Intelligence-Based Adaptive Digital Watermarking For Images In Wavelet Transform Domain

Oloyede, A.
Department of Computer Science
Caleb University
Imota, Lagos State

Adegbenjo, A.
Department of Computer Science & Information Technology
Babcock University
Ilishan-Remo, Ogun State
Email: ayglo55@yahoo.com
Phone Number: +2348033937115

ABSTRACT

Advances in technologies facilitate the end users to carry out unauthorized manipulation and duplication of multimedia data with less effort. Because of these advancements, the two most commonly encountered problems are (1) copyright protection and (2) unauthorized manipulation of multimedia data. Thus a scheme is required to protect multimedia data from those two above said problems. Digital Watermarking is considered as one of the security mechanisms to protect copyrights of multimedia data. The literature review reveals that the calculation of scaling and embedding parameters are not completely automated. In order to automate the procedure of calculating scaling and embedding parameters the computational intelligence need to be incorporated in the watermarking algorithm. Moreover the quality of the watermarked images could also be preserved by combining computational intelligence concepts. Thus watermarking schemes utilizing computational intelligence concepts could be called as intelligence based watermarking schemes and it is presented in this paper in detail.

Keywords: Intelligent-based, Adaptive, Digital, Watermarking, imaging, wavelets transform

CISDI Journal Reference Format
Oloyede, A. & Adegbenjo, A (2016): Intelligence-Based Adaptive Digital Watermarking For Images In Wavelet Transform Domain. Computing, Information Systems, Development Informatics & Allied Research Journal. Vol 7 No 4. Pp 79-86
Available online at www.cisdijournal.net

1. INTRODUCTION

Information sharing becomes very easy in Internet that permits the unauthorized manipulations of multimedia data with reduced efforts. In such circumstances protecting copyrights of multimedia data become very essential as cost involved in content development is very high. In Internet, huge volume of data available in the form of images, thus it is required to secure images in particular. Digital watermarking is considered as a most popular security mechanism to protect copyrights of digital images. In general digital watermarking techniques are carried out by inserting a piece of digital data in to a cover data. In order to keep the watermark inside a cover image, its content needs to be altered without affecting its quality (Al-Qaheri, 2010).

The amount of alteration of cover images decides the quality of cover images. Digital image watermarking techniques are broadly classified into spatial domain and frequency domain techniques. Researcher have carried out watermarking schemes in both working domains, but in order to make watermarking schemes robust it has to be carried out in frequency domain. In this paper, watermarking schemes carried out in wavelet transform domain combined with computational intelligence are presented. In the subsequent sections, the basics of digital watermarking, watermarking in transform domain, computational intelligence based watermarking schemes and conclusion are discussed in detail.

1.1 Basics of Digital Watermarking

Digital Watermarking is defined as a process of inserting a piece of digital data called watermark into digital images that are to be protected. The watermark to be inserted can be of logo, text data, numbers or any other type of images. The cover data could be of digital images, digital video sequences and digital audio signal. The inserted watermark should be extractable in future for verification of it to the intended purposes. One of the important properties of digital watermarking is its robustness against various attacks. Robustness is defined as the existence of the watermark even after various attacks as discussed in Anderson (2014).

1.2 Working Principle of Digital Watermarking

The general image watermarking system consists of a watermark, embedding algorithm and extraction algorithm. The embedding algorithm takes cover image and watermark as input and produce watermarked image as output. Similarly the watermark extraction algorithm takes watermarked image as input and extract watermark from it. Based on the requirements of original images the watermarking schemes could be classified into non-blind watermarking schemes or blind watermarking schemes. In this paper the non–blind adaptive watermarking schemes using wavelet transform techniques combined with computational intelligence are presented.

1.3 Requirements and Applications

In order to make invisible watermarking to be more effective, the inserted watermark should be visually imperceptible, reliable, unambiguous and resistant to common attacks. The requirements robustness and imperceptibility are conflict to each other, thus some equilibrium need to be achieved by modulating appropriate frequency components.

- **Imperceptible:** The watermark inserted should not introduce any perceptible artifacts into the original image and not degrade the perceived quality of the image.
- **Robustness:** The inserted watermark should still present in the watermarked image after common image processing attacks such as linear or non-linear filtering, image enhancements, noise addition, geometric distortion, resizing, and image compression.
- **Undeletable:** The watermark must be difficult or even impossible to remove by a hacker, at least without obviously degrading the original signal.
- **Unambiguous:** Retrieval of the watermark should unambiguously identify the owner, and the accuracy of identification should degrade gracefully in the face of attack.

