# A Singular Value Decomposition Based Low-Computational Zero-Watermark Algorithm for Digital Right Management

**K.Premkumar, T.Manikandan, V.Sapthagirivasan,V.Nandalal**

***ABSTRACT--- Digital rights management (DRM) is a systematic approach used for protecting the exclusive rights in the digital mass media. It uses a set of technologies to control doubling and reproducing exclusive rights for the digital works and software. The digital watermarking is one of the powerful technologies that play a vital role in numeral rights management. In this paper, a low-computational zero watermark (ZW) algorithm has been projected. It depends on the singular value decomposition (SVD) and implemented on standard cameraman, Barbara, Lena and living room images without attack and with various attacks. The significant feature of this algorithm is that it does not fuse any watermarking in the given source image and hence the result of the zero-watermark algorithm is looking very similar to the source image. This zero-watermark property is obtained by using SVD approach in which the ZW sequence is computed in accordance with the equivalence of prior digits of major remarkable worth in every slab. The implementation consequences shows highest similarity measures of 0.8658 for cameraman image. Further, the computational cost of the algorithm is calculated as 4.442 msec of execution time for all the images under watermark embedder and watermark extractor phases. The PSNR values are calculated for the watermarked images for testing the robustness in the algorithm that is proposed, and the observations have shown the promising results against attack.***

***Keywords: - Computational cost, Digital rights management, Similarity measure Singular value decomposition, Watermark.***

## 1. INTRODUCTION

The digital rights management is playing a significant role in digital data security services. It allows owners such as publishers or authors to prevent their digital content (Ghatak, 2004). Similarly, the companies holding digital media files can prevent them from unknown users so that they can avoid unauthorized usage. Through digital rights management, all the users are educated about copyright and intellectual property; users can secure files and keep them private; companies can have better licensing agreements and authors retain ownership of their works. DRM allows authors, musicians, movie makers and artists and related professionals for preventing illegal usage of the contented. It helps the companies to have controlled admission for personal data. Since these technologies are restricted to admission towards complex information, authorized users can be allowed to share the data securely. Using DRM, digital work is ensured that digital work remains unaltered (Stamp, 2003).

Various technologies are being used in digital rights management among which digital watermarking is one of the primary techniques used for hiding the content. In multimedia content, numeral images make for most modules in the form of digital arts, descriptive illustrations. These paintings are in the digitized system and digital photographs. Due to the advancement of computing hardware, software, and communication networks, various unwanted threats have been created for copyright protection and content integrity. These threats lead to unauthorized copying of images, modifying the content of the images and so on. To solve these kinds of problems, digital watermarking (DW) services as a hypothetically vibrant instrument that enables satisfied defense (Saini, 2014). In a few cases, the concept of encryption could be maintained with privacy along with integrity for protecting the content and further, DW is used for protecting the decrypted content.

Digital watermarking gives reliable solutions for patent defense of program forms presented as interacted situations. Watermarking algorithms can protect rightful ownership and they can also satisfy the required strength along with attack misrepresentations for shared image operations such as clarifying, firmness, and many more which is given in (Liu *et al.*, 2002). Basic idea behind watermarking process is to embed a dummy image into the original source image irrespective of the quality of the visual. The end user receives the watermarked image also this could be published for public (Rawat, 2013). When *et al.* (2003) implemented the zero-watermark technology without modifying the data of the original image using high order cumulates and achieved good performance.

Yuan *et al.* (2008) summarized robustness of the existing watermarking algorithms and they were compared using theoretical analyses and experimental validations. Authors conclude that the attack against the watermarks can cause significant impact. A robust ZW algorithm remaindered projected by Ye, (2011), all these are grounded on SVD. In this procedure, image has beenseparated into non-overlapping blocks along with all blocks were processed with SVD. Finally, particular price matrix remains distorted using discrete cosine transform. Since it used two transforms, the computational cost became high.

