

Simulation of Robust DWT-SVD Transform Domain Based Digital Image Watermarking Technique: A Survey

Shubham Arya, Mr. Pratyush Tripathi

Abstract— The purpose of this paper is to improve the robustness of traditional image watermarking based on singular value decomposition (SVD) by using optimization-based quantization on multiple singular values in the wavelet domain. In this work, we divide the middle-frequency parts of discrete-time wavelet transform (DWT) into several square blocks and then use multiple singular value quantizations to embed a watermark bit. To minimize the difference between original and watermarked singular values, an optimized-quality formula is proposed. First, the peak signal-to-noise ratio (PSNR) is defined as a performance index in a matrix form. Then, an optimized-quality functional that relates the performance index to the quantization technique is obtained. Finally, the Lagrange Principle is utilized to obtain the optimized-quality formula and then the formula is applied to watermarking. Experimental results show that the watermarked image can keep a high PSNR and achieve better bit-error rate. This paper represents different Digital Watermarking Techniques which permits an individual to add hidden copyright notice as well as any other verification messages to images so that it can be protected from the unauthorized access. Generally watermark is provided with two types one is visible watermark and other is invisible watermark. The main aim of paper is to explore the comparison of various digital image watermarking techniques and it also demonstrates that all these watermarking techniques provides image watermarking with full security and reasonable capacity.

Index Terms— Digital watermarking, Discrete Wavelet Transform, Singular value decomposition.

I. INTRODUCTION

Digital watermarking is the process of embedding information into a digital signal which may be used to verify its authenticity or the identity of its owners, in the same manner as paper bearing a watermark. For visible identification [1]. In digital watermarking, the signal may be audio, pictures, or video. If the signal is copied, then the information also is carried in the copy. A signal may carry several different watermarks at the same time. Image watermarking is an effective method to learn the unofficial use of authorized images. This method positions key data into sponsor picture which assists to locate the rightful control of image [2]. Generally digital image watermarking is just a way which is used to embed key data with some extra information in the original image which could be found when it will be required for different applications such as validation, operator recognition, material safety and trademark safety etc [3].

Shubham Arya, M.Tech Scholar, Department of Electronics & Communication Engineering, Kanpur Institute Technology Kanpur, India.
Pratyush Tripathi, Associate Professor, Department of Electronics & Communication Engineering, Kanpur Institute Technology Kanpur India.

Often the scaling factor can also be employed for watermark embedding [4].

In Watermarking scheme, watermark is employed into original image, for the purpose of authenticating the host [5]. Fig (1) reveals the step by step process of embedding watermark into the original image. Later on, because of noise or other attacks degraded image is obtained which further detects the watermark which was earlier embedded into the cover image.

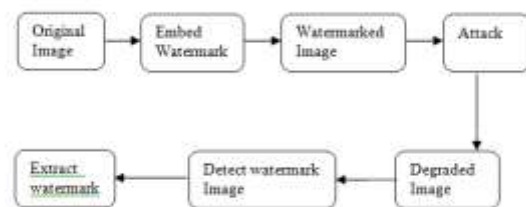


Figure 1: General Watermarking block diagram

II. DIGITAL WATERMARKING TECHNOLOGY

Digital Watermarking Attribute

In general, the characteristics of digital watermarking are as follows.

Security: Watermark is said to be secure only if an attacker is unable to eliminate the watermark without the knowledge of algorithm which was used for embedding [5]. Unauthorized parties can never access the watermark.

Robustness: Watermark is said to be robust if it remains same after some attack [6]. An embedded watermark is robust if it is not altered after a variety of operations and manipulations for instance scaling, filtering, compression etc.

Imperceptibility: If quality of first picture can never get influenced after embedding watermark then it is said to be imperceptible. Hence watermark should be invisible to human eyes [7].

Computational cost: Computational costs will be high if the complex algorithms are used for watermarking because complex algorithms always use more hardware as well as software resources. To reduce the computational costs, watermarking methods should be less complex [8].

Capacity: Image watermarking capacity is an evaluation of how much information can be hidden within a digital image. Watermarking capacity is determined by the statistical model used for the host image, by the distortion constraints on the data hider and the attacker, and by the information available to the data hider, to the attacker, and to the decoder.

