IJRESM

International Journal of Research in Engineering, Science and Management
Volume-2, Issue-2, February-2019
www.ijresm.com | ISSN (Online): 2581-5792

Secure and Robust Digital Image Watermarking using Stegnography

M. Archana[1], R. Bharathiraja[2]

[1]*M.E. Student, Dept. of Applied Electronics, Thanthai Periyar Govt. Institute of Technology, Vellore, India*

[2]*Assistant Professor, Department of ECE, Thanthai Periyar Govt. Institute of Technology, Vellore, India*

***Abstract*: This paper presents a chaotic encryption-based blind digital image watermarking technique applicable to both grayscale and color images. Discrete cosine transform (DCT) is used before embedding the watermark in the host image. The host image is divided into 8 × 8 non overlapping blocks prior to DCT application, and the watermark bit is embedded by modifying difference between DCT coefficients of adjacent blocks. Arnold transform is used in addition to chaotic encryption to add double-layer security to the watermark. Three different variants of the proposed algorithm have been tested and analyzed. The simulation results show that the proposed scheme is robust to most of the image processing operations like joint picture expert group compression, sharpening, cropping, and median filtering. To validate the efficiency of the proposed technique, the simulation results are compared with certain state-of-art techniques. The comparison results illustrate that the proposed scheme performs better in terms of robustness, security, and imperceptivity. Given the merits of the proposed scheme, it can be used in applications like e-healthcare and telemedicine to robustly hide electronic health records in medical images.**

***Keywords*: Water marking, semi blind and images**

1. Introduction

In the area of digital watermarking, image watermarking predominantly has engrossed a lot of interest in the research community. The majority of the research work is devoted to image watermarking as compared to audio and video. Some of the reasons are described below. The test images are readily available. Images carry sufficient redundant information so that watermarks can be embedded easily. It may be assumed that any successful image watermarking algorithm may be upgraded for the video also. Images are represented in spatial domain as well as in frequency domain. The image in the transform domain is represented in terms of its frequency coefficients and in spatial domain it is represented by pixels. Simply, transform domain means the image in the form of multiple frequency bands. To represent an image in the transform domain, reversible transforms like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) or Discrete Fourier Transform (DFT) can be used. Each of these transforms has its own features and represents the image in its own ways. Watermarks can be imposed within images by changing the transform domain frequency coefficients. In case of the spatial domain, simple watermarks could be imposed in the images by modifying the pixel values or the Least Significant Bit (LSB) values. However, more robust watermarks could be imposed in the transform domain of images by changing frequency coefficients. Digital watermarking techniques are classified into different types. This classification is based on several criteria which are: Watermark Type (noise, image); Robustness (fragile, semi-fragile, robust); Domain (spatial, frequency); Perceptivity (visible watermarking, invisible watermarking); Host Data (image, text, audio, video); Data Extraction (blind, semi-blind, non-blind). Requirements for image watermarking contain imperceptibility, robustness to common signal processing operations, and capacity. Common signal processing operations which the watermark should survive include compression (such as JPEG), filtering, rescaling, cropping, A/D and D/A conversion, geometric distortions, and additive noise.

2. Watermarking classification

- *Blind or public watermarking:* In public watermarking, there is no need for original signal during the detection processing to detect the watermark. Only the secret key is required. For example, in image blind watermarking we do not need the original image.
- *Non-blind or private water marking:* In non-blind or private watermark, original signal is required for detection the watermark.
- *Semi-blind water marking:* In semi-blind watermarking, sometimes we may need some extra information for detecting the watermark. Some watermarking require access to the original signal just after adding the watermarking, which is called published watermarked signal. This form of watermarking is called semi-blind watermarking.
- *DCT:* Discrete cosine transform (DCT) is widely used in image processing, especially for compression. Some of the applications of two-dimensional DCT involve still image compression and compression of individual video frames, while multidimensional DCT is mostly used for compression of video streams. DCT is also useful for transferring multidimensional data to

frequency domain, where different operations, like spread spectrum, data compression, data watermarking, can be performed in easier and more efficient manner.

