International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

An Optimal Digital Image Watermarking based on SVD and Genetic Algorithm

Shreya Tayal[1], SPS Chauhan[2]

[1]School of Computing Science and Engineering, Galgotias University, Uttar Pradesh, India

[2]Assistant Professor, School of Computing Science and Engineering, Galgotias University, Uttar Pradesh, India

Abstract: ***As technology amplifies, its causatum on our everyday life becomes more retentive. Likewise, enforced in the field of Digital Image Processing. As the appetency of images, audios & videos going exalt, the afflictive techniques are practised to lapse, contradict those. Hence, to overcome from this , watermarking comes to exalt. Watermarking technique implements to abstain felonious replicate of the work by embedding the copyright image. Watermarking lodge information in the elementary image which indistinct to the human visual system. The objective of robust watermarking is to preserve the individuality of an image, audio, and video without poignant its originality. The work equipped in this paper is an attempt to replenish a survey on the latest technologies that are occupied in watermarking technique.***

Keywords: Digital image processing, watermarking, SVD, GA, watermarking robustness parameters

1. Introduction

Expeditive augmentation of computer networks & Internet, the usage of multimedia data has emanate in quick and obtainable reciprocation of digital information.

Subsequently, such applications have also embossed concern about copyright & unauthorized alteration & dissemination of digital data. To actualize these issues, watermarking technology endorsed such problems.

Watermarking is the technique in which interpolation [2] of data into a multimedia element such as an image, audio & video file. The encapsulated data can later be extricated from the multimedia for analyzing the media owner.

Watermarking Algorithm for any image includes cover image, a watermark anatomy (structure), an embedding algorithm and also extraction algorithm. Distinct, approaches have been recommended for multimedia protection. Among those recommended methods, much engrossment has centralized on digital images [2,3,4,5]. As per the domain in which watermark interpolated are partite into two broad categories: Spatial domain & frequency domains. The inlay of watermark into spatial domain component of the original image is straight method. Advantages of spatial domain are low complexity & effortless implementation.

Despite, spatial domain watermarking algorithms are delicate to image processing operations. The frequency domain techniques inlay watermark by switching the magnitude of coefficients in a transform domain such as Discrete Fourier Transformation (DFT), Discrete Cosine Transformation (DCT), and Discrete Wavelet Transformation (DWT)[6,7,8]. The Computational costs of frequency domain of frequency domain methods are higher than spatial domain methods. One more technique is there i.e. Singular Value Decomposition (SVD) [15]. Singular value decomposition is a mathematical process which deals in the extraction of algebraic features from an image. The idea of implementing SVD approaches is to employ the SVD to the emtire cover image, small blocks of it and then revise the singular values to embed watermark. The performance of the watermarking process eminently depends on picking an appropriate scaling factor. “Ganic et al.[1] found that the scaling factor is set to be constant in some SVD- based studies.”

“Cox et al. [2] argued that considering a single & constant scaling factor may not be applicable in some cases, &they suggest users can use multiple scaling factors instead of one.”

The appropriate scaling factors are decided by Genetics Algorithm.

2. Singular Value Decompostion

The Concept of Singular Value Decomposition (SVD) was entrenched for real square matrices in the 1870s by Beltrami [22] and Jordan [23] for complex matrices ny Autonne in 1902[24] and has been prolonged to rectangular matrices inlay in image processing applications, inclusive image compression [25] ,image hiding [26], noise debasement.[27]

Matrix A is a decomposition of the form $A = U\,S\,V^{T}$

The SVD has a variety of applications in scientific computing, signal processing, automatic control, and many other areas.

SVD Based Watermarking- From the context of image processing, an image can be contemplated as a matrix along with non negative scalar entries. The SVD of an Image A with size m*m is given by $I = U\,S\,V^{n}$. U & V are orthogonal matrices and S is a diagonal matrix portrayed in decreasing order. This process is called **Singular Value Decompostion.**

SVD does not affect the visual apprehension of the cover image, which impels the watermarking embedding through minor alteration of SVs in the segmented images.

