JOURNAL OF CRITICAL REVIEWS
ISSN- 2394-5125 VOL 7, ISSUE 04, 2020

An Effective Optimization and High Authenticate Feature Extraction in digital Watermarking using 2-level DWT Transform

[1]Dr.A.Lakshmi [2]N.Bhuvaneswary, [3]S.Jeevitha, [4]Muthuvel Arumugam

[1]Associate Professor [2]Assistant Professor, Department of Electronics and Communication Engineering

Kalasalingam Academy of Research and Education, Krishnankoil-626 126
[3]Assistant Professor, Kalasalingam Institute of Technology, Krishnankoil- 626 126
[4]Assistant Professor, Mohamed Sathak Engineering College, Kilakarai-623 806
[1]lakshmi@klu.ac.in [2]bhuvaneswary.n@klu.ac.in ,[3] jeevitha.ramkumar@gmail.com ,
[4]muthua21@gmail.com

Received: 14 Feb 2020 Revised and Accepted: 25 March 2020

ABSTRACT

In the current scenario, the need for security in Image processing seems to be more significant. Digital watermarking is one such feature extraction. Generally PCA (Principle Component Analysis) method is used for feature extraction. A new methodology based on 'Energy Analysis' is proposed in this research work for feature extraction. Optimization techniques are used to enhance resolution and authentication of the image. The watermarked image can be hidden in the original image using 2-level DWT and as a final point watermarked image is created in wavelet domain. For a complementary watermark modulation, the perceptual lossless ratio (PLR) is initially derived in this proposed technique. From the simulation results, optimal values are calculated and compared for both Genetic Algorithm (GA) and Particle Swarm Optimization (PSO).

Keywords: Principle Component Analysis, 2-level DWT, Perceptual Lossless Ratio (PLR), Robustness, Optimal Values, Genetic Algorithm (GA), Particle Swarm Optimization (PSO).

1. INTRODUCTION

The most primitive way of hiding information is simply by means of private-key cryptography where 'key' is considered to be the knowledge of various modes being employed. Steganography books comprise numerous examples of such methods used throughout history. Greek messengers had handled different way of hiding information such as messages tattooed into their own shave head, concealing the message when their hair finally grew back. Wax tables were scraped down to bare wood where a message was scratched. Once the tables were re-waxed, the hidden message seems to be secure often. Research in primitive cryptographic techniques becomes more popular via increasing speed, capacity and highly confidential security of the transmitted information.

Technological advancement in crypto-graphical techniques in these recent days has reached the peak success in proper encrypted and secured communication for transmission of information in our daily life. In fact, it's anticipated that the most powerful algorithms using multi kilobit key lengths could not be comprised via brute force, even though all the computing worldwide power for the next 20 year focused on the attack. There is possibility of existence of vulnerabilities still or computing power breakthroughs could also arise, but in applications as per requirement of most users current cryptographic techniques are generally adequate and it is satisfactory

Information hiding is essential for several valuable reasons; the prime objective is being that "security through obscurity" isn't necessarily a bad thing, provided that it is not the only security mechanism employed. Steganography for an occasion hides encrypted information in mediums less liable to attract ones intention. A garble of random characters being transmitted among two users may tip off a watchful 3rd party that perceptive information is being transmitted.

This project will begin with a quick background on cryptography and steganography, which form the basis for a large number of digital watermarking concepts. The project will then move on to a discussion of what requirements a watermarking system must meet, as well as methods for evaluating the strengths of various algorithms.

This project focused on different watermarking techniques and its beneficial features and also its inconvenient features of all the techniques has been discussed. This project aims almost on the watermarking of digital images; however most of these similar ideas could be applicable to the watermarking of digital video and audio.

Due to the widespread of internet any Digital-contents can be easily copied, downloaded and processed. Therefore, a robust protection method of copyrights and a copy-control system are strongly required.

Watermarking is a method of embedding additional information into the digital contents that is invisible to listeners. This project investigates its techniques on data embedding, detecting, and coding also examines the difficulties concerning multimedia data hiding in the field of multimedia security and communication, addressing both theoretical and practical aspects, and tackling troubles of both design and attack. In the fundamental part, it identifies some key elements of data hiding as a layered structure. Data hiding is categorized as a communication problem since the embedded data is the required signal to be transmitted. A choice of each embedding mechanisms leads to different robustness- capacity tradeoffs. This studies trade off for two foremost categories of embedding mechanisms. In addition, irregular or random distribution of embedding capacity brings complexity in data hiding.

