ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 2, Issue 10, October 2013

Efficient and Secure Digital Image Watermarking Scheme using DWT-SVD and Optimized Genetic Algorithm based Chaotic Encryption

Ms. Roshan Jahan
GBTU
Lucknow, India

Abstract— **in this paper a new digital image security scheme is applied which incorporates watermarking algorithm using DWT-SVD and optimized chaotic based image encryption obtained through genetic algorithm with high level of robustness and security.**

In this proposed scheme first of all the watermark image has been encrypted using the best hybrid model for image encryption composed of genetic algorithm and chaotic function .after that the encrypted image is embedded into original image to form the watermarked image. In the first stage of proposed encryption algorithm encrypted images is constructed using secret key and chaotic function. In the next stage, these encrypted images are used as initial population for genetic algorithm.

In this paper first time genetic algorithm has been applied on the watermark image for encryption. The similar coefficient NC, peak noise to signal ration (PNSR) and correlation coefficient (CR) are used to evaluate the transparency, robustness and security of algorithm.

All the Experiment has been performed on MATLAB and results are provided to illustrate that the proposed approach is provide good results.

1. INTRODUCTION

With the development of digital technology, computer science, communication and network, image data transformation services are widely launched and applied. Meanwhile, there are many new challenges in image information industry, such as pirate, juggle and spread abroad. So image encryption is concerned by many people. Digital watermarking is an effective way to solve these problems and has become key study in this field [1, 2].

Digital watermarking should be unappreciable, reliable and stable, *etc*. [3]. There are two kinds of digital watermarking according to the embedding technology, Spatial Domain Watermarking [4] and Transform Domain Watermarking [5]. The main advantages of Spatial Domain Watermarking are succinctness, robustness to geometric transformation and compression, but with only few watermarking information contents and weak resistibility to most attacks. Then, the main advantages of Transform Domain Watermarking are its combination with Human Visual System and fitness to modern compression standards. Wavelet-based digital watermarking [6] becomes research

hotspot in recent years for the mature study and wide application of wavelet multi-resolution analytical approaches especially the good time-frequency characteristics in information processing. In transform domain, it is easier to combine Human Visual System with watermarking with a better concealment and robustness.

In the published papers about watermarking using wavelet and chaotic technology [7], most of papers use wavelet transforms to decompose the original image and chaotic sequences to encrypt, and finally embed the watermarking image into original image. The feature lies in wavelet transform is used twice in both original image and the chaos encrypted watermarking and the embedded watermarking is the low frequency part not the whole image. This operation enhances robustness largely [9]. Another better approach in terms of robustness and perceptual quality a hybrid DWT-SVD-based watermarking scheme that requires less computation effort is developed [10].

After that a new technique has been developed for optimize encryption [12], the chaotic function Logistic Map and a key extracted from the plain-image are used to encrypt the image. The method mentioned is employed to produce a number of encrypted images using the plain-image. These encrypted images are considered as the initial population for the genetic algorithm. Then, the genetic algorithm is used to optimize the encrypted images as much as possible. In the end, the best cipher-image is chosen as the final encryption image.

In this paper the combined approach of image watermarking which have been used that satisfies two requirements i.e. imperceptibility and robustness have used combination of discrete wavelet transform (DWT) and singular value decomposition to achieve the above requirements. As well as, the watermark image is embedded directly on the elements of singular values of the original image's DWT subbands.The encryption method which I have used for the watermark image is combination of a genetic algorithm and a chaotic function and more secured [12]. Every time an encrypted image with the highest entropy and the lowest correlation coefficient among adjacent pixels is produced.

The proposed system is the combination of our different modules, they are as follows:

1. Encryption of watermark image using chaotic encryption with GA
2. Embedding the encrypted watermark image into original image using DWT-SVD watermarking technique.
3. Extraction of the encrypted watermark image from the original image.
4. Decryption of watermark image.

