A Survey Study on Singular Value Decomposition and Genetic Algorithm Based on Digital Watermarking Techniques

Mokhtar Hussein and Manjula Bairam

Abstract In digital image watermarking, many techniques are used for obtaining optimal image representation; image decomposition as a standard set in the frequency domain is not necessary (DCT, DWT, and DFT). Therefore, another representation of transform was explored which is about using algebra methods and algorithms with watermarking like singular value decomposition algorithm based on watermarking. SVD algorithms have shown that they are highly strong against extensive range of attacks. In addition to that, Genetic Algorithm (GA) is used with SVD to optimize the watermarking. Many techniques and algorithms have already been proposed on the using of SVD and GA on digital watermarking. In this paper, we introduce a general survey on those techniques along with analysis for them based on the two measures, transparency and robustness.

Keywords Genetic algorithm · Singular value decomposition · Digital watermarking

1 Introduction

A digital watermarking can be defined as a sequence of special information inserted invisibly into another multimedia file; this information is related to the owner of the multimedia file and later can be extracted to be considered as copyright ownership evidence. Embedding a watermark w into the original image (cover image or host image) I is the primary conception of digital watermarking that is for achieving and obtaining copyright protection, monitoring of broadcast, access control, and etc. The watermark w could be a digital signal, a label, or a tag. The host digital media could be image, audio, video, or software. The watermarked media Iw is $I + w$.

M. Hussein (✉) · M. Bairam
Department of Computer Science, Kakatiya University, Warangal, Telengana, India
e-mail: msorori201201@gmail.com

M. Bairam
e-mail: manjulabairam@gmail.com

S.C. Satapathy et al. (eds.), *Proceedings of the First International Conference on Computational Intelligence and Informatics*, Advances in Intelligent Systems and Computing 507, DOI 10.1007/978-981-10-2471-9_2

Digital watermarking algorithms and techniques are categorized into two types or domains, namely spatial and transform domains.

Spatial domain techniques are minimal robust for several types of offensives and susceptible to manipulate (to forge) by prohibited users [1]. Techniques related to transform domain are more robust and secure to several and different types of attacks, these techniques embed *w* into *I* by modulating the coefficients like Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), Discrete Wavelets Transform (DWT), and Singular Value Decomposition (SVD). The size of *w* could be inserted into *I* is generally 1/16 of *I*. Robustness can be gained when considerable modifications are made to *I* while inserting *w*, regardless the domain without affecting the visual and quality of *I*. Those modifications are identifiable, and therefore, thus do not meet the requirements of invisibility (transparency) [2]. Designing and planning an optimal watermarking system for a specified application constantly include a trade-off in between those requirements, so that, if the mentioned issue can be addressed as an issue of optimization, then it can be resolved using one of the soft computing tools related to Artificial Intelligence (AI), viz., Genetic Algorithm (GA), Fuzzy Logic, and Neural Networks [3–5]. Watermark w could be scaled by the Scaling Factor (SF) denoted by k prior the process of embedding, this k is utilized to control the intensity and immovability of w. Watermark *w* can be embedded into *I* either via adjusting values of pixels or modifying the coefficients of transform domain. When SF is greater that means more distortion (more transparency) in the quality of *I* and stronger robustness. Furthermore, when SF is minimal that means much better quality of image and weaker robustness [4, 5]. Various spectral components may show diverse possibility to amendment. Thus, an individual SF may not be viable for adjusting all the values of *I*. Then, several SFs should be utilized for adapting to the divers spectral ingredients to minimize visual artifacts [1, 4].

For all the techniques and methods previously developed, they usually utilize predefined embedding essential rules and define their parameters of embedding, such as embedding strength and threshold. Often, it is hard to set optimal watermarking parameters, because watermarking algorithms have wider space of parameter. Consequence, those techniques and algorithms do not demonstrate desired performance [6, 7]. As a rule, digital watermarking is having two measures for performance, namely imperceptibly and robustness. Yet, inserting *w* inside *I* decrease the visual quality of image, while it is desirable that the dissolution must not be readily observed. Thence, imperceptibility indicates the concept which should be unrealizable to visual system of human. Both of the performance measures, imperceptibility and robustness, are conflicting with each other [8]. An optimal watermark system has to make equilibrium between the two. Hence, the problem of optimal watermark is from the multi objective optimization problem.