Digital watermarking can be used in a wide variety of applications. The performance of a given watermarking system can be evaluated on the basis of application for which it is designed. The some of the most common applications could be found in Aslantas, et al (2013)'s work. which include,

- **Owner's Identification:** The inserted information can prove ownership in court when dispute arise.
- **Transaction Tracking:** To trace the source of illegal copies, the owner can embed different watermarks in the copies of the data that are supplied to different customers. Transaction tracking is more often called fingerprinting.
- **Copy Protection:** The information stored in a watermark can directly control digital recording devices for copy protection purposes.
- **Broadcast Monitoring:** In order to protect a commercial advertisement, digital watermarking is an obvious method of coding identification information in each video or sound clip prior to broadcast for active monitoring system whether advertisements are broadcasted as contracted. As given in Aslantas, et al (2015), a broadcast surveillance system can check all broadcast channels and charge the TV stations according to their findings.
- **Data Authentication:** Inserting authentication mark to protect content of digital data. The authentication marks designed to become invalid after even the slightest modification of a cover data are called fragile watermarks. If a cover data containing an authentication mark is modified, then the authentication mark is also modified along with it which reveals how the cover data has been tampered with, as given by Aslantas, (2015). The digital watermarking scheme could also be used for image indexing, information retrieval and in medical applications

1.4 Classifications of Digital Watermarking Schemes

The digital watermarking schemes can be broadly categorized based on human perception and working domain and is presented below.

- **Working Domain:** Watermark could be inserted by modifying intensity values of pixels or it could be inserted by changing the frequency components. The pixel domain is also called spatial domain and hence called spatial domain watermarking and later is called frequency domain watermarking.
- **Human Perception:** The watermark could be inserted either perceptibly or imperceptibly, therefore watermarking schemes could be classified as visible and invisible watermarking schemes. Both visible and invisible watermarking schemes could be implemented either through adaptive approaches or through non-adaptive approaches.

2. COMPUTATIONAL INTELLIGENCE AND WATERMARKING SCHEMES

In Engineering, Science and medical fields the success rate of problem solving techniques has been increased by incorporating intelligence in the systems to mimic like a natural biological intelligence and hence the system could be called as computational intelligent systems. Computational intelligence is an alternate method for solving many complex real world problems. In recent days it has established itself as a mathematical tool for solving many complex problems. Most of the real world problems could not be solved using traditional approaches, in those problems computational intelligence comes into picture and help us to solve. The components of computational intelligence include artificial neural networks, evolutionary computation, swarm intelligence, artificial immune systems and fuzzy systems. In the subsequent sections the basics of each component of computational intelligence is presented in details (Engelbrecht, 2010).

2.1 Particle Swarm Optimization Technique

Particle swarm optimization (PSO) is a stochastic optimization approach, modeled on the social behaviour of bird flocks. PSO is a population-based search procedure where the individuals, referred to as particles, are grouped into a swarm. Each particle in the swarm represents a candidate solution to the optimization problem. A particle therefore makes use of the best position encountered by itself and the best position of its neighbours to position itself toward an optimum solution. The effect is that particles "fly" toward an optimum, while still searching a wide area around the current best solution. The performance of each particle is measured according to a predefined fitness function which is related to the problem being solved. Applications of PSO include function approximation, clustering, optimization of mechanical structures, and solving systems of equations.

In general in social networks of PSO, each particle is moved by two elastic forces, one force move the particle to the fittest location and it is updated in each iteration. For particle *i*, its velocity vector v_i is updated with some magnitude and other force make the particle to move to the best location with some magnitude. In PSO the velocity and position are represented as a vector as per formula shown in Equation 1 which is explained in Engelbrecht (2007)'s work.

$$v_i(t+1) = wv_i(\mathrm{t}) + \mathrm{c}_1 r_1(y_i(t) - x_i(t)) + \mathrm{c}_2 r_2(y_g(\mathrm{t}) - \mathrm{x}_i(\mathrm{t})) \qquad (1)$$

x_i, implies the current position of the particle, y_i denote the personal best position and y_g denote the global best position found by particle *i*. The parameter *w* controls the influence of the previous velocity vector, once the velocities of all particles have been updated, the particles move with their new velocity to their new positions according to the formula given in Equation 2.