3. Proposed system

Proposes a chaotic encryption based blind digital image watermarking technique applicable to both grayscale and color images. The watermark embedding unit and watermark security unit form two important sub-systems of the proposed system. The watermark security unit is aimed at improving the security of the embedded watermark so as to make it impossible for an adversary to get the exact watermark even if it has the knowledge of embedding algorithm. Chaotic theory and Arnold encryption have been used to achieve a better security. The mathematical preliminaries of Chaos and Arnold encryption are presented in the following sub-section.

4. Block diagram

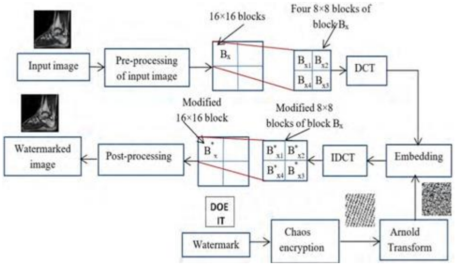

16×16 blocks
Four 8×8 blocks of block B_x
Input image
Pre-processing of input image
B_x
B_{x1} B_{x2} B_{x4} B_{x3}
DCT
Modified 16×16 block
Modified 8×8 blocks of block B_x
Watermarked image
Post-processing
B^*_x
B^*_{x1} B^*_{x2} B^*_{x4} B^*_{x3}
IDCT
Embedding
DOE IT
Watermark
Chaos encryption
Arnold Transform

Fig. 1. Block diagram

5. Chaos and arnold encryption

A chaotic based encryption algorithm is an effective method for data encryption. Chaos signals possess the qualities of pseudo-randomness, irreversibility and dynamic behavior. The systems having chaotic nature possess high sensitivity to initial parameters. The output chaotic sequence is similar to white noise having random behavior with improved correlation and complexity.

Cn+1=μ×Cn×(1−Cn)

Where 0<μ<4 typically μ is set to value 3.9 in order to achieve highest randomness and 0<Cn<1 is the nth value generated. Different values of Cn could be obtained by varying the value of n from 0 to L-1. Here, L is the maximum number of chaotic values. By setting the initial values of μ and C0, we can get the required chaotic signal. As it offers the joint advantage of speed and security, the use of chaotic encryption has been shown to offer increased security. The security of information can be increased by using various encryption techniques, and one of the effective techniques is Arnold transform. This encryption method, is two dimensional and works well in applications for encrypting images of type N×N. The Arnold transformation is mathematically represented as where (xn , yn) and (x, y) respectively represent the input image and encrypted image pixel coordinates represented as 2D matrices. The transform results in the change of the pixel positions to generate an image, which is disordered and different from original one. The result of Arnold transform is an encrypted image which has a one-to-one correspondence with the original image. The pseudo-random nature of the Arnold encryption results in a scrambled image which is not possible to be cracked down without knowing the sequence used the strength of encryption depends on the number of iterations, which can be defined at the start of the process. Inverse Arnold transform is used to decrypt the encrypted message.

[xnyn]=[1112][xy] (modN)

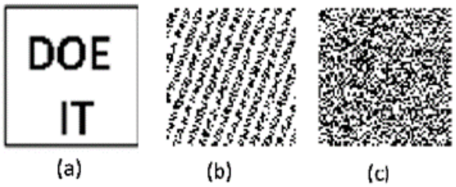
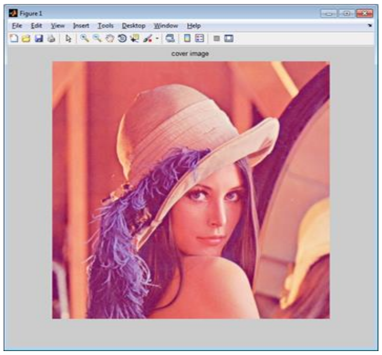


Fig. 2. (a)Original Watermark (b) First Level Watermark (c) Second Level Watermark.