A comprehensive solution has been proposed to this problem, addressing the considerations for selecting constant or variable embedding rate and enhancing the algorithms for binary images, color images and grayscale, and videos, covering such applications as tamper detection annotation, copy/access control, fingerprinting, and ownership protection. The designs affords solid examples in the choice of embedding mechanisms such as the selection of modulation/multiplexing technique(s) for hiding multiple bits, and handling of random/uneven embedding capacity. Data hiding can also be used in video communication to express side information for additional functionalities or better performance.

2. AIM AND SCOPE

Prime target is to compile an introduction to the subject of image watermarking. There already exist numerous studies technically complete treatments were not common. The survey obtained from papers, journals and conference proceedings describes best.

The next target is to seek for algorithms in executing the image encoding and watermarking successfully.

In addition to this a target on performance evaluation is essential regarding to quality and compression ratio since these factors have the major impact while executing the effort.

An ultimate goal is to design and implement a watermarking encoder. This has been implemented matlab. The source code should be easily accessible and understandable so that it can serve as a standard reference for a designer which is needed to implement a watermarking.

3. DIGITAL WATERMARKING

Digital watermarking is the practice of embedding information or messages 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. In digital watermarking, the signal may be image/pictures, audio or video. If the signal is copied, then the information also is carried with the copied signal. A single signal may carry numerous kinds of watermarks at the same time.

In visible digital watermarking, the information is visible as a picture or video. In general, if the information is assumed as text or a logo, it can be identified as the owner of the media. The image on the right side has a visible watermark. Hence if a television broadcaster adds its logo to the one corner along with the transmitted video, this logo can also be seen as a visible watermark.

In invisible digital watermarking, information is further added as digital data to any audio, picture, or video, but it cannot be perceived, although it may be possible to sense that little information is concealed in the signal). The watermark may be intended for widespread usage and thus it is made easier to retrieve or it may be in the form of steganography, where a party communicates a secret coded message embedded in the digital signal. In either case the target is to affix ownership or other descriptive information to the signal in a way that is difficult to fetch. It is also possible to use hidden embedded messages as a means of converting communication among individuals.

One best application of watermarking is in copyright protection systems, which are intended to put off in unauthorized copying of digital media. In this copyright protection the device initially fetches the watermark from the signal before copying and decides whether to copy or not by analyzing the contents enclosed in the watermark.

Another major application is in source tracing. A watermark is embedded into a digital signal at each point of distribution. If a copy of the work is found later on, then the watermark may be retrieved from the copy and the source of the distribution is identified. This technique reportedly has been used to perceive the source of illegally copied movies. Annotation of digital photographs with descriptive information is one more application of invisible watermarking.

In some file formats (.jpeg, .tiff, .png, .bmp) digital media may enclose additional information called metadata, so digital watermarking is unique in the way of data carrying in the signal.

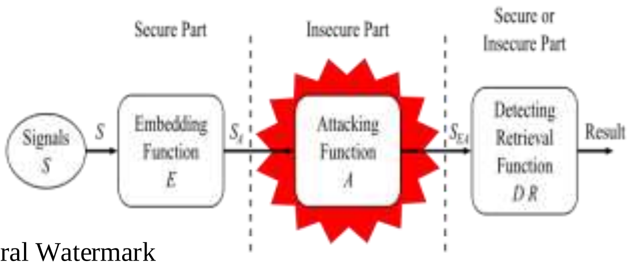


Fig. 1 - General Watermark lifecycle

4. DISCRETE WAVELET TRANSFORM

Calculation of wavelet coefficients at each and every possible scale is a fair amount of work, and it generates an lot of data. If the scales and positions are chosen based on powers of two, the so-called dyadic scales and positions, then calculating wavelet coefficients are efficient and just as accurate. This is attained from discrete wavelet transform (DWT).