Therefore, many techniques are used with digital watermarking; they generally called soft computing tools, such as neural networks, genetic algorithms, and fuzzy logic. In addition to that, a number of transformations are used along with these techniques, such as DFT, DCT, DWT, and SVD. In this paper, we are concentrating only on highlighting the digital image watermarking techniques which used the concepts of SVD and GA.

2 Digital Watermarking Based on SVD

This section represents a general description of SVD with digital watermarking. The notion of SVD was founded for real-square matrices by Beltramin and Joda in the 1870s, for complex matrices in 1902, by Autonne, and has been expanded to rectangular matrices in 1939 by Echart and Young. Finally, SVD has been utilized in image processing applications, such as image hiding, image compression, and noise reduction.

SVD is famed as a transformation of an algorithm matrix which is relay on Eigenvector. It is an athletic tool which is applied during matrices analyzes. It is familiar that SVD is considered one of the generality sturdy techniques used in the numeric analysis along with so many number of applications, including watermarking [4, 9, 10]. SVD is also known as a mathematical method used to elicit algebraic lineaments out of image. Substance idea of SVD-based approach is to stratify the SVD to the entire I or at least to few segments of that image, and, therefore, adjust the singular values to insert the watermark. Three features are there to utilize the SVD technique with digital watermarking scheme, the first one is that the size of matrices in SVD transformation is unspecified; second, there will be no large variation of image's singular values when a slight disruption is added to that image, and the third one is that SVs exemplify the actual algebraic properties of image [11]. The above-mentioned properties of SVD are quite likeable to evolve watermarking techniques and algorithms and techniques which are particularly robust against the geometric offensives. In general, the energy or strength of w can be controlled using a scaling factor. Watermarking approach effectiveness is extremely relies on selecting an appropriate scaling factor. Ganic et al. [12] pointed that the scaling factor is set to be constant in several SVD-based studies. While that Cox et al. [13] argued that considering a unique single consonant scaling factor may not be usable in some situations, then they proposed that users can use various or multiple scaling factors instead of using only one. SVD always decompose a real matrix A with M * N to three sub matrices A = USVT, where U and V are M * N and N * N orthogonal matrices, respectively, S is considered as N * N diagonal matrix, i.e., consider a real M * N matrix A, and gather this matrix into two orthogonal matrices (U and V) and a diagonal matrix (S). The elements or entries in S are only non-zero on the diagonal and are named as singular values of A. Matrices size from SVD transformation is not fixed, so that it could be a rectangle or a square. Singular values in a digital are minimal influenced to common image processing algorithms and techniques, because they resist against attacks. When r is the rank of the matrix A and $S = \text{diag}(\lambda_i)$ where $i = 1, 2, \ldots, n$, then these singular values satisfy the following equation:

$$\lambda 1 \geq \lambda 2 \geq \lambda 3 \geq \cdots > \lambda \text{rank}(A) > 0.$$

When A indicates a matrix that its elements are pixel values of that image, thereafter this image can be written as:

$$A = USV^T = \sum_{i=1}^{r} \lambda_i u_i v_i^T.$$

As known, watermarking system composed of two main processes, embedding and extraction processes.

2.1 Embedding Process

The algorithm used in embedding process first applies SVD to *I,* then modify *S* with *W,* then apply SVD to *Sm*, and, finally, compute the watermarked image *Iw*. This algorithm can be represented mathematically as the following:

1. $I = USV^T$
2. $Sm = S + Kw$
3. $Sm = Um\ Sw\ V^T w$
4. $Iw = U\ Sw\ V^T$

2.2 Extraction Process

In the extraction process, first apply SVD to *Iw* which is possibly distorted, then compute possibly corrupted and, finally, extracted the watermark. This algorithm represented mathematically as follows:

1. $Iw = U\ Sw\ V^T$
2. $Smc = Uw\ Sw\ V^T$
3. $w = (Sc - S)/k.$

3 Digital Watermarking Based on Genetic Algorithm

Among all digital watermarking, imperceptibility and robustness are considered as the two inconsistent requirements required by any digital watermarking system. An effective watermarking system necessarily has to make a delicate trade-off in between these conflicting properties. This section explains how to use GA to optimize the process of watermarking embedding with respecting to the two inconsistent or conflicting required conditions transparency and robustness for various types of attacks. It presents a general information on GA and how to apply them with digital watermarking.