6. Watermark and cover generation

The input image ‘I’ is passed through the pre-processing unit which acts as a buffer for grayscale images and as a converter for color images. To carry out watermark embedding into the luminance part of the image the pre-processing unit converts the input RGB image into YCbCr image, where Y stands for luminance information, Cb stands for chrominance blue information and Cr stand for chrominance red information of the image. The luminance part ‘Y’ is put forward as cover for the watermark because modification of this part of the image brings less noticeable changes to actual image compared to the chrominance information. On the other hand, if one wants to embed three watermarks into an RGB image, one in each plane, then the pre-processing unit extracts the RGB planes and then arranges all the three planes in a two-dimensional matrix so that each plane could be treated by the system as a P × Q grayscale plane, where P and Q respectively denote rows and columns of cover image. The resulting matrix values are brought in a range of −128 to 127 by subtracting 128 from the matrix.

7. Simulation result



cover image

Fig. 3. Input image

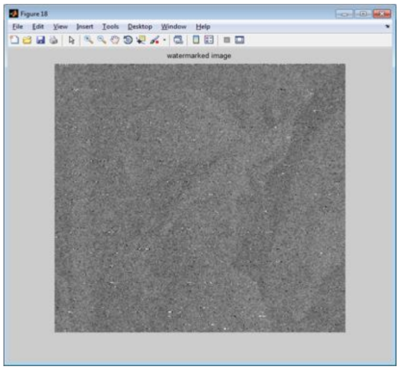


Fig. 4. Water making image

8. Conclusion

A secure and blind watermarking scheme in the DCT domain was proposed in this paper. Arnold transform and chaotic encryption were utilized to add double layer security to the watermark. The proposed embedding technique is based on the difference between the coefficients of adjacent blocks. A watermark bit is embedded by modulating the difference between two preselected mid-frequency coefficients; one from reference block and other from its succeeding block. Depending upon the value of watermark bit to be embedded the difference between two coefficients of the selected blocks is made to lie in a predefined range to facilitate proper extraction. The performance of various variants of our scheme was tested for many image processing operations such as rotation, cropping, filtering, Gaussian noise, etc. The experimental results reveal that besides being resilient to singular attacks, our scheme is highly resilient to combined attacks as well. The comparison results depict that proposed scheme outperforms many state-of-art schemes in terms of imperceptibility, robustness, and payload. Further, the double layer of security of the embedded watermark ensures that the scheme is highly secure in nature. Given the merits of the proposed scheme, we conclude that it is well suited for the application of copyright protection and ownership verification. The scheme could be used to solve various medical image integrity and electronic patient record (EPR), security issues in contemporary telemedicine and e-healthcare setups.

9. Future work

In future, the proposed algorithm will be tested for real time applications by implementing it on Field Programmable Gate Array (FPGA) platform.

References

[1] H. Tao,L.Chongmin, J. M, Zain, and A. N.Abdalla, “Robust image watermarking theories and techniques: A review,” Journal of Applied Research and Technology., vol. 12, no. 1, pp. 122–138, Feb. 2014.

[2] S.Voloshynovskiy, S. Pereira, T. Pun, J. J. Eggers, and J. K. Su, “Attacks on digital watermarks: classification, estimation based attacks, and benchmarks,” IEEE communications Magazine., vol. 39, no. 8, pp. 118-126, Aug. 2001.

[3] H.Nyeem, W. Boles, and C.Boyd, “Digital image watermarking: its formal model, fundamental properties and possible attacks,” EURASIP Journal on Advances in Signal Processing., pp. 1-22, Aug. 2014

[4] N.Zivic., “Watermarkin for Image Authentication,” in Robust Image Authentication in the Presence of Noise, ist ed. Switzerland, Springer International, Publishing, 2015, pp.43-47
[Online]. http://www.springer.com/in/book/9783319131559

[5] S. A. Parah, F.Ahad, J. A.Sheikh, and G. M. Bhat, “Hiding clinical information in medical images: A new high capacity and reversible data hiding technique,” Journal Of Biomedical Informatics.

[6] S. A. Parah, F. Ahad, J. A. Sheikh, and G. M. Bhat, “Reversible and high capacity data hiding technique for E-healthcare applications,” Multimed Tools Appl., vol. 76, no. 3, pp. 3943-3975, Feb.2017.

[7] S. A.Parah, J. A. Sheikh, J. A.Akhoon, N. A. Loan, and G. M.Bhat, “Information hiding in edges: A high capacity information hiding technique using hybrid edge detection,” Multimed. Tools Appl.