The algorithm to extract DWT coefficients is explained below: Let B be the original grey scale cover image. This image is segmented as non-overlapping using haar technique. This is denoted as,

B_k, n = 0, 1, 2, 3 ... N-1 (1)

A. WAVELET WATERMARKING TECHNIQUE

Wavelet domain seems to be one of the most promising watermark embedding. Separation of image into multiple components such as lower resolution approximation(LL) in addition with Horizontal(HL), vertical(LH) and diagonal(HH) components. Another possible domain for watermark embedding is that of the wavelet domain. This repetitive process is done to evaluate numerous "scale" wavelet decomposition like 2 scale wavelet transform as shown below.

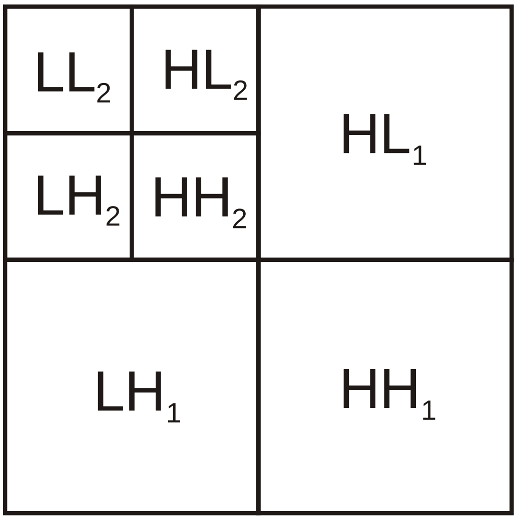


Fig. 2 - 2 Scale 2-Dimensional Discrete Wavelet Transform

The advantages of wavelet transform is trusted to be the most superior model aspects of the HVS while comparing with FFT or DCT. This beneficial feature of wavelet domain helps in permitting higher level of watermarks in regions where the HVS is known to be less sensitive to high resolution bands (LH,HL,HH) Embedding of watermarks in these regions leads to greater increase in robustness of our watermark and besides no impact on image quality.

One such straightforward techniques is to use a identical embedding technique to that used in the DCT, the embedding of a CDMA sequence in the detail bands according to the equation given below.

$$I_{W_{u,v}} = \begin{cases} W_i + \alpha |W_i| x_i, & u,v \in HL, LH \\ W_i & u,v \in LL, HH \end{cases} \qquad (2)$$

Where W_i indicates the coefficient of the transformed image, X_i denotes bit of the watermark to be embedded, and α a scaling factor. The same pseudo-random sequence used in CDMA generation is produced to perceive the watermark and estimate its correlation among two transformed detail bands. If the correlation exceeds beyond some threshold T, the watermark is predicted.

Multiple bit messages can also be easily generated by embedding multiple watermarks into the image. As in the spatial version, a separate seed is used for every PN sequence, later it is then added to the detailed coefficients. During detection, whenever the correlation exceeds T for a particular sequence a “1” is recovered; otherwise a zero. The recovery process then iterates throughout PN sequence till all the bits of the watermark have been recovered.

Moreover, the embedding process should have a certain extent to adaptability as the embedding holds the values of the transformed value in embedded which stores major watermark in larger coefficients. This claims that the embedding technique should prove resistant to JPEG compression, cropping, and other typical attacks.

The simplest example for Watermarked Lena and response of the watermark detector after JPEG-compression using 50% quality factor is clearly illustrated in the below fig.

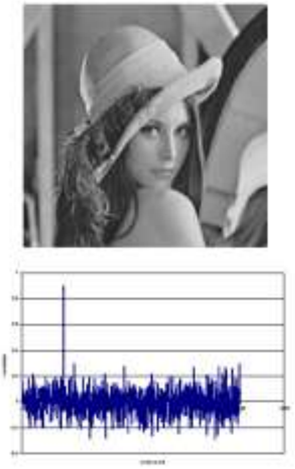


Fig. 3 - Watermarked Lena and response of the watermark detector after JPEG-compression using 50% quality factor.