$$\mathrm{xi(t+1) = xi(t) + vi(t)} \qquad (2)$$

After all particles have been moved to their new position, the function is evaluated in new positions and the corresponding personal best positions and the global best position are updated. Typical termination criteria for PSO algorithms have been executed until a maximum number of iterations it undergoes or the global best position has not been changed for a certain number of iterations, or a function value has been found which is better than a required threshold value. Janson et al (2008), listed advantages of using Particle Swarm Optimization technique in their work and listed as follows.

2.2 Review of Related Works

In this work, a novel watermarking scheme that supports authentication and transaction tracking functionalities is proposed by Ketcham, et al (2014). The principle of finite state machine is used for inserting watermark in his scheme. The proposed watermarking scheme could be classified as blind and asymmetric. In the blind watermarking scheme the original image is not required for watermark extraction. Similarly, two different key could be used for watermark embedding and watermark extraction. The algorithm is implemented and tested for its visual quality, compression overhead, execution time overhead and payload capacity. It is found that the algorithm has high visual quality, high payload capacity, low compression overhead and low execution time overhead.

The proposed watermarking scheme uses several arithmetic and swapping operations which, increases the difficulty of the attackers in estimating the operations imposed on the coefficients for embedding the watermark bit. The three operations, addition, subtraction and swapping provide the necessary confusion without adjusting the coefficients to the extent that perceptual distortion occurs.

The proposed a watermarking scheme could be used for both authentication and transaction tracking using the concept of state tables and state transition. As a single-pass algorithm, it is fast and is also able to achieve high visual quality in terms of PSNR. Furthermore, the addition of watermark has only small effect on the compression ratio. In terms of security, the algorithm allows the extraction of the messages with a different extraction key than the embedding key and it employs multiple modification actions to carry out the watermarking.

Intelligent Audio Watermarking Using Genetic Algorithm in DWT Domain . In this work, Kim, (2014) proposed an innovative watermarking scheme for audio signal based on genetic algorithms (GA) in discrete wavelet transforms. It is robust against watermarking attacks, which are commonly employed in literature. In this algorithm, GA is employed for the optimal localization and intensity of watermark.

3. METHODOLOGY

The watermark detection process can be performed without using the original audio signal, and could be classified as blind watermarking algorithm. The experimental results demonstrate that watermark is inaudible and robust to many digital signal processing, such as cropping, low pass filter, additive noise. The diagrammatic representation of watermarking process is shown in Figure 3.1 .