**Revised Manuscript Received on August 14, 2019.**

**K.Premkumar,** Research Scholar, Anna University, Meenakshi College of Engineering,Chennai, T.N, India E-mail: prem.embedded@gmail.com

**Dr.T.Manikandan,** Professor, Department of ECE, Rajalakshmi Engineering College, Chennai, T.N, India E-mail: manikandan.t@rajalakshmi.edu.in

**Dr. V. Sapthagirivasan,** Professor, Department of BME, Rajalakshmi Engineering College, Chennai, T.N, India. E-mail sapthagiri.ece@gmail.com)

**Dr.V.Nandalal,** Associate Professor, Department of ECE, Sri Krishna College of Engineering &Technology, Coimbatore, T.N, India E-mail: nandalal@skcet.ac.in

Leng *et al.* (2012) projected robust image ZW algorithm. This depends on the discrete wavelet transform (DWT) along with principle component analysis (PCA). The original image in the present work is initially transformed to wavelet transform. The LL band is then partitioned into non overlapping image blocks. In this, individually image blocks are distorted into a vector. PCA was then achieved by a set of vectors. In conclusion, ZW sequence was created. This is done by refereeing the positive and negative divergence of the coefficient having a greatest complete value in individually analysed vector. In spite of robustness planned algorithm was very good; the computational cost was high since it involved two subcomponents DWT and PCA.

Jian Zhao (2016) developed durable healthy ZW scheme. This is done by retaining multi resolution and multi scale representation structures of nonsubsampled shearlet convert. This are for analysing way for assumed image. The algorithm that is proposed is tested against compression and noise addition attacks. They concluded watermarking arrangement performed improved than the zero-watermark algorithm with DWT.

In this research work, a low-computational ZW algorithm is proposed. It is created on SVD. This algorithm does not fuse any watermarking in the given source image and hence the result of the zero-watermark algorithm is looking very analogous to source image. The property of zero-watermark which is obtained by using the singular value decomposition approach in which the zero-watermark sequence is computed in accordance with the parity. This parity is of initial number of main remarkable worth in each block. The algorithm is implemented using standard cameraman, Barbara, Lena and living room images with and without attacks.

## 2. DIGITAL WATERMARKING

Technique used for hiding information inside digital multimedia is known as Digital watermarking. It is widely used for copyright protection because it can produce a new image or any other form of multimedia by manipulating the source image content with a watermark image. In digital watermarking, various keywords are used among which the significant terminologies with explanation are listed in Table 1. The digital watermarking consists of three general steps namely, deciphering removed communication, withdrawal of watermark, and authentication of deciphered data. However, the digital imprint scheme comprises of the two major steps namely, watermark embedding, and detection as shown in Figure 1.

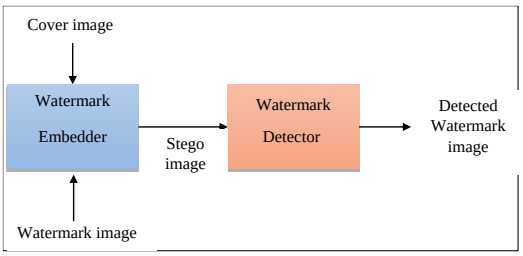


**Figure 1. Typical Digital watermarking approach**

**Table 1: Digital watermark terminology**

| Terminology | Explanation |
|---|---|
| Cover image/host image | Unique image castoff in watermarking |
| Stego / Secret image | Image that is used to hide or embed the original |
| Watermark embedding | Procedure for programming a watermark signal into an image |
| Watermark detection | Procedure for discovering a watermark concealed in an image |

The performance of the watermark algorithm can be accessed by its robustness, fidelity, security and computational cost properties. The robustness parameter of a watermark algorithm gives its ability to withstand against non-malicious distortions. The fidelity refers to the pictorial resemblance amongst secret image and its concealment image. The ability of the watermark is measured by security of a watermark for resisting malicious attacks. The various attacks are watermark insertion, estimation, removal and modification. The purpose is to reduce the safety purpose of watermarks as given in (Sunesh, 2011). Finally, the cost for computation is said to be the quantity of obligation for calculating the resources for performing watermarking, embedding and procedures of recognition.