Digital Watermarking Classification

Digital watermarking can be divided into robust watermarking and fragile watermarking according to its

characteristics. Robust watermarking is mainly used to sign copyright information of the digital works, the embedded watermark can resist the common edit processing, image processing and lossy compression, the watermark is not destroyed after some attack and can still be detected to provide certification. Fragile watermarking is mainly used for integrity protection, which must be very sensitive to the changes of signal. We can determine whether the data has been tampered according to the state of fragile watermarking. Digital watermarking can be divided into image watermarking, video watermarking, audio watermarking, and text watermarking and graphic watermarking based on the attached media. Image watermarking refers to adding watermark in still image. Video watermarking adds digital watermark in the video stream to control video applications. Text watermarking means adding watermark to PDF, DOC and other text file to prevent changes of text. Graphic watermarking is embedding watermark to two-dimensional or three-dimensional computer-generated graphics to indicate the copyright.

According to the detection process, digital watermarking can be divided into blind watermarking and visual watermarking. Blind watermarking does not need original data, which has wide application, but requires a higher watermark technology. Visual watermarking needs the original data in the testing course, it has stronger robustness, but its application is limited. See figure 2.

Digital watermarking can be divided into copyright protection watermarking, based on its purpose. Copyright protection watermarking means if the owners want others to see the mark of the image watermark then the watermark can be seen after adding the watermark to the image, and the watermark still exists even if it is attacked. Tampering tip watermarking protects the integrity of the image content, labels the modified content and resists the usual lossy compression formats. Anonymous mark watermarking can hide important annotation of confidential data and restrict the illegal users to use confidential data.

III. WATERMARKING TECHNIQUES

Discrete Wavelet Transform

If watermarking techniques can exploit the characteristics of the Human Visual System (HVS), it is possible to hide watermarks with more energy in an image, which makes watermarks more robust. From this point of view, the DWT is a very attractive transform, because it can be used as a computationally efficient version of the frequency models for



Figure 2: (a) the original Lena image (b) logo to be watermarked (c) visible watermarked image and (d) invisible watermarked image.

the HVS [5]. For instance, it appears that the human eye is less sensitive to noise in high resolution DWT bands and in the DWT bands having an orientation of 45° (i.e., HH bands). Furthermore, DWT image and video coding, such as embedded zero-tree wavelet (EZW) coding, are included in the upcoming image and video compression standards, such as JPEG2000 [9]. Thus DWT decomposition can be exploited to make a real-time watermark application.

Many approaches apply the basic schemes described at the beginning of this section to the high resolution DWT bands, LH, HH, and HL [10]. A large number of algorithms operating in the wavelet domain have been proposed till date.

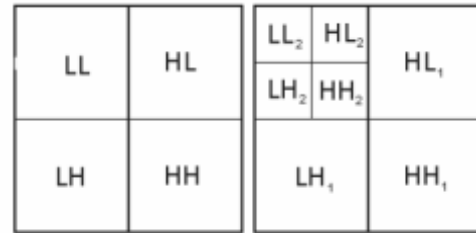


Figure 3: Level-1 and level-2, 2-Dimensional DWT

Singular Value Decomposition

The singular value decomposition (SVD) of $m \times n$ real valued matrix A with $m \geq n$, performs orthogonal row and column operations on A in such a way that the resulting matrix is diagonal and diagonal values (singular values) are arranged in decreasing value and coincide with the square root of the Eigen values of $A^T * A$ [11]. The column of the $m \times m$, U has mutually orthogonal unit vectors, as are the columns of the $n \times n$, V matrix. U and V are orthogonal matrices i.e.

$$U^T * U = V^T * V = VV^T = 1 \quad \dots(1)$$

S is a pseudo-diagonal matrix, having diagonal elements as singular values. We can get the matrix A again by using following approach:

$$A = USV^T \quad \dots(2)$$

Where U and V are orthogonal matrices, and $D = \text{diag}(\lambda_i)$ is a diagonal matrix of singular values λ_i , $i = 1, 2, \dots$, which are arranged in decreasing order. The columns of U are the left singular vectors, and the columns of V are the right singular vectors of image A .