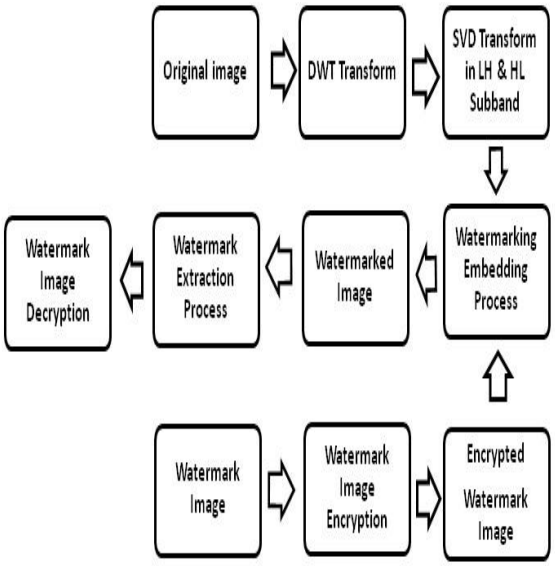

Fig.1) Proposed Model

2. DIGITAL IMAGE WATERMARKING USING DWT-SVD:

2.1 Discrete Wavelet Transform:

Discrete Wavelet Transform (DWT) is a multiresolution analytical approach of time-frequency and can describe partial characteristics of time and frequency domains. The basic thought is to decompose the image to sub images with different space and frequency, then, the coefficient is processed.
The DWT can be implemented as a multistage transformation. An image is decomposed into four subbands denoted LL, LH, HL, and HH at level 1 in the DWT domain, where LH, HL, and HH represent the finest scale wavelet coefficients and LL stands for the coarse-level coefficients.

2.2 Singular Value Decomposition:

image processing, an image can be viewed as a matrix with nonnegative scalar entries. The SVD of an image A with size n×n is given by I = USV T, where U and V are orthogonal matrices, and S = diag(λi) is a diagonal matrix of singular values
λi, i = 1, . . . , n, which are arranged in decreasing order. The columns of V are the right singular vectors, whereas the columns of U are the left singular vectors of image I.
The basic idea behind the SVD-based watermarking techniques is to find the SVD of the
cover image or each block of the cover image, and then modify the singular values to embed the watermark.

2.3 Hybrid DWT-SVD Watermarking Scheme:

The proposed DWT-SVD watermarking scheme is formulated as given here.

Watermark embedding

1) Perform one-level Haar Discrete Wavelet Transform which is used to divide the cover image I into four non-overlapping multi-resolution subbands (i.e., LL, LH, HL, and HH).

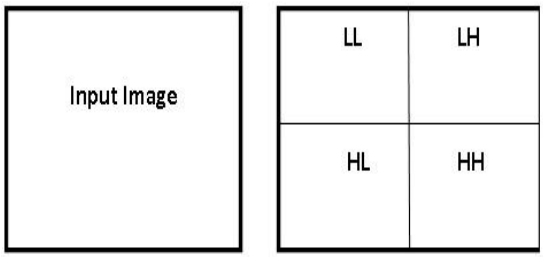

Fig. 2) input image and one level Haar DWT

2) Now Perform Singular Value Decomposition to LH and HL subbands, i.e.,

$$I_n = U_n S_n V_{nT} \quad ,n = 1, 2 \quad (1)$$

Where n represents one of two subbands.
3. Decompose the watermark image into two parts: $W = W_1 + W_2$,
where W_n denotes half of the watermark.
4) Modify the singular values in HL and LH subbands with half of the watermark image and then apply SVD to them,respectively, i.e.,

$$S_n + \alpha * W_n = U_{nw} S_{nW} V_{nTW} \quad (2)$$

where α denotes the scale factor. The scale factor is used to control the strength of the watermark to be inserted.
5) Apply the given method to obtain the two sets of modified DWT coefficients, i.e.,

$$I_{*n} = U_n S_{nW} V_{nT}, \quad n = 1, 2 \quad (3)$$

6) Now by performing the inverse DWT, obtain the watermarked image IW using two sets of modified DWT (i.e LH & HL) coefficients and two sets of unmodified DWT(LL & HH) coefficients.