The main objective of the watermarking is to have secret images to be comparable to cover image. Few watermarking algorithms may result in distortions in the secret images due to watermark embedding which leads to visual degrading of the image and security. This distortion property of the watermark algorithm is named as the imperceptibility or fidelity or perceptual transparency of a watermark. This property can be measured in relations of Peak-Signal to Noise Ratio (PSNR). PSNR value is higher, if there is a resemblance amongst secret image and corresponding cover image. For an 8-bit gray scale image, the PSNR value of a secret image associated with the cover image given by Equation 1.

$$PSNR = 10log_{10}\left(I_{MAX}^2/MSE\right) \quad [1]$$

Where, mean square error (MSE) is given by the equation2

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[f'(m,n) - f(m,n)]^2 \quad [2]$$

Another important parameter of the watermark algorithm is its computational cost. Since watermarking algorithms are naturally complex, they have high computational costs. The computational speed of a watermark algorithm is measured by the performance period of watermark implanting along with uncovering stages. Moreover, the hardware requirement such as processor for computing and hard disk for storing the processed images can also be used for the assessment of computational cost.

Robustness of the watermark algorithm is also an important parameter of interest which is affected by various attacks such as sound supplement, in complete collecting, elimination of row and elimination of column. These attacks on watermark images may lead to watermark detection failure without changing the visual appearance of the attacked image.

In this research work, a robust and low-computational zero-watermark algorithm is proposed using singular value decomposition and tested on standard digital images such as cameraman, Barbara, Lena and living room. The significant feature of this algorithm is that it does not result any watermarking on the given source image and hence it is called as ZW algorithm. Moreover, result of the ZW algorithm is looking very similar to the source image. This zero-watermark property is obtained by using SVD approach in which the zero-watermark sequence is computed in accordance with the equivalence of primary numeral of the main remarkable worth for each wedge.

The SVD is used as an effective tool to process the matrices. In SVD transformation, a matrix is decomposed addicted to three sub-matrices namely *U*, *D*, *V* components among which the unitary matrices are *U* and *V* and diagonal matrix is represented as D.

## 3. SINGULAR VALUE DECOMPOSITION

Linear Algebra helps the origin of SVD (Cao, 2006). The SVD can be applied on any real (m, n) matrix. For a matrix *A* with *m* rows and *n* columns, with rank *r* and $r \leq n \leq m$, the matrix *A* can be factorized into three matrices as given in Eq. 3.

$$A = UDV^T \quad [3]$$

Here the Matrix *U*is an orthogonal matrix of *m* x *m* which is given by the Eq. 4.

$$U = [u_1, u_2, \ldots u_r, u_{r+1}, \ldots, u_m] \quad [4]$$

Matrix V is an orthogonal matrix of *n* x*n* which is given by the Eq. 5.

$$V = [v_1, v_2, \ldots v_r, v_{r+1}, \ldots, v_n] \quad [5]$$

And, *S* is an *m* x *n* diagonal matrix having singe standards having diagonal direction which are denoted as $\sigma_1, \sigma_2, \ldots\ldots, \sigma_r, \sigma_{r+1}, \ldots\ldots, \sigma_n$. For $i = 1,2, \ldots\ldots, n, \sigma_i$ are known as particular standards of the matrix *A*.

As shown in Fig. 1, there are two stages of operations is projected as ZW scheme. The primary phase deals with the procedure called watermark embedding. The secondary stage deals with watermark detection extracting procedure. The algorithm is implemented using standard cameraman, Barbara, Lena and living room images without attacks and with attacks.

## 4. IMPLEMENTATION OF ZERO-WATERMARK ALGORITHM

### *4.1. Phase I: Watermark Embedder Algorithm*

The phase I of the proposed work deals with embedding the watermark in the given image. The cover image, secret image and test image used in this work are in gray-scale. The algorithm works well for gray-scale images and it is mandatory to convert the given image into gray-scale image, if the given image is in RGB format. The step by step procedure used in watermark embedder is summarized in the following steps and shown in Fig. 2(a).