There are two main properties to employ the SVD method in digital watermarking scheme [12,26]:

- Small Variation in singular values does not affect the quality of image.
- Singular Values of an image have high stability so; they don't change after various attacks.

In the past couple of years, several digital watermarking schemes have been proposed and based on DCT, DFT, and DWT transformations. Singular value decomposition (SVD)-based watermarking scheme [13,27] is proposed. SVD transformation preserves both one-way and non-symmetric properties, usually not obtainable in DCT and DFT transformations. In the proposed scheme, both of the D and U components are explored for embedding the watermark. In this work, we divide the middle-frequency parts of discrete-time wavelet transform (DWT) into several square blocks and then use multiple singular value quantizations to embed a watermark bit [14]. To minimize the difference between original and watermarked singular values, an

optimized-quality formula is proposed. First, the peak signal-to-noise ratio (PSNR) is defined as a performance index in a matrix form. Then, an optimized-quality functional that relates the performance index to the quantization technique is obtained. Finally, the Lagrange Principle is utilized to obtain the optimized-quality formula and then the formula is applied to watermarking as given in equation (2). Experimental results show that the quality of the watermarked image is good and that there is strong resistance against general image processing. Furthermore, the extracted watermark can still be easily identified after tampering.

Arnold Transform

Image scrambling determines change of the image which rearranges the spatial place of the pixels according to the rules, and makes image distortion for the purpose of security [15]. If the change rules and guidelines weren't provided, the initial image can't be reconstructed. Regular techniques for scrambling contain Arnold change, Miraculous change, Fractal Hilbert bend, Conway sport and Gray code change etc [16]. Arnold transform is surely an effective as well as strong iterative technique. It is used to provide randomization to the elements of any array and it could only be solved right back with the help of unique key. That stops the unauthorized accessibility of watermark despite with the successful extraction [17]. A matrix $P \times Q$ of an image having height N is scrambled by method:

$$\begin{pmatrix} P' \\ Q' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} P \\ Q \end{pmatrix} \text{ mod } (N)$$

Where (P, Q) is location of original image pixels, while (P', Q') are coordinates of transformed picture pixels [18]

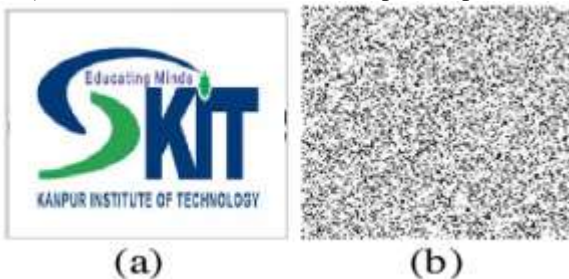


Figure 4(a) watermarked image (b) Arnold transformed watermarked image

Artificial Bee Colony

ABC is really an easy and effective population based optimization algorithm. It is related to the intelligent foraging activities of the honey bee swarms. The probable alternatives are displayed by the food source in ABC and fitness of some of these alternatives is displayed by the nectar quantity of the food source [19]. In this algorithm, you will find three categories of bees in colony of artificial bee: employed bees, onlookers and scouts. The total quantity of employed bees is corresponding to how many foodstuff options are there across the hive. Employed bee whose food resource got forgotten by the bees becomes scout [20]. ABC contains three necessary components.

- 1) Food resources: Profitability of food resources is related with many facets for instance abundance of food, their closeness to nest and the easily getting the power from the source.
- 2) Employed bees: These bees are linked with particular food option which they exploited as well as hold information regarding the precise source [21]. They reveal these details

with the forager bees that wait in the hive by dance that is a typical example of numerous interactions.

- 3) Unemployed bees: Unemployed bees contain onlookers and scouts. The scouts arbitrarily research food sources [22].