5. SINGULAR VALUE DECOMPOSITION

SVD is a numerical technique used to diagonalize matrices in numerical analysis in which this algorithm has been extends to wide range of applications. The core properties

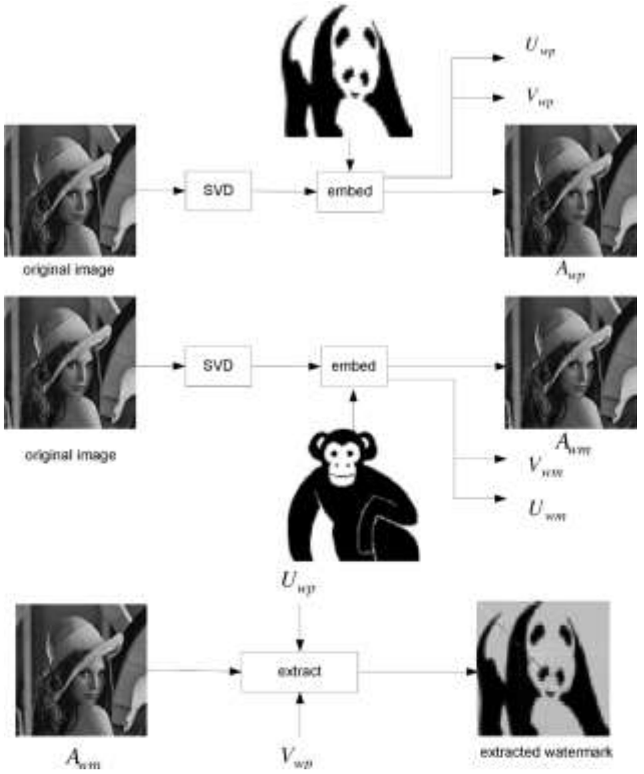


Fig. 4 - Extracted watermark is determined by the pair of SVD matrices employed in the watermark detection

of SVD in the view-point of image processing applications are:

1) The singular values (SVs) of an image have very fine stability, eventhough if a little undesired perturbation is included in the image its SVs do not change considerably.

2) SVs characterize intrinsic algebraic image properties. Based on SVD, we describe a watermark casting and detection scheme. We can examine that discrete image is considered an array matrix comprising of nonnegative scalar entries in the viewpoint of linear algebra. Let such an image be denoted by without loss of generality, we assume in the succeeding discussions that is a square image, denoted by, where depicts either the real number domain or the complex number domain. The SVD may defined as $A=USV^T$ (3) Here U and V considered to be the orthogonal matrices ($UU^T= I$, $VV^T = I$) of size mxm and nxn respectively. S, with size mxn, is the diagonal matrix with r (rank of A matrix) non-zero elements are known as singular values of A matrix.

U and V matrices columns are called left and right singular vectors respectively. Consider A as an image in our case, S have the luminance values of the image layers created by left and right singular vectors. Left singular vectors correspond to horizontal details while right singular vectors correspond to the vertical details of an image.

The unique aspect used in SVD based compression methods is that the SVs come in declining order which means significant fall from first SV to the last one.

Slight alteration of SVs does not cause any impact on image quality and also SVs do not seems much change even after attacks, which are the most needed pr o per ties in watermarking schemes.

In embedding stage, SVD based compression method is applied to the cover up image, watermark is further added with a gain parameter to the SV matrix S, SVD is applied just once, the resultant U and V matrices are stored and resultant SV matrix is used up with U and V matrices of the cover image to compile the watermarked image.

In extraction stage, the embedding steps are reversed: SVD is applied to watermarked image. An intermediate matrix is composed by making use of stored U and V matrices and singular matrix of watermarked image. The watermark is extracted from the intermediate matrix by subtracting singular matrix of cover image.

A. EXAMPLES

Consider a example, a 256x256 image "Lena" is taken as the host image A. "Panda" image is taken as watermark Wp and "Monkey" image is taken as watermark Wm. Both the watermarks are applied to the host image and generating two watermarked images Awp and Awm and also to attain the matrix S and SVD signature matrices Uwp and Vwp for the watermark Wp has also obtained.

Here the scaling parameter is $\alpha = 1/255$. At the detector end, there is no evidence for watermark whether is embedded or not. Now if we try to identify whether watermark Wp ("Panda") is embedded in the watermarked image Awm (with watermark Wm—"Monkey").

Ideally, the extracted watermark Wmp must have no correlation with "Panda" because the embedded watermark is a "Monkey." On the other hand, as predicted in Section I, the extracted watermark Wmp is a "Panda" in its place of the real embedded watermark "Monkey," there are slight differences in diagonal values, as shown in Fig.