*Step1:* Decompose the cover image into (*n* x *n*) small blocks as rows and columns.

*Step2:* Apply SVD transformation to all(*n* x *n*) small blocks to segment *U*, *D*, *V* components among which the unitary matrices are *U* and *V* and diagonal matrix is represented as D.

*Step3:* The non-zero coefficient is computed in the *D* module for each slab for calculating the difficulty of the block.

*Step4:* Choose the high complexity blocks using pseudo random number generator and *D* component.

*Step5:* Calculate the magnitude difference amid the neighbouring constants that is in primary support of *U* for the selected complex block.

*Step6:* Compare and check the magnitude difference against the secret watermark image. If the difference is matching with watermark, retain the coefficients otherwise modify the coefficient.

*Step7:* Fix a threshold value and associate the changes charge having verge value.

*Step 8:* Retain difference value, if it is above the threshold value and change the difference value if it is lesser than threshold value for attaining meaningful robustness of the watermark.

### *4.2. Phase II: Watermark extractor algorithm*

The watermark extractor algorithm works very similar to watermark embedder algorithm except the last step. The phase II of the proposed work deals with extracting the cover image from watermarked image. The step by step procedure used in watermark embedder is summarized in the following steps and shown in Fig. 2(b).

*Step 1:* Decompose the cover image into (*n* x *n*) small blocks as rows and columns.

*Step 2:* Apply SVD transformation to all(*n* x *n*) small blocks to segment *U*, *D*, *V* components among which the unitary matrices are U and V and diagonal matrix is represented as D.

*Step 3:* Compute amount of non-zero coefficient in the *D* component for each block to calculate the complexity of the block.

*Step4z:* Calculate the relationship of *U* component using would-be chance amount generator and *D* component feature.

*Step5:* Assign value of 1, which is nothing but the bit value for a positive association; for the extracted watermark, a bit value of 0 is assigned.