In Artificial Bee Colony algorithms, first of all it initializes the solution population and evaluates it. Further it generates new solutions for employed bees and evaluates those generated solutions for keeping the very best option among current and the candidate. According to fitness of onlooker bees a visited solution is selected and later it generates new solutions for onlooker bees and evaluates those generated solutions. Now again keep the very best solution among current and candidate. Furthermore it checks for abandoned food source and if it exists then replace it with scout bee and it saves the best solution in memory.

IV. WATERMARKING ATTACKS

Due to some reasons, there is need of adding, altering or removing false watermarks. Attacks on watermarks may be accidental or intentional. Accidental attacks may cause due to the standard image processing or due to the compression Procedures. Intentional attacks includes cryptanalysis, steganalysis, image processing techniques or other attempts to overwrite or remove existing watermarks.

We need to distinguish two reasons for an attack against a watermark image:

- Hostile or malicious attacks, which are an attempt to weaken, remove or alter the watermark, and
- Coincidental attacks, which can occur during common image processing and are not aimed at tampering with the watermark.

There are four large categories of attacks can be invoked to penetrate a watermarking system:

- Removal attacks
- Geometrical attacks
- Cryptographic attacks
- Protocol attacks

Removal attacks attempt to separate and remove the watermark. If somebody tries to remove the watermark from the data, this is called a removal attack. The goal is to add distortion to the host image in order to render the watermark undetectable. The attack is successful if the watermark cannot be detected anymore, but the image is still intelligible and can be used for a determined purpose.

Geometrical attacks are not aimed at removing the watermark, but try to either destroy it or disable its detection. They attempt to break the correlation detection between the extracted and the original watermark sequence, where the image is subjected to translation, rotation, scaling and/or cropping. This can be accomplished by shuffling the pixels. The values of corresponding pixels in the attacked and the original image are the same. However, their location has changed. The **cropping** is a very common attack since in many cases the attacker is interested in a small portion of the watermarked object, such as parts of a certain picture or frames of video sequence. In order to survive, the watermark needs to be spread over the dimensions where this attack takes place.

Cryptographic attacks are aimed at cracking the security methods in watermarking schemes and thus finding a way to remove the embedded watermark information or to embed

misleading watermarks. One such technique is brute-force search for the embedded secret information. Practically, application of these attacks is restricted due to their high computational complexity. They cover, for example, direct attacks to find the secret key or attacks called collusion attacks. Cryptographic attacks are very similar to the attacks used in cryptography.

Protocol attacks neither aim at destroying the embedded information nor at disabling the detection of the embedded information (deactivation of the watermark). Rather, they take advantage of semantic deficits of the watermark's implementation. The protocol attacks aim at attracting the concept of the watermarking application. This can create a situation of ambiguity with respect to the real ownership of the data. The requirement of non-invertability on the watermarking technology implies that it should not be possible to extract a watermark from non-watermarked image. As a solution to this problem, the authors proposed to make watermarks signal-dependent by using a one-way function. Consequently, a watermark must not be invertible or to be copied. A copy attack would aim at copying a watermark from one image into another without knowledge of the secret key. It also belongs to the group of the protocol attacks. Here, the goal is not to destroy the watermark or impair its detection, but to estimate a watermark from watermarked data and copy it to some other data, called target data.

V. CONCLUSION AND FUTURE SCOPE

A digital watermarking is probably the strong implies to uncover the particular unauthorized uses of copyrighted image. So this paper shows about the comparison of various techniques based on image watermarking. This paper indicates that the ABC for watermarking has improved results when implemented on the DWT, SVD techniques but there are some issues such as the use of watermark scrambling still are unattended. In near future a new technique will be proposed which will improve the speed and security of the watermarking technique further.

Digital watermarking has been proposed as one way to protect such interests. Though much research remains before watermarking systems become robust and widely available, there is much promise that they will contribute significantly to the protection of proprietary interests of electronic media. Collateral technology will also be necessary to automate the process of authentication, non-reputable transmission and validation. An exhaustive list of watermarking applications is of course impossible. However, it is interesting to note the increasing interest in fragile watermarking technologies. Especially applications related to copy protection of bills with digital watermarks. Various companies have projects in this direction solutions will soon be available. In addition to technological developments, marketing and business issues are extremely important and require in-depth analysis and strategic planning. It is very important to prepare the industry to the usage of digital watermarks and it is very likely that fully functioning to convince them of the added value their products can gain if they employ digital watermarking technologies.