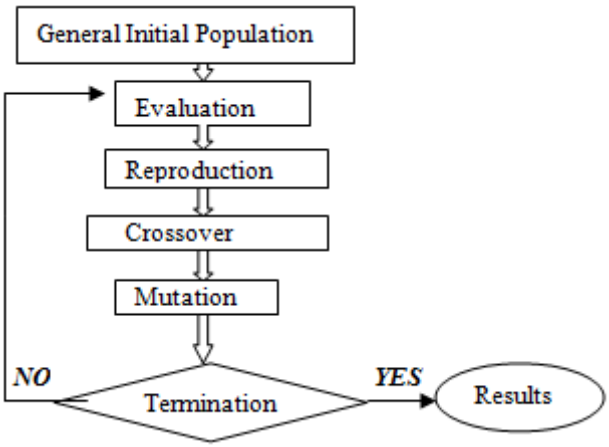
According to the description in Liu and Tan's method [9], the watermark embedding and extraction procedures can be described as follows:

3. Embedding Process

1. SVD is applied to host image I:
$I = U.S.V^n$
2. A Watermark A is multiplied by a scaling factor c and added to the matrix S:
$D = S + c.A$
3. SVD is further applied on new matrix D:
$D = U_a.S_a.V^n{}_a$
4. The Watermarked image will be computed as:
$I_a = U.S_a.V^n$

EXTRACTION PROCESS-
Embedding and extraction is inversely proportional to each other.
1. SVD is performed on the watermarked image:
$I^*_a = U^*.S^*_a.V^*$
2. The matrix D^* is computed as:
$D^* = U_a.S^*_a.V_a{}^n$
3. Watermark is extracted as:
$A^* = (D^* - S)/a = (U_a.S^*_a.V_a{}^n - S)/a$

4. Genetics Algorithm



Genetics Algorithm is the most prominent algorithm extensively used for optimization developed by Holland[21] in the 1960s and 1970s as a basic principle, and conclusively popularized by Goldberg . Chromosomes epitomize set of genes, codes independent variable. Every chromosome epitomizes an explication of the given problem.[14]

5. General Initial Population

Initial population is referred by the set of chromosomes which indicates a solution of a problem. This population can be propagated through some problem-specific heuristic. It is considerable that the chromosome is proclaimed as a string of genes, which can be illustrated, based on the application, by the integers or real numbers, binary alphabet[21].

Evaluation- This subsists of classifying the chromosomes from best to worst as reported by their fitness values, in contemplation to reflect their significance in forming the next generation. The value is enumerated using an objective function.

Reproduction- This permits a chromosome the possibility to generate the next generation. The probability that a chromosome will be opted on the basis of its fitness value. The operator plays a significant role in the search of a better solution and maintain assortment in the population. The basic methods of reproduction are:-
Roulette wheel selection
Tournament Selection

Crossover- Crossover is a genetic operator used to distinguish the programming of a chromosome from proceeding generation. It is corresponding to reproduction and biological crossover, upon which genetic algorithms are based. It requires combining the parents to generate off springs.

Mutation- Used to maintain genetic diversity**,** from one generation of a population of genetic algorithm chromosomes to the next. This applies to some offspring chromosomes.

6. Related Work

In this section, some SVD-based watermarking schemes proposed in the past years are briefly reviewed. Ganic et al.[1] presented a double watermarking scheme based on SVD that embeds the watermark twice. In the first layer the cover image is divided into smaller blocks and a piece of the watermark is embedded in each block. In the second layer, the cover image is used as a single block to embed the whole watermark. The purpose of considering two layers to embed watermark is that layer one allows flexibility in data capacity, and layer two provides additional robustness to attacks.

Lee et al. [19] proposed an SVD-based image content authentication method with improved security is proposed. By embedding watermark into randomly ordered block, adjusting and dithering the quantized largest singular value of an image block, the proposed method is robust against VQ attack and is safe from histogram analysis attack. Calagna et al.[20] introduced an image watermarking scheme based on the SVD compression. They divided the cover image into blocks and applied the SVD to each block. The watermark is embedded in all the non-zero singular values according to the local features of the cover image so as to balance embedding capacity with distortion. Mohan and Kumar [16] presented a robust image watermarking scheme for multimedia copyright protection. In their work, the proposed method uses SVD domain and dither quantization for embedding the watermark in both *D* and *U* matrices obtained from SVD. In the proposed method, the largest singular values of the cover image and the coefficients of the *U* matrix a remodified to embed the watermark. Mohammad et al. [29] presented an SVD-based watermarking technique. This technique is an improved version of the SVD-based technique proposed by

Liu and Tan [9].The proposed techniques non-invertible and its main applications in protecting rightful ownership. Basso et al. [30] proposed a block-based watermarking scheme based on SVD. The watermark is inserted by modifying the angles formed by the right singular vectors of each block of the original image.

