protection. The proposed scheme is used applied compressive sensing on watermark image before embedding while existed schemes are embedded watermark image directly into host medium. The proposed scheme is used four image processing transforms while existed schemes are used one or two image processing transforms. The payload capacity of proposed scheme is almost 65 K bytes while payload capacity of existed schemes is up to 17 K bytes. The performance measures of proposed scheme are better than existed schemes available in the literature.

The execution time of any watermarking technique is an important parameter when data is transfer over the high-speed internet. So the execution time of proposed scheme is compared with execution time of existed schemes. The execution time for watermarked image generation and extraction of watermark image in Thakkar scheme and Nguyen scheme is around 5.42 s, 11.03 s respectively. The execution time for watermarked image generation and extraction of watermark image in proposed scheme is

Fig. 14. Watermarked Video Frames with PSNR values using Proposed Scheme without watermarking attacks.

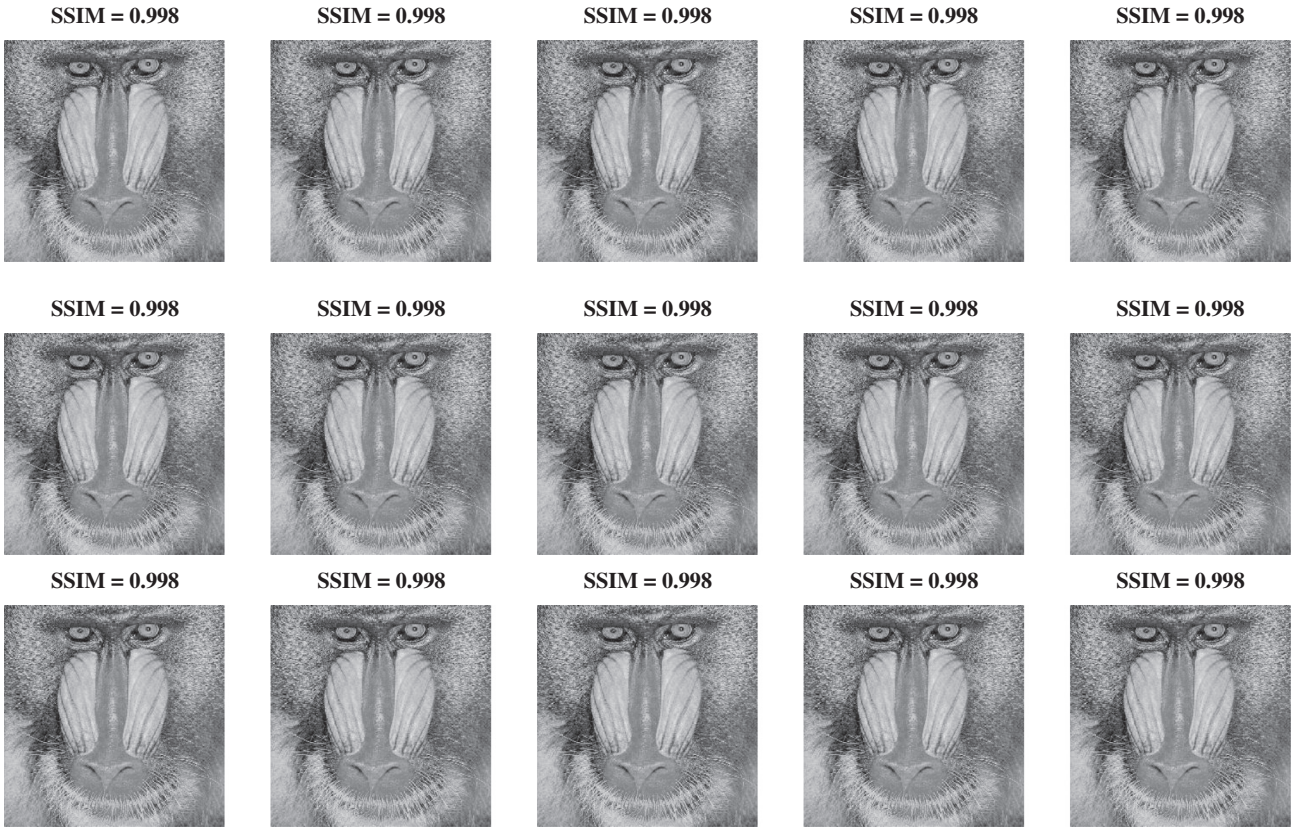

Fig. 15. Extracted Watermark Image for Watermarked Video Frames using Proposed Scheme.