VI. APPLICATIONS

The technique "Digital Watermarking" is the recent research in the field of multimedia and internet copyright protection

field. There are various applications of DWM as broadcast monitoring, owner identification, proof of ownership, transaction hacking, content authentication, copy control, device control and so on. Out of these, some important applications are described as follows

1. Broadcast Monitoring: This application identifies that when and where works are broadcast by recognizing watermarks embedded in these works. There are varieties of technologies to monitor playback of sound recording on broadcast. The DWM is alternative to these technologies due to its reliable automated detection. A single PC based monitoring station can continuously monitor to 16 channels over 24 hours with no human interaction. Resulted monitoring is assembled at central server and is now available to interested one. The system can distinguish between identical versions of songs, which are watermarked for different distribution channel. Such system requires Monitoring infrastructure and watermarks to be present in content. Watermarking video or music is planned by all major entertainment companies possessing closed networks.

2. Encoding: According to the thinking of major music companies and major video studios, encoding happens at mastering level of sound recording. In such downstream, transactional watermarks are also considered. Each song is assigned with unique ID from the identifier database. After completion of all mastering processes, ID is encoded in sound recording. To enhance encoding of audio or video recordings requiring special processing, the human-assisted watermark key is available.

3. Copy and playback control: The data carried out by watermark may contain information about copy and display permissions. We can add a secure module into copy or playback equipment to automatically extract the permission information and block further processing if required. This approach is being taken in Digital Video Disc (DVD).

4. Content authentication: The content authentication is nothing but embedding the signal information in Content. This signature then can be checked to verify that it has not been alter. By watermarks, digital signatures can be embedded into the work and any modification to the work can be detected.

REFERENCES

- [1] Gary L. Friedman, The trustworthy digital camera: restoring credibility to the photographic image, *IEEE Trans. Consum. Electron.* 39 (4) (1993)905-910.
- [2] V.M. Potdar, S. Han, E. Chang, A survey of digital image watermarking techniques, 3rd IEEE International Conference on Industrial Informatics INDIN'05 (2005) 709-716.
- [3] Patra, Jagdish Chandra, et al. "An improved SVD-based watermarking technique for image and document authentication." *Circuits and Systems, 2006. APCCAS 2006. IEEE Asia Pacific Conference on. IEEE, 2006.*
- [4] Karaboga, Dervis, and Bahriye Basturk. "Artificial bee colony (ABC) optimization algorithm for solving constrained optimization problems." *International Fuzzy Systems Association World Congress. Springer Berlin Heidelberg, 2007.*
- [5] Zhao, Mingwei, and Yanzhong Dang. "Color image copyright protection digital watermarking algorithm based on DWT & DCT." *Wireless Communications, Networking and Mobile Computing, 2008. WiCOM'08. 4th International Conference on. IEEE, 2008.*
- [6] Narasimhan, Harikrishna. "Parallel artificial bee colony (PABC) algorithm." *Nature & Biologically Inspired Computing, 2009. NaBIC 2009. World Congress on. IEEE, 2009.* 8. R Liu, T Tan, An SVD-based watermarking scheme for protecting rightful ownership. *IEEE Transactions on Multimedia* 4(1), 121-128 (2002)