The correlation coefficient of the extracted watermark with the reference watermark "Panda" is 0.9982. It perceived "Panda" from a watermarked image along with a "Monkey" watermark using the watermarking method. The basic imperfection is that the reference watermark "Panda" is "stamped" besides at the detector end. Unlike the illustration we presented here, the true embedded watermark and the reference watermark that generates the SVD matrices employed in the detector are the alike. The correlations of the extracted watermark through a set of watermarks are then evaluated. In such cases, the "stamped" reference watermark will certainly exist at the detector end as we analysed. SVD transformation enriched with a number of attractive properties. Foremost, the matrix need not be a square, it can also be a rectangle.

Second, the singular values *i*, λ of an image matrix have excellent stability, i.e., when a large perturbation is added to an image, its SVs do not alter significantly. It motivates watermark embedding by modify the SVs of image slightly. Where *I*λ, *i* = 1, 2,…, *R* are the Eigen values of **H** and they are satisfied$\lambda 1 \geq \lambda 2 \geq \lambda R$. **U** is $M \times M$ matrix, **V** is $N \times N$ matrix, and they are the Eigen vectors of **H.** The size of **S** is $M \times N$. The upper right *T* is the transpose of the matrix.

6. DIGITAL WATERMARK EMBEDDING AND EXTRACTING

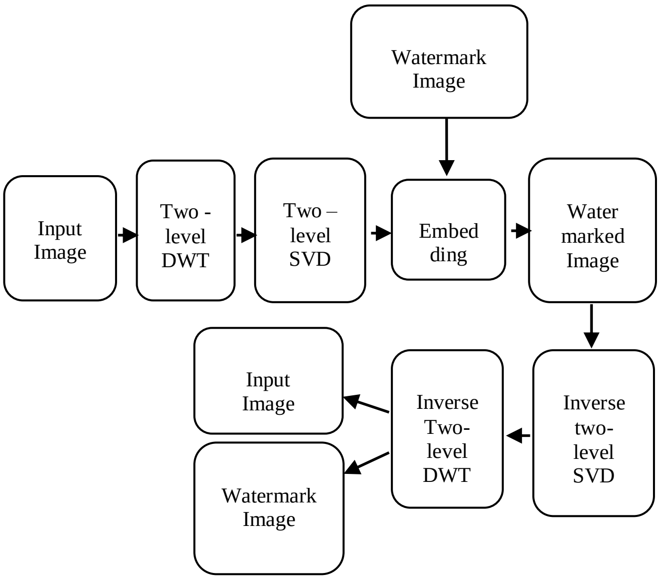


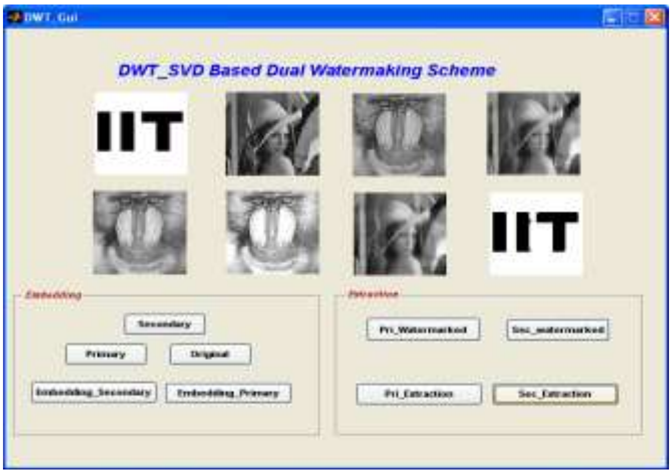
Fig. 5 - Embedding and extracting the watermark image

The proposed digital watermark embedding process is divided into 6 steps and is briefly described as below:

Step 1: The original image I (512x512) is first divided into square blocks of size 8x8 pixels, and then the DCT is applied in each block twice. Then each new block is expressed as the matrix $F_{m,n}$ ($1 \leq m \leq 64$, $1 \leq n \leq 64$).