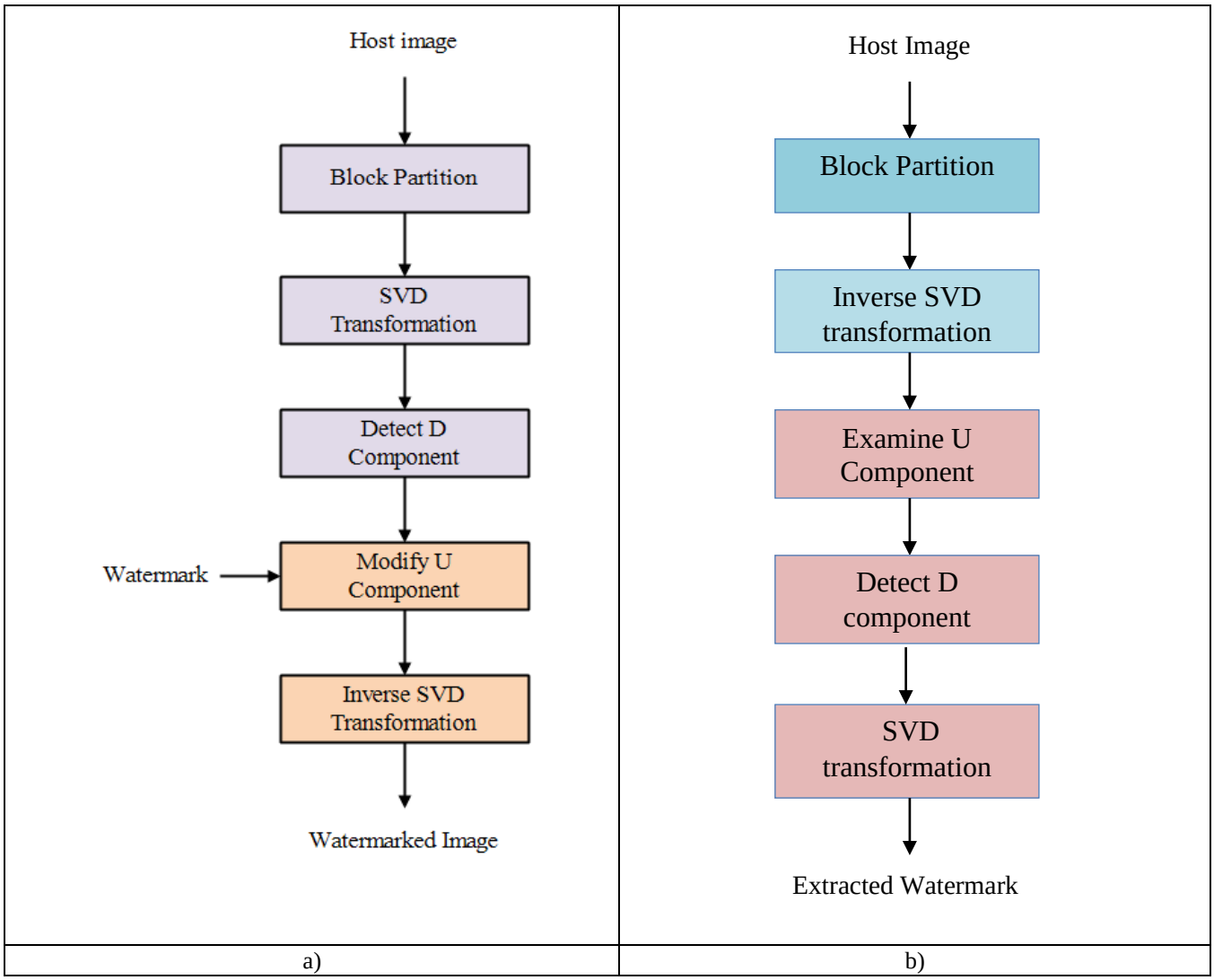


**Figure 2. Watermark algorithm, a) Embedder, and b) Extractor**

## 5. RESULTS AND DISCUSSION

The zero-water mark algorithm is implemented using standard cameraman, Barbara, Lena and living room images without attack and with and without attacks. In phase I operation of the proposed work deals with embedding the watermark in the given image. The original cover image and secret images are used to perform the embedding operation. The implementation results of the algorithm for the standard cameraman image and Lena image are shown in Figs. 3 and 4, respectively. From the figures, based on the visual appearance, it is observed that the original image and watermarked images are looking similar to each other because of the zero-watermark algorithm. The significant feature of this algorithm is that it does not fuse any watermarking in the given cover image and hence results of the zero-watermark algorithm looks very comparable to cover image.

The cover images having the dimensions are selected as 512 x 512 pixels with 4 KB size of the secret image. However, figures 5 and 6show the sample results of digital watermark extractor algorithm for cameraman image and Lena image respectively. Under noise conditions, the extractor algorithm is applied on the images and similarity measurements are calculated. The highest similarity measure of 0.8658is are obtained for cameraman image compared with Lena, Barbara and living room images as shown in Table 2. It is observed that the cameraman image is well adopted for the proposed zero-watermark algorithm than other images.