- [7] Gaurav Bhatnagar, Balasubramanian Raman, A new robust reference watermarking scheme based on DWT-SVD, *Comput. Stand. Interfaces* 31 (5)(2009) 1002–1013.
- [8] Lai, Chih-Chin, and Chih-Hsiang Yeh. "A hybrid image watermarking scheme based on SVD and DCT." *Machine Learning and Cybernetics (ICMLC)*, 2010 International Conference on. Vol. 6. IEEE, 2010.
- [9] Choudhary, Rita, and Girish Parmar. "A robust image watermarking technique using 2-level discrete wavelet transform (DWT)." *Communication Control and Intelligent Systems (CCIS)*, 2016 2nd International Conference on. IEEE, 2016.
- [10] N. Divecha and D. N. N. Jani, "Implementation and performance analysis of DCT-DWT-SVD based watermarking algorithms for color images," *International Conference on Intelligent Systems and Signal Processing (ISSP)*, pp. 204-208, 2013.
- [11] J. Guru, H. Dhamecha and B. Patel, "Fusion of DWT and SVD digital watermarking Techniques for robustness," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 4, no. 9, pp. 791-797, 2014.
- [12] C-C Chang, P Tsai, C-C Lin, SVD-based digital image watermarking scheme. *Pattern Recogn. Lett.* 26(10), 1577–1586 (2005)
- [13] KL Chung, WN Yang, YH Huang, ST Wu, YC Hsu, On SVD-based watermarking algorithm. *Application. Math. Comput.* 188, 54–57 (2007)
- [14] RA Ghazy, NA El-fishawy, MM Hadhoud, MI Dessouky, FEA El-Samie, An efficient block-by-block SVD-based image watermarking scheme, in 2007 Radio Science Conference, Cairo, 2007, pp. 1–9.
- [15] Zheng, Peijia, and Jiwu Huang. "Discrete wavelet transform and data expansion reduction in homomorphic encrypted domain." *IEEE Transactions on Image Processing* 22.6 (2013): 2455-2468.
- [16] Musrat Ali, Chang Wook Ahn, Millie Pant, A robust image watermarking technique using SVD and differential evolution in DCT domain, *Opt.: Int. J.Light Electron Opt.* 125 (1) (2014) 428–434.
- [17] Nasrin M. Makbol, Bee Ee Khoo, A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition, *Digital Signal Process.* 33 (2014) 134–147.
- [18] Guo, Jianting, Peijia Zheng, and Jiwu Huang. "Secure watermarking scheme against watermark attacks in the encrypted domain." *Journal of Visual Communication and Image Representation* 30 (2015): 125-135.
- [19] Gonge, Sudhanshu Suhas, and Ashok Ghatol. "A Robust and Secure DWT-SVD Digital Image Watermarking Using Encrypted Watermark for Copyright Protection of Cheque Image." *International Symposium on Security in Computing and Communication*. Springer International Publishing, 2015.
- [20] Harjito, Bambang, and Heri Prasetyo. "False-positive-free GSVD-based image watermarking for copyright protection." *Electronics and Smart Devices (ISESD)*, International Symposium on. IEEE, 2016.
- [21] Ansari, Irshad Ahmad, Millie Pant, and Chang Wook Ahn. "ABC optimized secured image watermarking scheme to find out the rightful ownership." *Optik-International Journal for Light and Electron Optics* 127.14 (2016): 5711-5721.
- [22] L Xiao, H Wu, Z Wei, Multiple digital watermarks embedding in wavelet domain with multiple-based number. *J. Computer. Aided. Design. Computer. Graphics.* 15(2), 200–204 (2003)
- [23] P Bao, X Ma, Image adaptive watermarking using wavelet domain singular value decomposition. *IEEE Transactions on Circuits and Systems for Video Technology* 15(1), 96–102 (2005)
- [24] CV Serdean, MK Ibrahim, A Moemeni, MM Al-Akaidi, Wavelet and multiwavelet watermarking. *IET Image Process.* 1(2), 223–230 (2007)
- [25] OZ Azza, M Achraf, B Ammar, Wavelet domain watermark embedding strategy using TTCQ quantization. *J. Computer Sci. Network Security.* 7(6), 165–170 (2007)
- [26] B Gaurav, R Balasubramanian, A new robust reference watermarking scheme based on DWT-SVD. Elsevier: *Computer Standards and Interfaces*, 2009, pp. 1–12
- [27] CC Lai, CC Tsai, Digital image watermarking using discrete wavelet transform and singular value decomposition. *IEEE Trans. Instrum. Meas.* 59(11), 3060–3063 (2010)

Shubham Arya, M.Tech Scholar, Department of Electronics & Communication Engineering, Kanpur Institute Technology Kanpur, India.

Pratyush Tripathi, Associate Professor, Department of Electronics & Communication Engineering, Kanpur Institute Technology Kanpur India