7. Requirements of Watermarking

Transparency or Fidelity
Transparency expatiates that the quality of the image is not conciliated after the watermark is implied on it. Cox et al. (2002) define transparency or fidelity as "perceptual similarity between the original and the watermarked versions of the cover work". It makes sure that there should not be any visible distortions in the image after watermarking is implied because it degrades the commercial value of image.

Robustness
Cox et al. (2002) defines robustness as "ability to detect the watermark after common signal processing operations". A watermarked image can be removed by simple image processing like brightness or contrast enhancement and compression, filtering.

Criteria to test robustness of watermarking algorithm, there are some attacks-
1- Cryptographic Attacks
2- Protocol Attacks
3- Remote Attacks
4- Attacks which remove watermark completely.

Capacity
"The number of bits a watermark encodes within a unit of time or work" defines the capacity or data payload Cox et al. (2002). This property handles the amount of data that should embed as a watermark for successful detection during extraction. Watermark should contain uniqueness.

Watermarking Attacks

Removal Attacks: Removal attacks aim at the entire eradication of the watermark information from the watermarked data without using the key. No processing can recover the watermark from the attacked data. This category consists non voice, quantization (compression), remodeled and collusion attacks, all these methods will be very close to their goal of complete watermark removal, but they although destroy the watermark information notably[13].

Geometrical Attacks: In comparison with removal attacks, the geometrical attacks do not absolute remove the embedded watermark itself, but contemplate to deteriorate the watermarked data prior to. The detector could recover the embedded watermark information when perfect synchronization is regained. In spite of, the required synchronization process might be too great to be practical.

Cryptographic Attacks: Intention of cracking the security methods in watermarking schemes and thus searching a way to eradicate the embedded watermark information or to embed misleading watermarks.

Protocol Attacks: Protocol attack aim at attacking the whole concept of the watermarking application. A type of protocol attack is based on the concept of invertible watermarking. The idea behind the revulsion is that the attacker subtracts his own watermark from the watermarked data and pretense to be the keeper of the watermarked data.

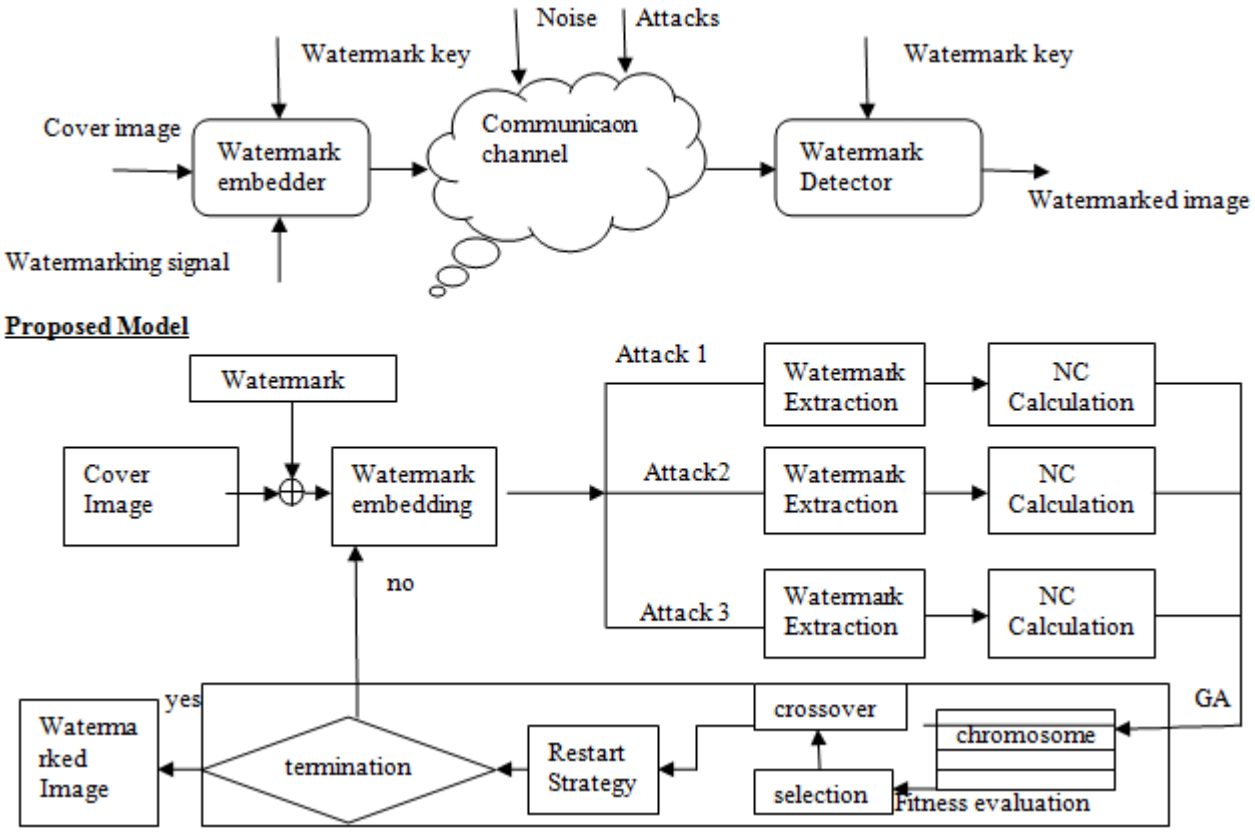
This is responsible for the ambiguity with respect to the true ownership of the data. Another protocol attack is a copy attack, In this case, the intention is not to destroy the watermark, impair its detection, but to estimate a watermark from the watermarked data, and copy it to the some other data called target data. The copy attack is applicative when a valid watermark in the target data can be produced with neither algorithmic knowledge of the watermarking technology nor knowledge of the watermarking key.