Genetic Algorithm is the most popular evolutionary algorithm widely used for optimization initiated by Holand in the 1960s and 1970s, as a basic principle, and attracted a great attention in several areas as a way and methodology for learning, adaptability and optimization after publishing Goldberg's book in 1984. Various techniques for digital watermarking have been optimized based on GA in spatial and frequency domains by many of the researches. GA deemed as a search and optimization technique based on the norm of natural and genetic selection. Cover image I with M * N can have a number N of SVs which might detect diverse possibility to amendment. The technique or algorithm is necessary and needed to attain the optimum SFs which are output extreme transparency and robustness. Hence, an effective and powerful optimization algorithm is in needed for this objection. So for that, GA which is a familiar modernistic heuristic optimization algorithm is mostly used. The basic Genetic Algorithm is composed of five components namely: Random Number Generator (RNG), Fitness Evaluation (FE), Genetic Operator for Reproduction (GOR), Crossover (Cro.), and the last component is Mutation Operation (MO). Figure 1 represents the basic components of GA.

As stated in Fig. 1, the initial population is demanded to be at the starting of algorithm. The initial population is a group of number strings produced by GNA. Each series treated as an impersonation solution to the optimization problem being addressed.

To acquire or approach the limit of maximum performance of earlier developed watermarking algorithms, we have to locate their optimal parameters. One of the

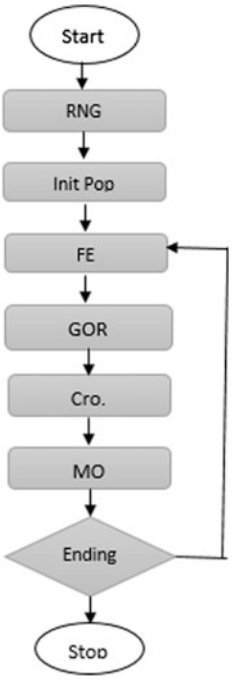

Fig. 1 Basic components of GA

common ways of solving the problem of optimal watermarking is to treat it as a problem of optimization. Based on that, Genetic algorithms (GA) can be exercised and used to solve the problem of optimization [14].

4 Survey of Watermarking Techniques Using SVD and GA

In this section, we will introduce different proposed methods and techniques related to the using of SVD- and GA-based watermarking. First, we will present watermarking techniques based on SVD, then techniques based on GA, and finally, we will concentrate on the techniques that use both terms SVD and GA. Ganic et al. [15] suggested a dual SVD scheme based on watermarking embeds *w* twice. In the first layer, *I* is segmented to tiny segments and a part of *w* is embedded in each block. In the second layer, *I* is utilized as a single partition or block to insert the entire watermark. The intent of considering two layers to insert watermark, because the first one permits elasticity in the capacity of data, the second layer provides extra robustness and resistance to different offensive. Lee et al. [16] suggested a method for image content authentication based on SVD with enhanced security by insert or embed *w* into blocks which are ordered randomly, modifying and dithering the quantized greatest singular value of image block, the proposed technique is strong and powerful against VQ attack and is secure from the attacks of histogram analysis. Calanga et al. [17] presented a scheme of watermarking based on compression SVD. They split *I* into small blocks, then applied SVD to every block. In this technique, *I* is inserted into all non-zero singular values based on the topical features of *I* so as to make a balance in distortion with embedding capacity. Mohan and Kumar [18] introduced a robust image watermarking technique for the copyright protection of multimedia. In their suggested technique, they used SVD domain and dither quantization for inserting *w* in the both matrices (U and V) acquired from SVD. They stated that in their method, the greatest SV of *I* and U matrix coefficients is adjusted to embed *w*. Mohammad et al. [19] introduced a technique of SVD-based watermarking which is an amended version of the SVD-based technique suggested by Liu and Tan at [13]. The suggested technique or algorithm is non-invertible and it is mainly used for protecting legitimate ownership. Basso et al. [20] introduced a scheme of block-based watermarking based on SVD. The watermark is inserted by means of adjusting the angularity created by right singular vector of each block of *I*.