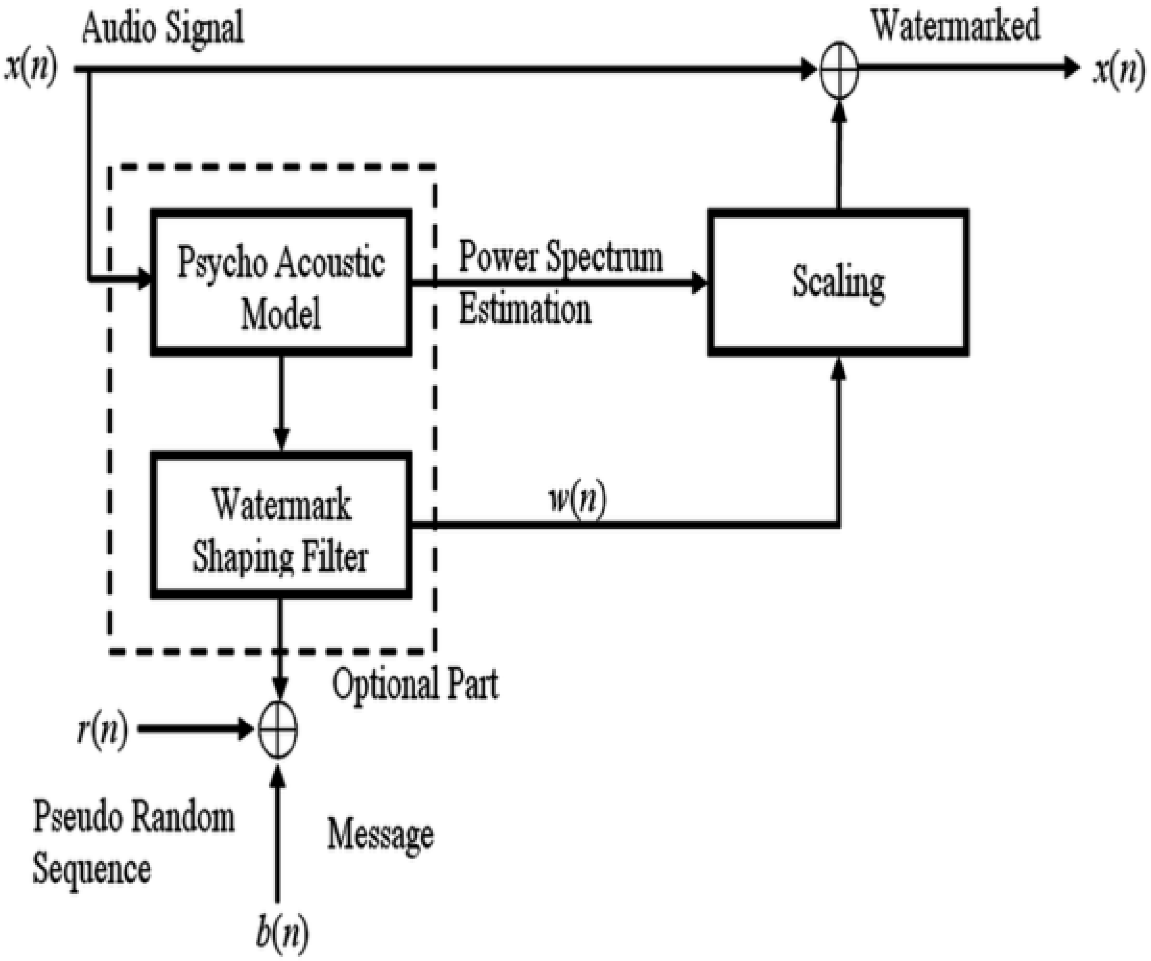

Figure 3.1. Watermark Embedding Model

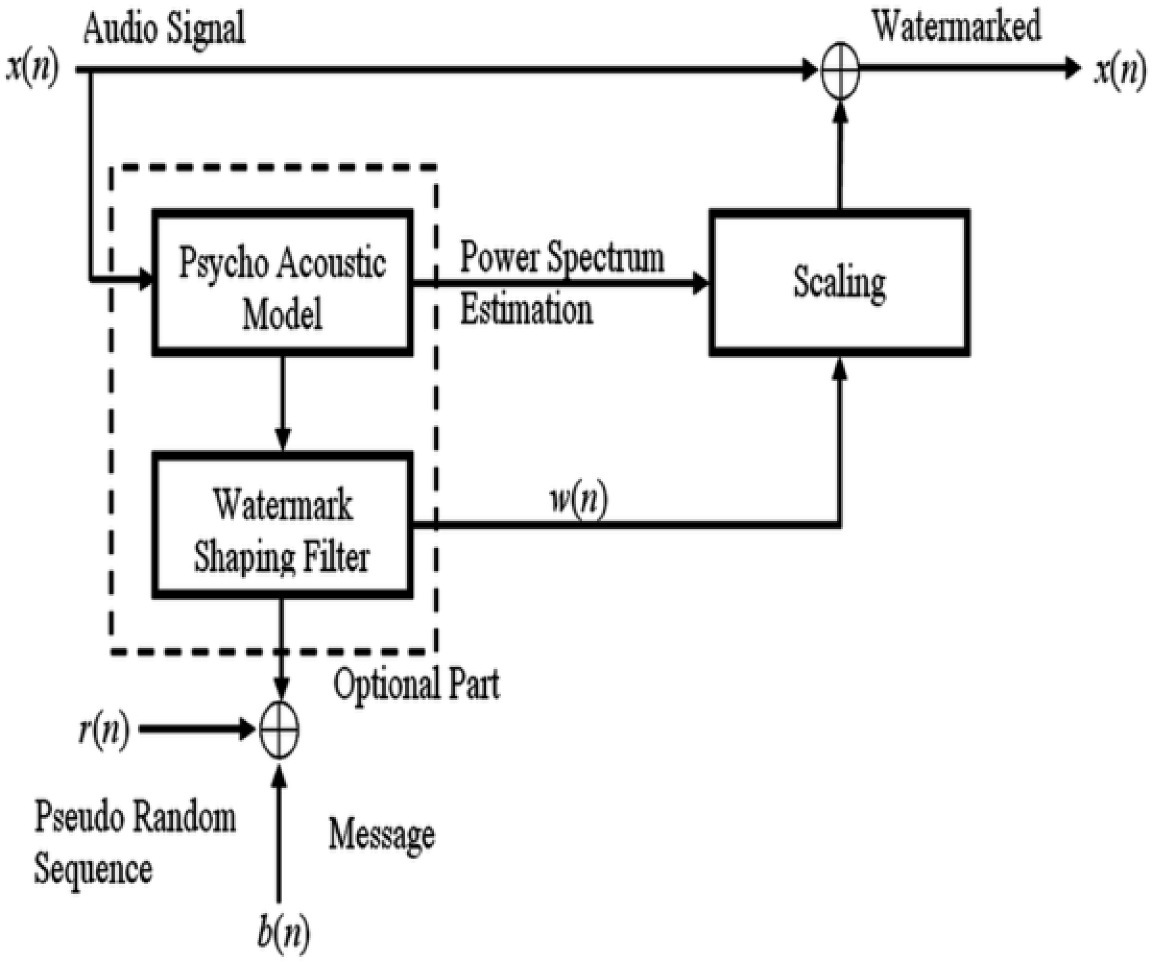

Figure 3.2. Watermark embedding model (Contd)

The reproduction operator performs a natural selection function known as “seeded selection”. Individual strings are copied from one set (representing a generation of solutions) to the next according to their fitness values, the higher the fitness value, the greater the probability of a string being selected for the next generation. The crossover operator chooses pairs of strings at random and produces new pairs. The simplest crossover operation is to cut the original “parent” strings at a randomly selected point and exchange their tails. The number of crossover operations is governed by a crossover rate (CR). The mutation operator randomly mutates or reverses the values of bits in a string. The number of mutation operations is determined by a mutation rate (MR). A phase of the algorithm consists of applying the evaluation, reproduction, crossover and mutation operations. A new generation of solutions is produced with each phase of the algorithm. The watermark embedding model is shown in Figure 3.2.