Table 8
The performance of proposed scheme for different embedding factor with sharpening attack, histogram equalization attack, rotation attack, cropping in term of SSIM values for reconstructed watermark.

Watermarking Attacks	SSIM	Decision about Host Image Authentication
JPEG Compression Attack Q = 80	0.00004	Unauthenticated
JPEG Compression Attack Q = 60	0.00014	Unauthenticated
JPEG Compression Attack Q = 40	0.00020	Unauthenticated
JPEG Compression Attack Q = 20	0.00013	Unauthenticated
Gaussian Noise (Variance = 0.001)	0.00110	Unauthenticated
Salt & Pepper Noise (Variance = 0.005)	0.00008	Unauthenticated
Speckle Noise (Variance = 0.004)	0.00043	Unauthenticated
Median Filter (Filter Mask Size = 3 × 3)	0.00048	Unauthenticated
Median Filter (Filter Mask Size = 5 × 5)	0.00002	Unauthenticated
Median Filter (Filter Mask Size = 7 × 7)	0.00170	Unauthenticated
Mean Filter (Filter Mask Size = 3 × 3)	0.00036	Unauthenticated
Mean Filter (Filter Mask Size = 5 × 5)	0.00043	Unauthenticated
Mean Filter (Filter Mask Size = 7 × 7)	0.00003	Unauthenticated
Gaussian LPF (Filter Mask Size = 3 × 3)	0.00012	Unauthenticated
Gaussian LPF (Filter Mask Size = 5 × 5)	0.00016	Unauthenticated
Gaussian LPF (Filter Mask Size = 7 × 7)	0.00048	Unauthenticated
Sharpening	0.00015	Unauthenticated
Histogram Equalization	0.00015	Unauthenticated
Rotation (90°)	0.00170	Unauthenticated
Cropping (10%)	0.00074	Unauthenticated

around 3.84 s. This is indicated that this proposed scheme is performed faster than existed schemes available in the literature. This proposed scheme can be used for authentication of multimedia data over the high-speed internet.

5. Multimedia authentication over cloud – An application scenario of proposed scheme

In this paper, a fragile and imperceptible watermarking scheme is proposed which have a different layer of security. This scheme can be used in various applications for multimedia data authentication over the internet, mobile storage and cloud. The scheme provides security to multimedia data using different keys such as embedding factor, sampling factor, measurement matrix, information of U, V matrices and information of wavelet basis matrix. The one possible application scenario of proposed scheme is shown in Fig. 16. The application scenario shows security of multimedia data over cloud where data is a store.

Suppose the watermarked data is stored at cloud A where user 1 has all ownership rights for watermark data along with all key 1 to

Table 9
The PSNR values of proposed scheme for different embedding factor with different wavelet packets.

Schemes	Thakkar Scheme et al. (2016)	Kothari Scheme et al. (2015)	Liu Scheme et al. (2013)	Nguyen et al. (2006)	Proposed Scheme
Host Medium	Digital Image	Digital Video	H.264/AVC Standard based Digital Video	H.264 Video Standard based Digital Video	Digital Image and Video
Size of Payload	6 K bytes	17 K bytes	1739 bits	3 K bytes	65 K bytes
Used	Multimedia Protection	Multimedia Protection	Multimedia Protection	Multimedia Protection	Multimedia Authentication
Compressive Sensing is Used	Yes	No	No	No	Yes
PSNR (dB)	35.44	37.18	37.00	37.00	47.19
SSIM	0.98	0.92	Not mentioned	0.92	1.00
Execution Time (in sec)	5.42 seconds	Not mentioned	Not mentioned	11.03 seconds	3.84 seconds