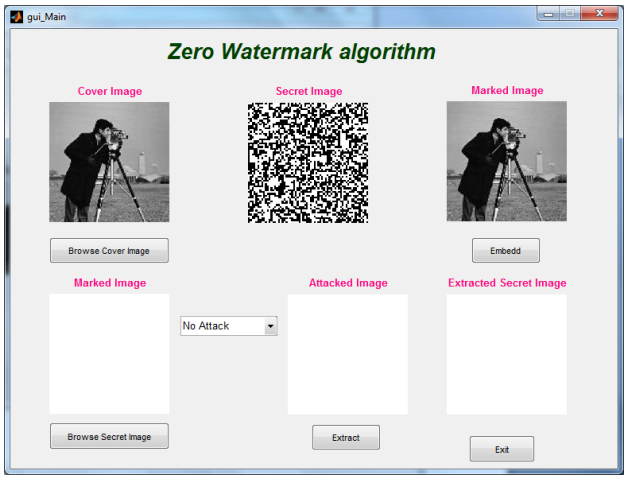


**Figure 3. Result of digital watermark Embedder Algorithm for cameraman**

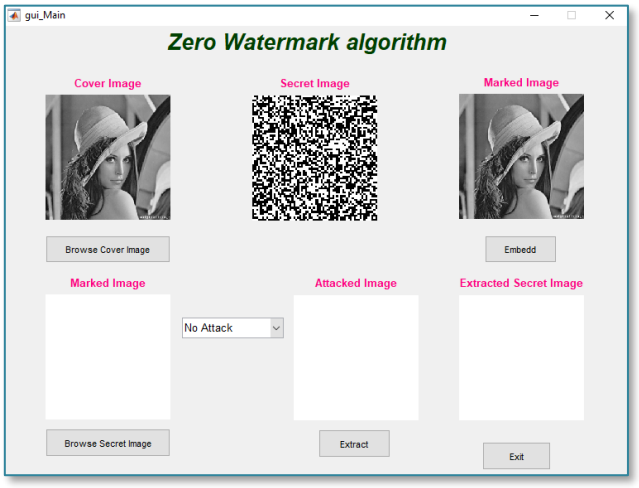


**Figure 4. Result of digital watermark Embedder Algorithm for Lena**

**Table 2: Performance analysis of the proposed algorithm for standard images with Salt and pepper attack**

| Images | Dimension | Secret Image | PSNR (dB) | Similarity Measure |
|---|---|---|---|---|
| Lena | 512x512 | 4KB | 46.35 | 0.8592 |
| Barbara | 512x512 | 4KB | 46.39 | 0.8647 |
| Cameraman | 512x512 | 4KB | 46.82 | 0.8658 |
| Living room | 512x512 | 4KB | 46.17 | 0.8575 |
| | | **Mean** | **46.43** | **0.8638** |

The robustness for the projected methodology is measured by the following way. Images namely pepper noise, Gaussian noise and noise, are considered, to which various attacks are applied. JPEG compression, cropping and mean attacks and respective PSNR values have been computed. The PSNR value is higher, if there is a similarity amongst secret image along with corresponding cover image. The PSNR and similarity measure values for the cameraman image are seen in Table 3. A higher PSNR value of 46.8231 dB is reported for salt and pepper noise along with a higher similarity value of 0.8658 as summarized in Table 3. Thus, the proposed algorithm is performing well against salt and pepper noise with significant values of PSNR and similarity measure.

**Table 3: Robustness of proposed scheme under various attacks**

| Attacks | PSNR (dB) | Similarity Measure |
|---|---|---|
| Gaussian Noise | 46.2811 | 0.8456 |
| Salt and Pepper Noise | 46.8231 | 0.8658 |
| JPEG Compression | 45.1802 | 0.8523 |
| Cropping | 46.5032 | 0.8466 |
| Mean | 46.6969 | 0.8472 |

Further, the computational cost of the algorithm is calculated as 4.442 msec of execution time for all the images under watermark embedder and watermark extractor phases using x64-based Intel Pentium III processor at 1.60 GHz with 4 GB random access memory (RAM). Though it a promising computation cost of the proposed algorithm, it can be improved further by increasing the size of RAM memory device.