Watermark extraction

1) Perform one-level Haar DWT to divide the watermarked (possibly distorted) image I∗W into four sub bands (i.e. LL, LH, HL, and HH.)
2) Perform Singular Value Decomposition to LH and HL sub bands, i.e.,

$$I_{*nW} = U_{*n} S_{*nW} V_{*nT}, \quad n = 1, 2 \quad (4)$$

where *n* represents one of two subbands.

3) Compute $E_{*n} = U_{nW} S_{*nW} V_{nTW}$, $n = 1, 2$

4) Now Extract half of the watermark image from each subband, i.e.,

$$W_{*n} = (E_{*n} - S_n)/\alpha, \quad n = 1, 2 \quad (5)$$

5 Combine the results of Step 4 to obtain the embedded watermark:

$$W_* = W_{*1} + W_{*2}$$

3. Encryption of Watermark image

3.1 Chaos Theory

Chaos theory is a branch of mathematics which studies the behavior of certain dynamical systems that may be highly sensitive to initial conditions. As a result of this sensitivity,which manifests itself as an exponential growth of error, the behavior of chaotic systems appears to be random. That is, tiny differences in the starting state of the system can

lead to enormous differences in the final state of the system even over fairly small timescales. This sensitivity is popularly referred to as the butterfly effect.

Chaos-based image encryption techniques are very useful for protecting the contents of digital images and videos.The complex structure of the traditional block ciphers makes them unsuitable for real-time encryption of digital images and videos. Real-time applications require fast algorithms with acceptable security strengths.

A chaos-based image encryption system based on logistic map, in the framework of stream cipher architecture, is proposed. This provides an efficient and secure way for image encryption and transmission.

The chaotic functions are like noise signals but they are completely certain, that is if we have the primary quantities and the drawn function, the exact amount will be reproduced. The advantages of these signals will be as follows: [13]

1) The sensitivity to the primary conditions.
2) The apparently accidental feature.
3) The Deterministic work.

The equation (1) shows one of the most famous signals which has chaotic features and is known as the logistic map signal.

$$C_{n+1} = \alpha C_n (1-C_n) \quad (1)$$

In which the C_n will get the number between [0, 1]. The signals shows three different features in three different range based on the division of the r parameter of which the signal features will be as well by considering the C_0=0.3

.

1) If we have $\alpha \in [3, 3.57]$, then the signal feature in the first 200 repetition showed some chaos and after that it was fixed.
2) If we have $\alpha \in [3.57, 4]$, then the signal feature is completely chaotic.
3) if we have $\alpha \in [0,3]$, then the signal feature in the first 10 repetitions showed some chaos and after that it was fixed.

According to the given description and the research requirements for the complete chaotic features for image Encryption, the logistic map chaotic signals with the primary values of C_0=0.3 and $\alpha \in [3.57, 4]$, are used.

3.2 Genetic Algorithm

The genetic algorithm is optimization and search technique based on the principles of genetics and natural selection.

GA composed of five components that are random number generator, fitness evaluation unit and genetic operators for reproduction, crossover and mutation operations. The initial population required at the start of the algorithm is a set of number strings generated by the random number generator. Each string is a representation of a solution to the optimization problem being addressed. Associated with each string is a fitness value (fval) computed by the evaluation unit. The reproduction operator performs a natural selection function known as "seeded selection". Individual strings are copied from one set to the next according to the fitness values, the higher the fitness value, the greater is 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 mutation operator randomly mutates or reverses the values of bits in a string. A phase of algorithm consists of applying the evaluation, reproduction, crossover and mutation operations. A new generation of solutions is produced with each phase of the algorithm.