Legal Attacks: Legal Attacks are the potentiality of an attacker to expulsion on the watermarking scheme in the courts. These attacks lean on existing and future legislation on copyright laws and digital information ownership, the reliability of the owner and of the attacker, [13]the financial background of the owner versus that of the attacker, the expert witness, and the competence of the lawyers. A robust watermarking scheme has to decrease the attackers strength to cast doubt on technical evidences presented in court.

Basic Attacks: Basic Attacks take advantages of the drawback in the design of embedding techniques. Simple spread spectrum techniques, for example, are able to endure amplitude distortion and noise addition but are vulnerable to timing errors. Synchronization of the chip signal is required in order for the technique to work so reconcile the synchronization can cause the embedded data to be lost. It is viable to alter the length of a piece of audio without changing the pitch and this also be an effective attack on audio files.

8. General Watermarking System

A Digital Watermarking Scheme, in general is a collection of several algorithms that permit us to embed some information into some host signal in such a way that these watermarks can later be extracted and detected, even if the cover objects are corrupted by a small amount of acceptable noise[4]. A watermarking scheme consists of three major components. A watermark generator produces aspired watermarks for a particular application, which are optionally based on some keys. An embedder embeds the watermark into the cover object, sometimes dependent on an embedding keys. A detector is responsible for detecting the existence of some predefined watermark in a cover object, and sometimes it is desirable to extract an message from the watermarked cover object.



The proposed watermarking scheme.

In this section, the powerful numerical analysis SVD transformation and the hypothesis of SVD-based watermarking are first popularized. The proposed watermarking scheme which utilizes the GA to actuate proper multiple SVs and to embed the watermark is then described. The block diagram of the proposed approach is described.

9. Conclusion

In this paper, an image watermarking technique is based on SVD and GA has been proposed. The singular values of the cover image are converted to embed the watermark. The GA endeavors an arranged way to deliberate the improvement of the scaling factors that are used to control the strength of the embedded watermark. With the proposed scheme, the embedded watermark can successfully survive after attacked by image processing operations. Simulation results show that the proposed scheme outperforms the other similar works. Further work of extending the proposed approach with human visual systems.