Huang and Wu [21] suggested a technique of image watermarking using GA in DCT domain, GA was utilized to search for suitable embedding locations in between DCT coefficients of image blocks. Kumsawat et al. [6] discussed that a framework of watermarking based on GA for performance was debated, so that GA searched for parameters of watermarking which include threshold and embedding strength. Lin et al. [22] discussed a minor searching algorithm based on GA to

minimize long times of computation. Shieh et al. [23] presented a technique of watermarking optimization using GA to search optimal frequency bands for embedding watermarks. In the previous researches and presented techniques and methods, two goals for using GA, the first one is searching for an optimum parameters of watermarking (e.g., embedding strengths and threshold) [24], and the second one is to find the most appropriate embedding positions.

Veysel Aslantas presented a novel scheme of optimal watermarking based on SVD with GA, he modified SV values of I to embed w, then these amendments are optimized by employing GA to obtain the highest possible robustness without losing transparency, means without degrading the image quality. The size of I used in experiments was 256 * 256 and w with size of 32 * 32. In his suggested algorithms, GA is utilized to acquire multiple SF. Experiments outcomes show that feasibility of multiple SFs evaluated by GA and its notability over the use of a single SF. For further studies, he suggested to be executed along with the components of SVD (U and V). B. Jagdesh et al., they presented a novel scheme for optimal watermarking based on SVD and GA. This proposed technique relies on step size optimization using GA to improve the fineness of Iw and robustness of w to evaluate the effectiveness of the method, they used a cover image I with the size of 512 × 512 and w with size of 64 × 64. I is partitioned it into 8 × 8 before performing SVD on each block. They applied the embedding and extraction processes based on the suggested algorithm. They used an error matrices to test and make sure that the algorithms is normalized cross correlation NC for the robustness and peak signal-to-noise rate (PSNR) for transparency based on the following equations:

$$\text{PSNR} = 10\log_{10}\left(\frac{\sum_{i=1}^{N}\sum_{j=1}^{N}(F(i,j))^2}{\sum_{i=1}^{N}\sum_{j=1}^{N}(f(i,j)-F(i,j))^2}\right)$$

$$\text{NC} = \left(\frac{\sum_{i=1}^{N}\sum_{j=1}^{N}(w(i,j)-w_{\text{mean}})(w'(i,j)-w'_{\text{mean}}}{\sqrt{\sum_{i=1}^{N}\sum_{j=1}^{N}(w(i,j)-w_{\text{mean}})^2\sum_{i=1}^{N}\sum_{j=1}^{N}(w'(i,j)-w'_{\text{mean}})^2}}\right).$$

Then, calculate the fitness of solution based on both the transparency PSNR and robustness $fval = -(PSNR + NC)$ based on the suggested algorithm. Different types of attacks are used to test the robustness of w. The experiments results show that the quality of Iw looks good with respect to perceptibility and PSNR, and in addition to that, this technique also presents robust to the following attacks: JPEG compression, low-pass filtering, resizing, media filtering, salt and pepper noise, and column blanking and copying. Chih-china et al., presented an adaptive amended SVD-based watermarking technique through stratify statics of the image with GA.