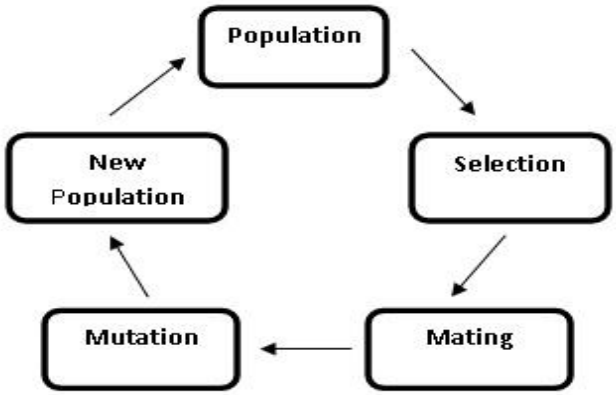

Fig. 3) Basic Genetic Algorithm Cycle

3.3 Hybrid Watermark Encryption Algorithm

(1) Divide the input image into our equal quadrants.

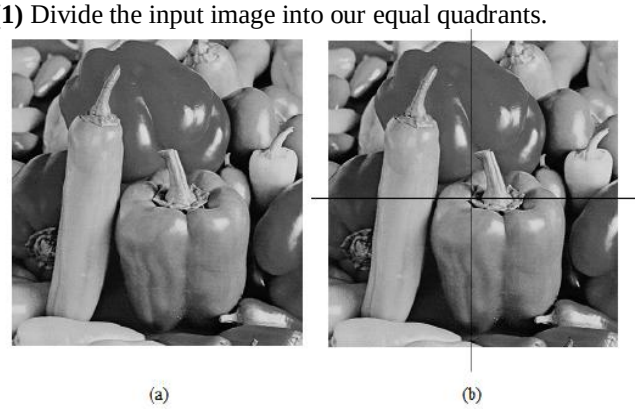

Fig. 4) (a) plain image (b) plain image divide to 4 equal parts

(2) Apply chaotic unction logistic map to individually encrypt pixels o each quadrant of image. Steps for Encryption using chaotic function logistic maps as follows:

(2.a) First of all five pixels are selected from first row of each quadrant of image which is to be used to form the initial value. Now obtain encryption key from each quadrant o the image.in this way First member of population is formed.

(2.b) Now to obtain Initial value of logistic map function, I have used following equation:

P = [P1, P2, P3, P4, P5] (Decimal) (2)

(2.c) Given equation is then used to convert K into binary number as follows:

Bin=[$P_{1,1}$, $P_{1,2}$, $P_{1,3}$,...,$P_{2,1}$...., $P_{5,7}$, $P_{5,8}$] (Binary)

(2.d) Next Equation is used to determine initial value of chaotic map function as follows:

$$U_{0k} = \frac{P_{1,1} \times 2^{39} + P_{1,2} \times 2^{38} + \cdots + P_{2,1} \times 2^{31} + \cdots + P_{5,7} \times 2^{1} + P_{5,8} \times 2^{0}}{2^{40}} \quad k=1, 2, 3, 4$$

(2.e) For each part of plain image step 2.b & 2.c is repeated.

(2.f) For encrypting pixels in each part f plain image following equation is used:

NewValue=round (U_{ik} ×255) ⊗ oldValue.

(3) Genetic Optimization: In this algorithm Genetic algorithm uses crossover operation.

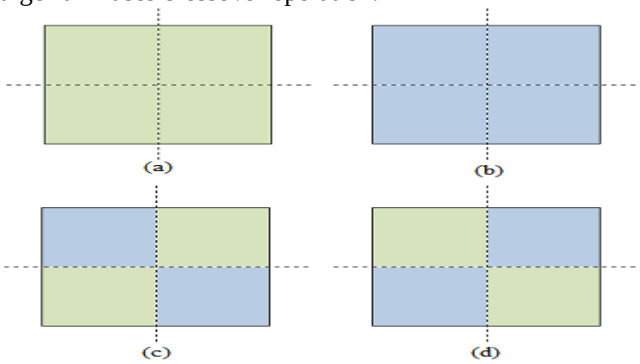

Fig.5) a,b) input images c,d)image after crossover

(4) Correlation coefficient between pairs of adjacent pixels is used to obtain fitness function.