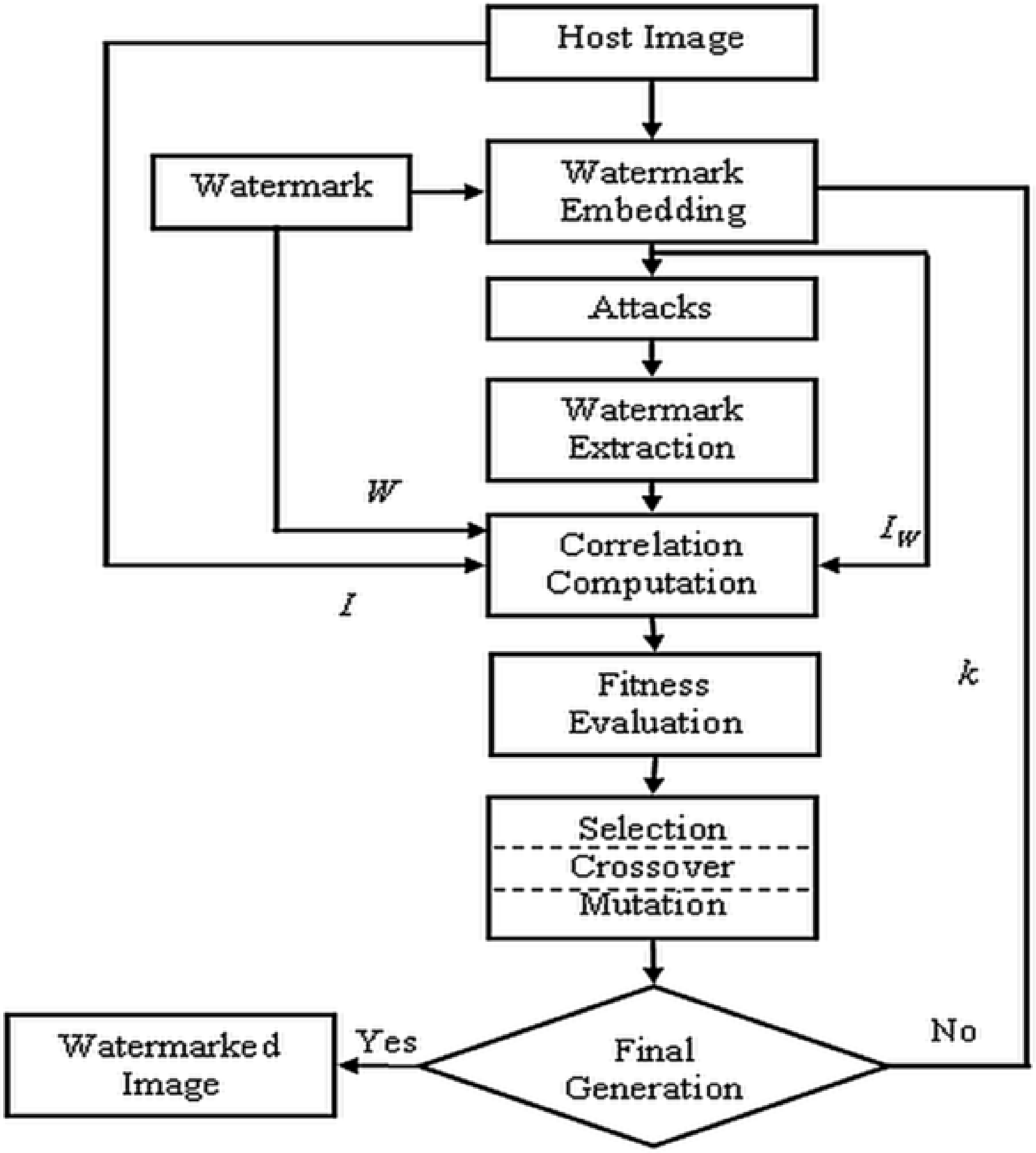

Figure 3.3: Watermark embedding process

4. DISCUSSION OF RESULTS

Experimental results show the feasibility of multiple SFs estimated by GA and its superiority over the use of a single SF. The watermarked imag and original images are shown in Figure 8. Further research can be carried out with the U and V components of the SVD. The developed system can also be applied to watermarking in DWT, DFT, DCT and the spatial domains, by changing the SVD embedding algorithm into the other domain embedding algorithms. Due to the flexibility of the developed system, the attacking modules used in this work can easily be replaced with the other attacking schemes.

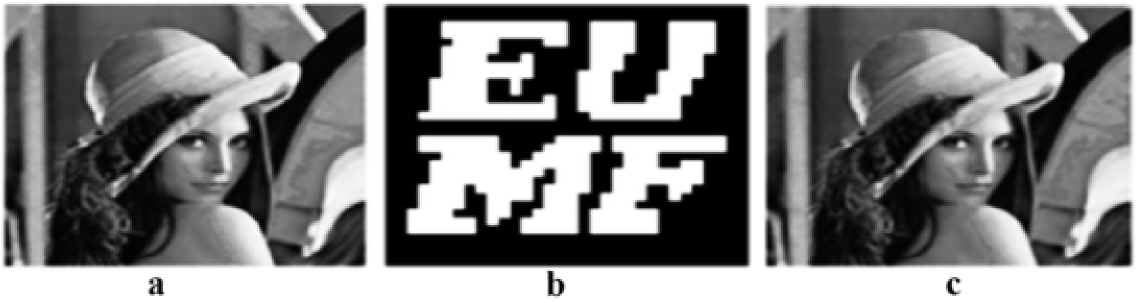

Figure 4.1 (a) Original image (b) watermark (c) watermarked image

The natural immune system (NIS) has an amazing pattern matching ability, used to distinguish between foreign cells entering the body (referred to as *non-self*, or *antigen*) and the cells belonging to the body (referred to as *self*). As the NIS encounters antige the adaptive nature of the NIS is exhibited, with the NIS memorizing the structure of this antigen for faster future response the antigen. This artificial immune system could also be used in digital watermarking schemes.