The proposed approach used GA to optimize the strength of *w*. They used *I* as a gray-level image (size of 512 * 512) and *w* (size of 32 * 32). In their experiments, the suggested approach maintains high perceptual quality of *Iw*. For the sake of valuation, the robustness of the suggested method, *w,* was examined against five attacks: Geometrical Attack (Cropping), Noising Attack (Gaussian Noise), De-noising Attack (Median filtering), Format Compression Attack (JPEG Compression), and Image Processing Attack (Sharpening, Histogram Equalization and Tempering), [CR, GN, MF, JPEG, and (SH, HE)]. So as to show the notability of their approach, they compare it with another SVD-based watermarking techniques and algorithms. Experiments results show both of the considerable amelioration in imperceptibility and robustness against various attacks and techniques of image manipulation. Shih-Chin Lai suggested an innovative technique for image watermarking through merging SVD technique with tiny GA. Appropriate scaling factors are specified using the tiny algorithm. For the purpose of testing, he used *I* with size of 256 × 256 and *w* with size of 64 × 64. The relative parameters which are used with tiny GA as follows: 5 is the size of population, 300 is the utmost generation number, and 0.95 is the probability of crossover. Lai divided the experiments into two steps, in the first step, he evaluated the robustness of the suggested approach, *Iw* was examined versus five sorts of attacks (CR, Rotation RO, GN, Average Filtering AF, JPEG, HE and Darken DK). In the second step: Lai compared this schema with [25, 26] to check the capability of resistance to various types of attacks, Extracted watermark quality is specified by values of NC. In [26], they apply the SVD to the whole *I* and insert *w* in the diagonal matrix of the SVD transformation and the SF is set to a single constant value. In [25] the author suggested a watermarking technique based on SVD and micro-GA (μ-GA). Singular values of *I* are adjusted through considering various scaling factors to insert *w*. The μ-GA is applied to effectively search the appropriate values of scaling factors. Result shows that in shih proposed approach, the robustness performance is superior to the other similar approach. One main disadvantage for this approach proved by Khaled that it suffers from a highly probability of detection of false positive. which means that the proposed watermarking scheme might be on-effective in the term of probability of false positive detection of *I*.

Poonam et al. proposed the modern technique used to get the robustness and imperceptibility much better in watermarking. In this method, the singular value of *w* is inserted into singular value of third-level DWT approximation matrix of *I*. They used the GA to optimize the scaling factor with which the watermark is embedded to *I*. The proposed algorithm makes use of fitness function that takes two values PSNR and correlation. They used a host image [size of 512 × 512] and watermark [size of 64 × 64], they carried out watermarking based on DWT-SVD procedure through GA on ten training samples, these procedures repeated for five attacks: Geometrical Attack, Format compression, Noising Attack, De-Noising Attack, and Image Processing Attack. They observed that after applying several types of attacks, the correlation value in between the original watermarking and the extracted one is larger if the scaling factor is high. The results shown that PSNR for

the suggested algorithm is rising with the increasing value of scaling factors and their result was the best. They show that when the scaling factor increased, they got bestead performance particularly with robustness.

5 Conclusion

In this study, we have covered only the techniques of digital watermarking based on SVD and GA, we found that only a few researches have been done on the field of digital watermarking, which rely on combining SVD and GA, most of the mentioned studies in this study concentrate on some attacks, they do not cover all known attacks. Some of them concentrate on achieving higher PSNR and the other on NC. More studies need to be done in those fields to achieve more equilibrium between the two contradictory requirement perceptibility and robustness (i.e., PSNR and NC).

References

1. I.J. Cox, M.L. Miller, and J.A. Bloom, "Digital Watermarking," Morgan Kaufmann Publishers, 2002.
2. B. Jagadeesh, et al, "Image Watermarking Scheme Using Singular Value Decomposition, Quantization and Genetic Algorithm", 978-0-7695- 3960-7/10 $26.00 © 2010 IEEE.
3. Veysel Alantas, "An SVD Based Digital Image Watermarking Using Genetic Algorithm", 1-4244-0779-6/07/$20.00 ©2007 IEEE.
4. Veysel Alantas, "A singular-value decomposition-based image watermarking using genetic algorithm", 2007 Elsevier GmbH, Int. J. Electron. Commun. (AEÜ) 62 (2008) 386–394.
5. J.S. Pan, H.C. Huang, and L.C. Jain, "Intelligent Watermarking Techniques", World Scientific Publishing Company, 2004.
6. C.H. Huang, J.L. Wu, Fidelity-guaranteed robustness enhancement of blind-detection watermarking schemes, Information Sciences 179 (6) (2009) 791–808.
7. C.-C. Lai, H.-C. Huang, C.-C. Tsai, A digital watermarking scheme based on singular value decomposition and micro-genetic algorithm, International Journal of Innovative Computing, Information and Control 5 (7) (2009) 1867–1874.
8. P. Kumsawat, K. Attakitmongcol, A. Srikaew, A new approach for optimization in image watermarking by using genetic algorithm, IEEE Transactions on Signal Processing 53 (12) (2005) 4707–4719.
9. Liu R, Tan T. "An SVD-based watermarking scheme for protecting rightful ownership. IEEE Trans Multimedia 2002;4:121–8.
10. Bao P, Ma X. Image adaptive watermarking using wavelet domain singular value decomposition. IEEE Trans Circuits Systems Video Technol 2005;15:96–102.
11. R. Liu, T. Tan, An SVD-based watermarking scheme for protecting rightful ownership, IEEE Trans. Multimedia 40 (1) (2002) 121–128.
12. E. Ganic, N. Zubair, A.M. Eskicioglu, An optimal watermarking scheme based on singular value decomposition, in: Proc. IASTED Int'l Conf. on Communication, Network, and Information Security, 2003, pp. 85–90.