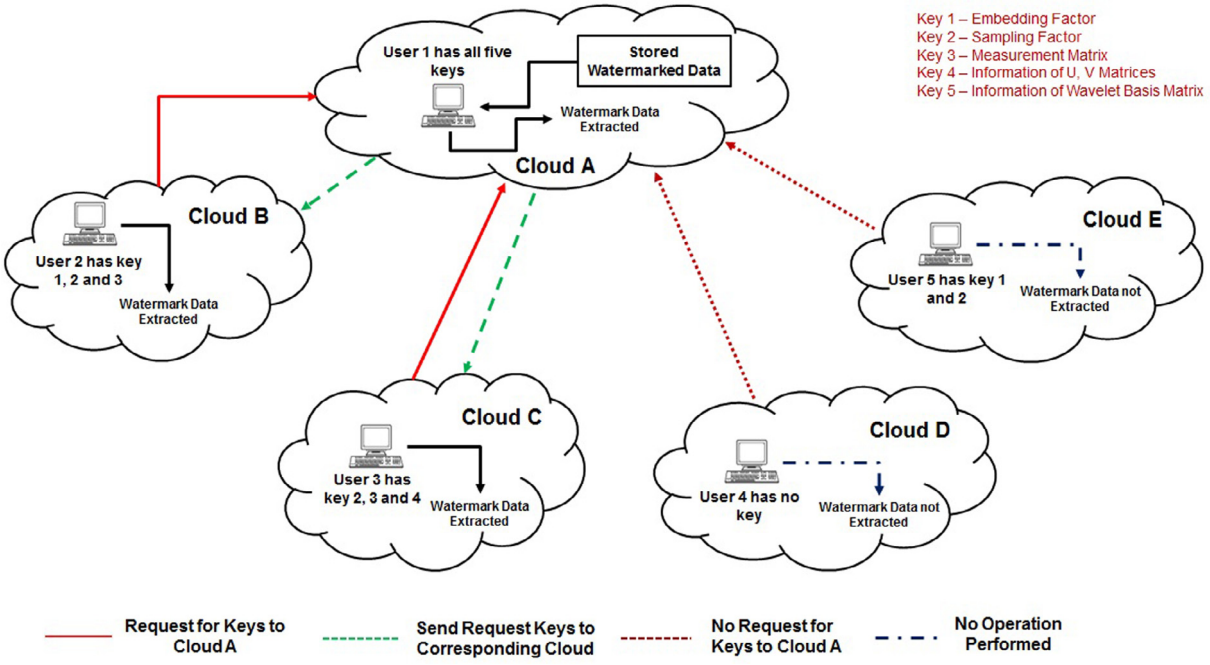

Fig. 16. Application Scenario of Proposed Scheme.

key 5. If user 1 is cloud A can be able to extract watermark data from watermarked data using all keys and prove that multimedia data secured and authenticate. But when users in cloud A get corrupted or manipulated watermarked data then user1 in cloud A can't get watermark data using all keys. This is indicated to user 1 in cloud A that watermarked data is corrupted or manipulated by an attacker.

This watermarked data is also shared copyright contents using the internet with another user 2 in cloud B, user 3 in cloud C and user 4 in cloud D and user 5 in cloud E with different security levels and keys. The User 2 in cloud B has key 1, key 2 and key 3. The user 3 in cloud C has key 2, key 3 and key 4. The user 4 in cloud D has no keys. The user 5 in cloud E has key 1 and key 2. So user 2 in cloud B can extract watermark data by sending a request for key 4 and key 5 to user 1 in cloud A. Similarly, user 3 in cloud C can extract watermark data by sending request for key 1 and key 5 to user 1 in cloud A. If user 2 and user 3 have corrupted watermarked data then user 2 can't watermark data using all keys. This is indicated user 2 in cloud B and user 3 in cloud C that watermarked data is corrupted by an attacker during transmission over the internet. The user 4 in cloud D tires to get watermark data without any sending request for keys to user 1 in cloud A about keys. Then user 4 can't get watermark data. Similarly, User 5 in cloud E can't get watermark data using key 1 and 2 without getting key 3, 4 and 5.

So above description indicated any user in any cloud can't get watermark data without requesting for keys to authorized user 1 in cloud A. So this proposed scheme provides a different level of security for data at cloud and data transmission between two clouds using the internet. This is situation indicated that this proposed scheme can be used for multimedia data authentication in the cloud. This proposed scheme also can be user for multimedia data protection when data transferred from one cloud to another cloud.