(5) Selection of Best cipher image is on the basis of calculation of entropy and correlation coefficient. Image having highest entropy and lowest correlation coefficient is selected as best cipher image and then this image is send to the destination.

4. Experimental Results

In order to test the proposed approach of watermarking algorithm, a watermark embedding is made of a "Lena" image of 256*256.The watermarking is a "cameraman" image size of 128*128.

The results are shown in Fig.5.

Fig.6) (a) is original image, (b) is original watermark image, (c) is the watermark image after chaos with optimized GA encryption, (d) is the watermark embedded image and (e) is the watermark image after extraction and decryption process.

As a test of the embedding, Peak noise to signal rations (PSNR) and similarity degree are chosen as detection indexes. From the figures, we can see that (d) keeps a good quality with a PSNR=40.16dB.Where PSNR is higher than 30dB; it is hard to distinguish between original image and the reconstructed one. Figure (e) is also highly similar to original watermarking (NC=1.0).There is nearly no visible difference. So this algorithm is of good invisibility.

A good encryption algorithm is one in which the correlation coefficients between pairs of encrypted adjacent pixels are at the least possible level. In Figure(c) correlation coefficient is -0.2419. so this algorithm also provides higher security.

5. Conclusion

In this paper, an algorithm based on DWT-SVD and GA based chaos image encryption is referred. The security is enhanced by randomized nature of genetic algorithm and it also provides good robustness.

References

[1] Cox I J, Miller M L. Watermarking Application and Their Properties. Proc. of Int'l Conf. on Information Technology:Coding and Computing, 2000: 27-29.
[2] Cox I J, Miller M L. Watermarking Application and Their Properties. Proc. of Int'l Conf. on Information Technology:Coding and Computing, 2000: 27-29.
[3] MKutter, FJordan, FBossen. Digital Watermarking of color Image using Amplitude modulation. Journal of electronic Image, 1998.7 (2): 326-332.
[4] Liu Ruizhen; Tan Tieniu. Survey of watermarking for digital images. Journal of china institute of communications,2000,21(8)39-48.
[5] C I Prodilchuk, E J De1p Digital watermarking algorithms and applications, IEEE Signal Processing Magazine，2001, 69 (13):33-46
[6] Xiang Desheng; Xiong Yueshan Image watermarking algorithm based on DWT. Computer Engineering and Design,2005,26(3)611-613.
[7] Zhang Xiaofeng, Duan Huilong. Image Watermarking Based on Wavelet Transform. Compute Engg. And Applications，2004(11):667-671.
[8] Qiu Yuehong,He Chen, Zhu Hongwen. One Chaotic Map with Infinite Collapses and Its Quantified Sequences, Journal of Shanghai Jiaotong University,2002.1
[9] Qiang Wang,Qun Ding,Zhong Zhang,Lina Ding," Digital Image Encryption Research Based on DWT and Chaos", IEEE,Fourth International Conference on Natural Computation,2010
[10] Chin-Chin Lai and Cheng-Chih Tsai," Digital Image Watermarking Using DWT and SVD", IEEE Transactions On Instrumentation And Measurement, VOL. 59, NO. 11, November 2010
[11] X. Tong and M. Cui. Image and Vision Computing. 26(6) (2008) 843–850.
[12] Rasul Enayatifar and Abdul Hanan Abdullah," Image Security via Genetic Algorithm" IACSIT Press, Singapore, 2011
[13] H. S. Kwok and W. K.S. Tang, Chaos Solitons and Fractals, (2007) 1518–152