13. I.J. Cox, J. Kilian, F.T. Leighton, T. Shamoon, Secure spread spectrum watermarking for multimedia, IEEE Trans. Image Process. 6 (12) (1997) 1673–1687.
14. Jun Wang, Hong and Peng, "An optimal image watermarking approach based on a multi-objective genetic algorithm", Information Sciences 181 (2011) 5501–5514, Elsevier Inc., doi:10.1016/j.ins.2011.07.040.
15. E. Ganic, N. Zubair, A.M. Eskicioglu, An optimal watermarking scheme based on singular value decomposition, in: Proc. IASTED Int'l Conf. on Communication, Network, and Information Security, 2003, pp. 85–90.
16. S. Lee, D. Jang, C.D. Yoo, AN SVD-based watermarking method for image content authentication with improved security, in: Proc. ICASSP05, 2005, pp. 525–528.
17. M. Calagna, H. Guo, L.V. Mancini, S. Jajodia, A robust watermarking system based on SVD compression, in: Proc. 2006 ACM Symposium on Applied Computing, 2006, pp. 1341–1347.
18. B.C. Mohan, S.S. Kumar, A robust image watermarking scheme using singular value decomposition, J. Multimedia 3 (1) (2008) 7–15.
19. A.A. Mohammad, A. Alhaj, S. Shaltaf, An improved SVD-based watermarking scheme for protecting rightful ownership, Signal Process. 88 (9) (2008) 2158–2180.
20. A. Basso, F. Bergadano, D. Cavagnino, V. Pomponiu, A. Vernone, A novel block based watermarking scheme using the SVD transform, Algorithms 2 (2009) 46–75.
21. C.H. Huang, J.L. Wu, A watermark optimization technique based on genetic algorithms, The SPIE Electronic Imaging, San Jose, CA, 2000.
22. C.H. Lin, J.L. Wu, C.H. Huang, An Efficient Genetic Algorithm for Small Search Range Problems and its Applications, Intelligent Multimedia Processing with Soft Computer, Springer, 2005.
23. S. Shieh, H.C. Huang, F.H. Wang, J.S. Pan, Genetic watermarking based on transform domain techniques, Pattern Recognition 37 (3) (2004) 555–565.
24. P. Kumsawat, K. Attakitmongcol, A. Srikaew, A new approach for optimization in image watermarking by using genetic algorithm, IEEE Transactions on Signal Processing 53 (12) (2005) 4707–4719.
25. C.-C. Lai, H.-C. Huang, C.-C. Tsai, Image watermarking scheme using singular value decomposition and micro-genetic algorithm, in: Proc. of the Fourth International Conference on Intelligent Information Hiding and Multimedia, Signal Processing, 2008, pp. 239–242.
26. F. Harung. M. Kuter, "Multimedia watermarking techniques", Proc. IEEE 87 (7) (1999) 1079–1107.

http://www.springer.com/978-981-10-2470-2

Proceedings of the First International Conference on Computational Intelligence and Informatics
ICCII 2016
Satapathy, S.C.; Prasad, V.K.; Rani, B.P.; Udgata, S.K.; Raju, K.S. (Eds.)
2017, XIV, 724 p. 274 illus., Softcover
ISBN: 978-981-10-2470-2