6. Conclusion

The applications such as multimedia authentication in the cloud, secure multimedia data transferred over the high-speed internet, the watermarking schemes with less payload capacity and high execution time are not suitable. Therefore, a hybrid watermarking scheme with combination of CS theory is proposed in this paper. This proposed scheme can be solved over mentioned issues by providing high payload capacity and have faster execution time. The execution time of proposed scheme for water-

marked data generation and extraction of watermark data is 3.84 s. This is indicated that this proposed scheme can be used for authentication of data at cloud and data transferred over the high-speed internet. The payload capacity of proposed scheme is around 65 k bytes which are more compared to the payload capacity up to 17 k bytes of existed schemes in the literature. This is indicated that proposed scheme also solves the payload capacity of existed schemes. After above discussion, it is clearly seen that the proposed scheme have high payload capacity, faster execution time and used for multimedia data authentication.

This scheme provides copyright ownership or authentication of multimedia data using various security keys. The various keys are provided by watermarking technique and CS theory. The authenticity of multimedia data is verified against various watermarking attacks such as compression, noise addition, filters attacks and geometric attacks with different embedding factor. The proposed scheme is also tested various host images and host video where one host image has low frequency coefficients and the second host image has high frequency coefficients. The host video has low frequency coefficients contents. The proposed scheme is also tested by various CS measurements of watermark image. The CS measurements of watermark image are generated using various wavelet packets such as Haar, Bior 6.8 and Sym8. The PSNR values for these wavelet packets shows that the scheme is performed better when CS measurements of watermark image are generated using Haar wavelet. The quality measures values of proposed scheme are also better than quality measures values of existed schemes in the literature.

Moreover, in future, the curvelet transform is used to get sparse coefficients of watermark image in proposed scheme instead of wavelet transform which may be improved the performance. Also, real time implementation of proposed scheme can be performed in the future.

References

Arena, S., Caramma, M., Lancini, R., 2000. Digital watermarking applied to MPEG-2 coded video sequences exploiting space and frequency masking. Proc. Int. Conf. Image Process. 2, 796–799.

Bangaleea, R., Rughooputh, H., 2002. Performance improvement of spread spectrum spatial domain watermarking scheme through diversity and attack characterization. 6th Africon Conference in Africa, 2002. IEEE AFRICON, pp. 293–298.

Bhatnagar, G., Raman, B., 2009. A new robust reference watermarking scheme based on DWT-SVD. Comput. Stand. Interfaces 31, 1002–1013.

Candes, E., Demanet, L., Donoho, D., 2005. Fast discrete curvelet transforms. Appl. Comput. Math., 1–44

Candes, E., 2006. Compressive sampling. In: Proceedings of the International Congress of Mathematicians, Madrid, Spain.

Chan, C., Cheng, L., 2004. Hiding data in images by simple LSB substitution. Pattern Recogn. 37, 469–474.

Cox, I., Kilian, J., Shamoon, T., Leighton, F., 1997. Secure spread spectrum watermarking for multimedia. IEEE Trans. Image Process. 6 (12), 1673–1687.

Dajun, H., Qibin, S., Tian, Q., 2003. A semi-fragile object based video authentication system. Proc. Int. Symp. Circuits Syst., 814–817

Dili, R., Mwangi, E., 2007. An image watermarking method based on the singular value transformation and the wavelet transformation. Proc. IEEE AFRICON, 1–5.

Donoho, D., 2006. Compressed sensing. IEEE Trans. Inf. Theory 52 (4), 1289–1306.

Ejima, M., Miyazaki, A., 2000. A Wavelet Based Watermarking for Digital Images and Videos. IEEE International Conference on Image Processing, pp. 678–681.

Elbasi, E., 2007. Robust MPEG video watermarking in wavelet domain. Trakya University J. Sci. 8 (2), 87–93.

Essaouabi, A., Ibnelhaj, E., 2009. A 3D wavelet based method for digital video watermarking. In: Proceedings of the 4th IEEE Intelligent Information Hiding and Multimedia Signal Processing.