Step 2: Perform SVD on the matrix $F_{m,n}$ ($1 \leq m \leq 64, 1 \leq n \leq 64$) to get matrices $Uf_{m,n}$, $Sf_{m,n}$ and $Vf_{m,n}$ for each matrix $F_{m,n}$, and the $Sf_{m,n}$ (1,1)of every matrix $Sf_{m,n}$ is collected together to get a new matrix A (64x64).
Step 3: Perform SVD on the new matrix A (64x64) and obtain U, V and S.
Step 4: Using W (32x32) to represent the grey watermark. Then according to $S+\alpha W \Rightarrow U_1\ S_1\ V_1^T$, obtain$V_1$, U_1 and then obtain Aˆ (64x64) according to Aˆ <= US_1^T, V (α =0.1).
Step 5: Using Aˆ(m, n) ($1 \leq m \leq 64, 1 \leq n \leq 64$) to replace the Sfm,n (1,1) of every matrix Sfm,n to get $S^*f_{m,n}$, then the $F_{m,n}$ which obtained in step 1 become $F^*_{m,n}$ according to $F^*_{m,n}$<= Ufm,n $S^*f_{m,n}$ V $f_{m,n}$.
Step 6: Apply inverse 8x8 block DCT and 8x8 SVD to $F^*_{m,n}$ twice to produce original image I *(512x512).

7. SIMULATION RESULT



WATERMARKING	PSNR	CC
Without Noises or Attacks	28.5300	-0.11003-i2.3656e^{-017}
With Noise(Salt & Pepper Noise)	27.4680	-0.11003+ i1.6177e^{-017}
With Rotation	57.6563	-0.11003-i2.4571e^{-017}
With Cropping	61.1781	-0.11003-i1.0973e^{-017}

TABLE 1 PSNR and CC comparison for various outputs

8. CONCLUSION

The main scope of the project is to increase the authentication and the quality of the image. In this project two stages are there first stage is watermarking and the second stage is optimization. In the first stage, watermark image is hided into the original image in embedding process and the watermark image and original image are separated in an extraction process. The figure shows the arrangement of original image, primary image and a secondary image. And followed to that, the watermark image is embedded into the primary image and secondary image to get a primary watermarked image and Secondary watermarked image. At last the watermark image is extracted from the primary image and the secondary image. By using this dual DWT Watermarking technique, the capacity of the invisible watermarking increases and it is highly robust.

9. REFERENCES

[1] Acken.J.M.(1998),"How watermarking adds value to digital content " , Communications of the ACM, Vol.41, No.7, pp.74-77.

[2] Andrews. H. C and Patterson. C. L. (1976), "Singular Value Decomposition (SVD) image coding", IEEE Trans. on Communications, pp. 425-432.

[3] Barni. M, Bartolini. F, Cappellini. V and Piva. A. (1998), "A DCT-domain system for robust image watermarking", Signal Processing, Vol.66, No.3, pp. 357-372.

[4] Cox. I. J, Kilian. J, Leighton. F. T and Shamoon. T. (1997), "Secure Spread Spectrum Watermarking for Multimedia", IEEE Trans. on Image Processing, Vol.6, No.12, pp.1673-1687.

[5] Craver. S, Memon. N, Yeo. B. L and Yeung. M. M. (1992), "Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks, and implications", IEEE Journal on Selected Areas in Communications, Vol.16, No.4.

[6] Craver. S, Memon. N, Yeo. B and Yeung. M. (1996), "Can invisible watermarks resolve rightful ownership", Technical Report RC 20509, IBM Research Division.

[7] Liu. R and Tan. T. (2002), "An SVD-Based Watermarking Scheme for Protecting Rightful Ownership", IEEE Transactions on Multimedia, Vol. 4, No. 1.

[8] Nikolaidis. N and Pitas. I. (1996), "Copyright protection of images using robust digital signatures", Proc. of ICASSP'96, Vol. 4, pp. 2168-2171.

[9] Nikolaidis. N and Pitas. I. (1998), "Robust image watermarking in the spatial domain", Signal Processing, Vol.66, No.3, pp.385-403.

[10] Swanson. M. D, Zhu. B, Tewp. A. H. (1996), "Transparent robust image watermarking", Proc. IEEE International Conf. on Image Processing (ICIP96), Vol. III, Lausanne, Switzerland, pp. 211-214.

[11] Wolfgang. R. B and Delp. E. J. (1997), "A watermark technique for digital imagery: further studies", Proc. of International Conference on Imaging Science, Systems, and Technology, Las Vegas, Nevada.