5. CONCLUSION

Digital Watermarking is considered as most important method to protect copyrights of digital images. As per the survey many existing watermarking schemes uses constant scaling factor which may destroy the quality of underlying cover image data. Moreover, in adaptive watermarking schemes cited in literature demonstrates that the automatism in inserting watermark is not complete and it implies that the dependency of user is required. Thus it is required to calculate scaling and embedding parameter using the content of cover image to make watermarking useful to the intended purpose. In order to calculate scaling and embedding factors adaptively it is required to incorporate computational intelligence such as neural networks, fuzzy logic, and optimization techniques and so on. It is observed from the literature review that the adaptive digital watermarking using computational intelligence is still in infant stage. Some of the works using intelligence concepts are presented elaborately in this paper. In future the calculation of parameters from the content of the cover image could be carried out by incorporating intelligence more efficiently using hybrid approaches. In addition intelligence based watermarking could be carried for protecting video sequences also.

REFERENCES

1. Al-Qaheri, H., Mustafi, A., & Banerjee, S. (2010). Digital watermarking using ant colony optimization in fractional Fourier domain. Journal of Information Hiding and Multimedia Signal Processing, 1(3), 179–189.
2. Anderson, R. J., & Petitcolas, F. A. (2014). On the limits of steganography. IEEE Journal on Selected Areas in Communications , 16(4), 474–481. doi:10.1109/49.668971
3. Aslantas, V. (2013). A singular-value decomposition-based image watermarking using genetic algorithm. AEÜ. International Journal of Electronics and Communications , 62(5), 386–394. doi:10.1016/j.aeue.2007.02.010
4. Aslantas, V., Dogan, A. L., & Ozturk, S. (2015). DWT-SVD based image watermarking using particle swarm optimizer. In *Multimedia and Expo, 2008 IEEE International Conference on*. IEEE. 10.1109/ICME.2008.4607416
5. Engelbrecht, A. P. (2010). Computational intelligence: an introduction . John Wiley & Sons. doi:10.1002/9780470512517
6. Hartung, F., & Kutter, M. (2016). Multimedia watermarking techniques. Proceedings of the IEEE , 87(7), 1079–1107. doi:10.1109/5.771066
7. Ho A. T. Shen J. Tan S. H. Kot A. C. (2012). Digital image-in-image watermarking for copyright protection of satellite images using the fast Hadamard transform.Proc. IEEE International Symposium on Geoscience and Remote Sensing. 10.1109/IGARSS.2002.1027166
8. Hsu, C. T., & Wu, J. L. (2008). Hidden digital watermarks in images. IEEE Transactions on Image Processing , 8(1), 58–68. doi:10.1109/83.736686
9. Ketcham, M., & Ganokratanaa, T. (2014). The Evolutionary Computation Video Watermarking Using Quick Response Code Based on Discrete Multiwavelet Transformation. In Recent Advances in Information and Communication Technology (pp. 113-123). Springer International Publishing. doi:10.1007/978-3-319-06538-0_12
10. Ketcham, M., & Vongpradhip, S. (2011). Intelligent audio watermarking using genetic algorithm in DWT domain. International Journal Of Intelligent Technology , 2(2), 135–140.
11. Kim, Y. S., Kwon, O. H., & Park, R. H. (2014). Wavelet based watermarking method for digital images using the human visual system. Electronics Letters , 35(6), 466–468. doi:10.1049/el:19990327
12. Kutter M. Bhattacharjee S. K. Ebrahimi T. (2008). Towards second generation watermarking schemes.Proc. International Conference on Image Processing.
13. Lande, P. U., Talbar, S. N., & Shinde, G. N. (2010). A Fuzzy logic approach to encrypt Watermarking for still Images in Wavelet domain on FPGA. *International Journal of Signal Processing*. Image Processing and Pattern Recognition, 3(2), 1–9.
14. Mishra, A., & Goel, A. (2015). A Novel HVS Based Gray Scale Image Watermarking Scheme Using Fast Fuzzy-ELM Hybrid Architecture. In *Proceedings of ELM-2014*. Springer International Publishing. 10.1007/978-3-319-14066-7_15
15. Naheed, T., Usman, I., Khan, T. M., Dar, A. H., & Shafique, M. F. (2014). Intelligent reversible watermarking technique in medical images using GA and PSO. Optik-International Journal for Light and Electron Optics , 125(11), 2515–2525. doi:10.1016/j.ijleo.2013.10.124