Fakhr, M., 2012. Robust watermarking using compressed sensing framework with application to MP3 audio. Int. J. Multimedia Appl. (IJMA) 4 (6), 27–43.

Fan, L., Yanmei, F., 2006. A DWT based Video Watermarking Algorithm Applying DS-CAMA. In: IEEE Region 10 Conference TENCON 2006.

Ganic, E., Eskicioglu, A., 2004. Secure DWT-SVD domain image watermarking embedding data in all frequencies. ACM Multimedia Security Workshop 2004, 1–9.

Gupta, A., Raval, M., 2012. A robust and secure watermarking scheme based on singular value replacement. Sadhana 37 (4), 425–440.

Hernandez, J., Amado, M., Perez-Gonzalez, F., 2000. DCT domain watermarking techniques for still image: detector performance analysis and a new structure. IEEE Trans. Image Process. 9, 55–68.

Huang, F., Guan, Z., 2004. A hybrid SVD-DCT watermarking method based on LPSNR. Pattern Recogn. Lett. 25, 1769–1775.

Kothari, A., 2013. Design, Implementation and Performance Analysis of Digital Watermarking for Video Ph.D. Thesis. JJT University, India.

Kamlakar, M., Gosavi, C., Patankar, A., 2012. Single channel watermarking for video using block based SVD. Int. J. Adv. Comput. Inf. Res. 1 (2).

Kothari, A., Dwivedi, V., 2015. Video watermarking – embedding binary watermark into the digital video using hybridization of three transforms. Int. J. Signal Image Process. Issues 2015 (1), 9–17.

Koz, A., Alatan, A., 2008. Oblivious spatio-temporal watermarking of digital video by exploiting the human visual system. IEEE Trans. Circuits Syst. Video Technol. 18 (3), 326–337.

Langelaar, G., Setyawan, I., Lagendijk, R., 2000. Watermarking of digital image and video data – A state of art review. IEEE Signal Process. Mag., 20–46

Lee, Y., Chen, L., 2000. High capacity image steganographic model. In: IEEE proceedings of Vision Image and Signal Processing, pp. 288–294.

Liu, X., Yu, J., Yue, Y., Wei, Y., 2014. Double encrypted digital image watermarking algorithm based on compressed sensing. J. Comput. Inf. Syst. 10 (12), 5113–5120.

Liu, Y., Li, Z., Ma, X., Liu, J., 2013. A robust data hiding algorithm for H.264/AVC video streams. J. Syst. Software 86, 2174–2183.

El-Gayyar, Mahmoud, 2006. Watermarking Techniques – Spatial Domain Digital Rights Seminar. Media Informatics. University of Bonn, Germany.

Mansouri, A., Mahmoudi Aznaveh, A., Azar, F., 2009. SVD based digital image watermarking using complex wavelet transform. Sadhana 34 (3), 393–406.

Mostafa, S., Tolba, A., Abdelkader, F., Elhindy, H., 2009. Video watermarking scheme based on principal component analysis and wavelet transform. IJCSNS Int. J. Comput. Sci. Network Security 9 (8), 45–52.

Nguyen, C., Tay, D., Deng, G., 2006. A Fast Watermarking System for H.264/AVC Video. In: Asia Specific IEEE Conference on Circuits and Systems, pp. 81–84.

Orovik, I., Stankovic, S., 2013. Combined compressive sampling and image watermarking. In: IEEE Symposium, ELMAR, 41–44.

Preda, R., Vizireanu, D., 2007. Blind Watermarking capacity analysis of MPEG2 coded video. In: Proceedings of Conference of Telecommunications in Modern Satellite, Cable and Broadcasting Services, Serbia, pp. 465–468.

Podilchuk, C., Delp, E., 2001. Digital watermarking: algorithms and applications. IEEE Signal Process. Mag. 18 (4), 33–46.

Raghavendra, K., Chetan, K., 2009. A blind and robust watermarking scheme with scrambled watermark for video authentication. In: Proceedings of IEEE International Conference on Internet Multimedia Services Architecture and Applications.

Rajab, L., Al-Khatib, T., Ai-Haj, A., 2008. Hybrid DWT-SVD video watermarking. In: Proceedings of International Conference on Innovations in Information Technology, pp. 588–592.