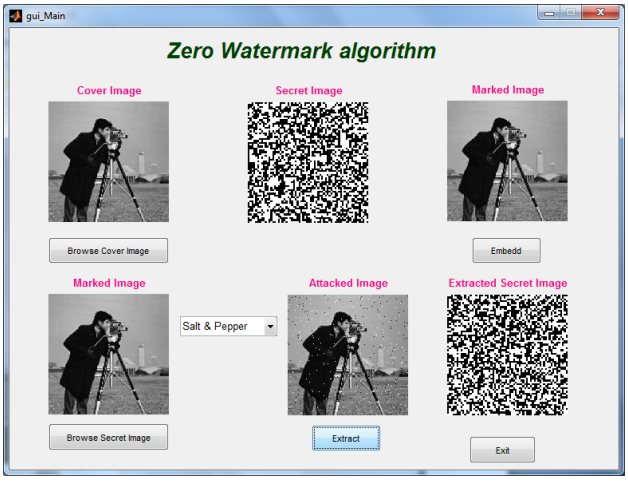


**Figure 5. Result of digital watermark extractor algorithm for cameraman**

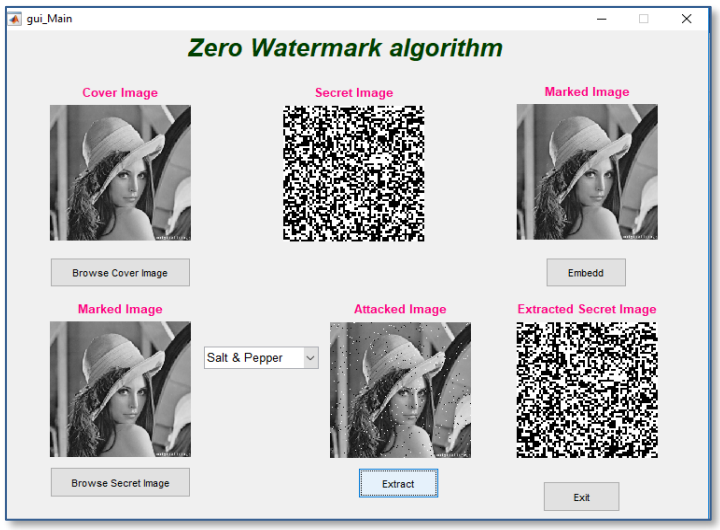


**Figure 6. Result of digital watermark extractor algorithm for Lena**

### *5.1 Comparative analysis*

To show the performance for the algorithm that is proposed, an comparative analysis is supported. In this analysis, the results obtained have been compared with existing work. The obtained results compared with Craver, *et al.* (1998), Barni, *et al.* (2003), &Akhaee,*et al.* (2010) has been tabulated in Table 4.

**Table 4: A comparative performance analysis of the proposed algorithm with existing works**

| Existing work | With Attack (Salt & Pepper) | | Without Attack | |
|---|---|---|---|---|
| | PSNR (dB) | Similarity Measure | PSNR (dB) | Similarity Measure |
| Craver, *et al.* (1998) | 45.23 | 0.85 | 54.67 | 0.92 |
| Barni, *et al.* (2003) | 44.67 | 0.84 | 51.58 | 0.95 |
| Akhaee,*et al.* (2010) | 45.56 | 0.85 | 51.08 | 0.97 |
| Proposed algorithm | 46.8231 | 0.8658 | 54.378 | 0.9781 |

From the analysis, Craver, *et al.* (1998) proposed noninvertible watermarking schemes and analysed against attacks. They achieved a PSNR value of 45.23 dB with a similarity measure of 0.85 for salt and pepper noise attack.Barni, *et al.* (2003) addressed about the finest decoding along with recognition of multipath multiplicative watermark using Weibull-distributed features and obtained a PSNR value of 44.67 dB with a similarity measure of 0.84.Akhaee, *et al.* (2010) gives out the system that supports improved multiplicative image watermarking in the contour let domain where the watermarked information is been embedded in directional sub-band. They calculated watermarked noisy coefficients by modelling the contour let coefficients with General Gaussian Distribution. This work reported a PSNR value of 45.56 dB with a similarity measure of 0.85.The proposed research work results higher values of PSNR and similarity measure as 46.8231 dB and 0.8658 for salt and pepper noise attack respectively than the existing works.