References

[1] 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.
[2] 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.
[3] A.M. Ahmed, D.D. Day, Applications of the naturalness preserving transform to image watermarking and data hiding, Digital Signal Process. 14 (2004) 531–549.
[4] F. Hartung, M. Kutter, Multimedia watermarking techniques, Proc. IEEE 87 (7) (1999) 1079–1107
[5] T.V. Nguyen, J.C. Patra, A simple ICA-based digital image watermarking scheme, Digital Signal Process. 18 (2008) 762–776.
[6] M. Barni, F. Bartolini, A. De Rosa, A. Piva, Optimal decoding and detection of multiplicative watermarks, IEEE Trans. Signal Process. 51 (4) (2003) 1118–1123.
[7] A. Briassouli, M.G. Strintzis, Locally optimum nonlinearities for DCT watermark detection, IEEE Trans. Image Process. 13 (2) (2004) 1604–1617
[8] A. Nikolaidis, I. Pitas, Asymptotically optimal detection for additive watermarking in the DCT and DWT domains, IEEE Trans. Image Process. 12 (5) (2003) 563–571.
[9] R. Liu, T. Tan, An SVD-based watermarking scheme for protecting rightful ownership, IEEE Trans. Multimedia 40 (1)(2002) 121–128
[10] M. Köppen, K. Franke, R. Vicente-Garcia, GAs for image processing applications, IEEE Computat. Intell. Mag. 2(2006) 17–26.
[11] F. Hartung, M. Kutter, Multimedia watermarking techniques, Proc. IEEE 87 (7) (1999) 1079–1107.
[12] I. Podilchuk, E.J. Delp, Digital watermarking: algorithms and applications, IEEE Signal Process. Mag. 18 (4) (2001) 33–46.
[13] S. Voloshynovskiy, S. Pereira, T. Pun, J.J. Eggers, J.K. Su, Attacks on digital watermarks: classification, estimation based attacks, and benchmarks, IEEE Commun. Mag. 39 (8) (2001) 118–126.

[14] M. Gen, R. Cheng, Genetic Algorithms and Engineering Design, Wiley, New York, NY, 1997
[15] E. Ganic and A. M. Eskicioglu, "Robust embedding of visual watermarks using discrete wavelet transform and singular value decomposition," *J. Electron. Imaging* **14**, 043004 (2005).
[16] B. Mohan and S. Kumar, "A robust image watermarking scheme using singular value decomposition," *Multimed. Tools Appl*. **3**, 7–15 (2008).
[17] X. P. Zhang and K. Li, "Comments on "An SVD−based watermarking scheme for protecting rightful ownership"," *IEEE T. Multimedia* **7**, 593–594 (2005).
[18] K. Loukhaoukha and J.−Y. Chouinard, "On the security of ownership watermarking of digital images based on SVD de− Composition," *J. Electron. Imaging* **19**, 013007 (2010).
[19] 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.
[20] 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.
[21] Holland, J.H.: Adaptation in Natural and Artificial Systems. University of Michigan Press (1975)
[22] E. Beltrami, Sulle funzioni bilineari, *Proc. of Giornale di Mathematiche*, vol. 11, pp. 98-106, 1873.
[23] C. Jordan, Mmoire sur les formes trilinaires, *Journal de Mathmatiques Pures et Appliques*, vol. 19, pp. 35-54, 1874.
[24] L. Autonne, Sur les groupes linaires, rels et orthogonaux, *Bulletin de la socit mathmatique de France*, pp. 121-143, 1902.
[25] C. Eckart and G. Young, A principal axis transformation for non-hermitian matrices, *Bulletin of American Mathematical Society*, vol. 45, no. 2, pp. 118-121, 1939.
[26] P. Waldemar and T. Ramstad, Image compression using singular value decomposition with bit allocation and scalar quantization, *Proc. of Nordic Signal Processing Symposium*, pp. 83-86, 1996.
[27] K. Chung, C. Shen, and L. Chang, A novel SVD and VQ-based image hiding scheme, *Pattern Recognition Letters*, vol. 22, no. 9, pp. 1051-1058, 2001.
[28] K. Konstantinides, B. Natarajan, and G. Yovanof, Noise estimation and _ltering using block-based singular value decomposition, *IEEE Trans. Image Processing*, vol. 6, no. 3, pp. 479-483, 1997.
[29] A.A. Mohammad, A. Alhaj, S. Shaltaf, An improved SVD-based watermarking scheme for protecting rightful ownership, Signal Process. 88 (9) (2008) 2158–2180.
[30] A. Basso, F. Bergadano, D. Cavagnino, V. Pomponiu, A. Vernone, A novel blockbased watermarking scheme using the SVD transform, Algorithms 2 (2009) 46–75.