Ramalingam, M., 2011. Stego machine – video steganography using modified LSB algorithm. World Acad. Sci. Eng. Technol. 74, 502–505.

Raval, M., Joshi, M., Rege, P., Parulkar, S., 2011. Image tampering detection using compressive sensing based watermarking scheme. In: Proceedings of MVIP 2011.

Raval, M., Rege, P., 2003. Discrete wavelet transform based multiple watermarking scheme. Proc. Convergent Technol. Asia-Pacific Region 3, 935–938.

Santhi, V., Thangavelu, A., 2009. DWT SVD combined full band robust watermarking technique for color images in YUV color space. Int. J. Comput. Theory Eng. 1 (4), 424–429.

Serdean, C., Ambroze, M., Tomlinson, M., Wade G., 2002. Combating geometrical attacks in a DWT based blind video watermarking system. In: IEEE Region 8 International Symposium on Video/Image Processing and Multimedia Communications, Zadar, Croatia, 263–266.

Sheikh, M., Baraniuk, R., 2007. Blind error free detection of transform domain watermarks. In: IEEE International Conference on Image Processing, San Antonio, Texas, United States.

Sridevi, T., Krishnaveni, B., Vijayakumar, V., Ramadevi, Y., 2010. A Video Watermarking Algorithm for MPEG Videos. In: A2CWiC 2010 – Amrita ACM-W Celebration of Women in Computing.

Tagliasacchi, M., Valenzise, G., Tubaro, S., Cancelli, G., Barni, M., 2009. A compressive sensing based watermarking scheme for sparse image tampering identification. Proc. ICIP 2009, 1265–1268.

Thanki, R., Kothari, A., 2016. Digital watermarking – Technical art of hiding a message. Intell. Anal. Multimedia Inf., 426–460

Thakkar, F., Srivastava, V., 2016. A fast watermarking algorithm with enhanced security using compressive sensing and principle components and its performance analysis against a set of standard attacks. Multimedia Tools Appl. 75 (21), 1–29.

Tiesheng, F., Guiqiang, L., Chunyi, D., Danhua, W., 2013. A Digital image watermarking method based on the theory of compressed sensing. Int. J. Autom. Control Eng. 2 (2), 56–61.

Tropp, J., Gilbert, A., 2007. Signal recovery from random measurements via orthogonal matching pursuit. IEEE Trans. Inf. Theory 53 (12), 4655–4666.

Veena V., Jyothish Lal G., Vishnu S., Sachin S., Soman K., 2012. A robust watermarking method based on compressed sensing and Arnold scrambling. In: IEEE Conference on Machine Vision and Image processing, pp. 105–108.

Vidakovic, B., 1999. Statistical Modelling by Wavelets. Wiley, pp. 115-116.

Voloshynovskiy, S., Pereira, S., Thierry, Pun., 2001. Attacks on digital watermarks: classification, estimation based attacks and benchmarks. IEEE Commun. Mag., 118–126

Wang, Z., Bovik, A., 2004. A universal image quality index. J. IEEE Signal Process. Lett. 3, 84–88.

Yamac, M., Dikici, C., Sankur, B., 2013. Robust watermarking of compressive sensed measurements under impulsive and Gaussian attacks. In: IEEE Proceeding of 21st European Conference on Signal processing, 1–5.

Yan, J., 2009. Wavelet Matrix. Department of Electrical and Computer Engineering, University of Victoria, Victoria, BC, Canada.

Yang, Z., Yan, W., Xiang, Y., 2015. On the security of compressed sensing-based signal cryptosystem. IEEE Trans. Emerg. Topics Comput. 3 (3), 363–371.

Zang, Q., Sun, Y., Yan, Y., Liu, H., Shang, Q., 2013. Research on algorithm of image reversible watermarking based on compressed sensing. J. Inf. Comput. Sci. 10 (3), 701–709.

Zhang, X., Qian, Z., Ren, Y., Feng, G., 2011. Watermarking with flexible self-recovery quality based on compressive sensing and compositive reconstruction. IEEE Trans. Inf. Forensics Secur. 6 (4), 1123–1132.