## 6. CONCLUSION

A low-computational and high vigorous ZW algorithm was proposed using SVD and implemented on the standard cameraman, Barbara, Lena and living room images with and without attacks. Initially, the cover image was decomposed into small blocks on which singular value decomposition transformation was applied. Then, the complex blocks were identified by computing non-zero coefficient. Finally, the magnitude difference against the secret watermark image was calculated and the robustness of the watermark was obtained by fixing suitable vergeworth. Performance of proposed ZW algorithm was accessed by means of PSNR values and similarity values. The highest similarity measure of 0.8658was obtained for cameraman image under salt and pepper noise attack with a higher PSNR value of 46.8231 dB.Further, the computational cost of the algorithm was calculated as 4.442 msec of execution time for all the images under watermark embedder and watermark extractor phases. Thus, the proposed algorithm can be utilised as a promising approach in digital rights management to protect the copying and reproducing of copyrighted digital media and works.

## REFERENCES:


1. Akhaee, M.A.,Sahraeian, S.M.E.,Marvasti, F. (2010),"Contourlet-Based Image Watermarking using Optimum Detector in a Noisy Environment", IEEE Transactions on Image Processing, Vol. 19, No. 4, 967-980.
2. Barni, M., *et al.* (2013), "Optimum Decoding and Detection of Multiplicative Watermarks", IEEE Transactions on Signal Processing, Vol. 51, No. 4, 1118-1123.
3. Burt, P.J., Adelson, E.H. (1983),"The Laplacian pyramid as a compact image code", IEEE Transactions on Communications, Vol. 31, No. 4, 532-540.
4. Cao, L. (2006),"Singular value decomposition applied to digital image processing", Division of Computing Studies, Arizona State University Polytechnic Campus, Mesa, Arizona State University polytechnic Campus.
5. Craver, S., *et al.* (1998),"Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitation, Attacks and Implications", IEEE Journal on Selected Areas in Communication, Vol. 16, No. 4, 573-586.
6. Jian Zhao., Wensheng X., Shunli Zhang., Shuaishuai Fan., and Wanru Zhang. (2016), "A Strong Robust Zero-Watermarking Scheme Based on Shearlets' High Ability for Capturing Directional Features", Mathematical Problems in Engineering, Vol. 2016, 1-11. Ghatak, P., Tripathi, R., Chakravarti, A. (2004), "Digital Rights Management: An Integrated Secure Digital Content Distribution Technology", Journal of Intellectual Property Rights, Vol. 9, 313-331.
7. Leng, X., Xiao, J., and Wang, Y. (2012),"A robust image zero-watermarking algorithm based on DWT and PCA", International Conference on Communication and Information Processing (ICCIP), Springer, 484-492.
8. Liu, R.Z., and Tan, T.N.(2002), "An SVD-Based Watermarking Scheme for Protecting Rightful Ownership", IEEE Transactionson Multimedia, Vol. 4, No. 1, 121–128.
9. Rawat, H., Kumar, A. and Kumar, S.(2013), "Robust Digital Image Watermarking Scheme for Copyright Protection", International Journal of Computer Applications, Vol. 75, No. 18.
10. Saini, L.K., Shrivastava, V. (2014),"A Survey of Digital Watermarking Techniques and its Applications", International Journal of Computer Science Trends and Technology,Vol. 2, No. 3.
11. Stamp, M. (2003),"Digital Rights Management: The Technology Behind the Hype", Journal of Electronic Commerce Research, Vol. 4, No. 3, 102-112.
12. Sunesh, H. (2011), "Watermark Attacks and Applications in Watermarking", In proceedings published in International Journal of Computer Applications, National Workshop-Cum-Conference on Recent Trends in Mathematics and Computing.
13. Wen, Q., Sun, Y.-f., Wang, S.-x. (2003),"Concept and Application of Zero-watermark", Acta Electronica Sinica, Vol. 31, No. 2, 214-216.
14. Ye, T. (2011),"A Robust Zero-Watermark Algorithm Based on Singular Value Decomposition and Discreet Cosine Transform', In: Qi L. (eds) Parallel and Distributed Computing and Networks,2010, Communications in Computer and Information Science, Vol 137, Springer, Berlin, Heidelberg.
15. Yuan, D.-y., Xiao, J., Wang, Y. (2008),"Study on the Robustness of Digital Image Watermarking Algorithms to Geometric Attacks", Journal of Electronics and Information Technology, Vol. 30, No. 5, 1251-1256.