ISSN: 0976-3104
REGULAR ISSUE
Shaik and Masilamani

THE IIOAB JOURNAL

RESEARCH ARTICLE OPEN ACCESS

A ROBUST DIGITAL IMAGE WATERMARKING BASED ON SINGULAR VALUE DECOMPOSITION AND TABU-SEARCH

Ayesha Shaik* **and Vedhanayagam Masilamani**

Department of Computer Engineering, IIITD & M Kancheepuram, Chennai, INDIA

ABSTRACT

Digital Watermarking has become an essential tool for protecting copyrights of digital data. A singular value decomposition (SVD) and Tabu Search based digital image watermarking method has been proposed. In this approach, the singular value of the original data has been modified using multiple scaling factors for embedding the watermark image. These multiple scaling factors are generated using a meta-heuristic approach known as Tabu search. The Watermarked image obtained by the proposed approach is robust under various attacks such as rotation, cropping, JPEG compression, Histogram equalization, Average filtering and Gaussian noise.The experiment done on the standard benchmark data set shows the proposed algorithm which uses Tabu Search is more robust than the best known algorithm which uses Genetic Algorithms (GA).

Received on: 7th-April-2015
Revised on: 8th-May-2015
Accepted on: 4th-June-2015
Published on: 1st-July-2015

KEY WORDS

Watermarking; Singular Value Decomposition; Tabu Search; Meta-Heuristic; Multiple Scale factors; Robust;

***Corresponding author:** Email: ayeshanoormd@gmail.com; masila@iiitdm.ac.in **Tel:** +91-44-27476391/ 6346

INTRODUCTION

The rapid development of the Internet and availability of networked computers has made the distribution of multimedia data very fast and convenient without losing information. The consequences of such applications lead to modification and distribution of illegal data easier for the unauthorized parties. To overcome these problems, digital watermarking technique came into existence. Digital watermarking is a technique of inserting copyright (watermark) into the digital data, such as text, audio, image and video, etc. The applications of digital image watermarking are: copyright authentication, data authentication, user identification, copy protection and automated monitoring [1, 35]. The watermarking techniques can be classified based on the domain (as Spatial domain and Transform domain), the strength of the watermark (as fragile, semi-fragile and robust), visibility of the watermark (as visible and invisible) and the requirement of the original image while extracting the watermark (as Non-Blind and Blind) [2]. Also the requirements of digital watermarking such as transparency, fidelity, robustness and capacity or data payload of the watermark have been discussed.

Secure Spread spectrum watermarking has been presented in [3] and the methodology can be generalized to audio, video and multimedia data, where the watermark is independent and identically distributed Gaussian random vector and embedded imperceptibly into most significant spectral components of the original image. This method is robust to signal processing operations and common geometric distortions provided that the original image is available, i.e. the method discussed is Non-Blind watermarking. The watermarking scheme need to be adaptive in order to be robust as discussed in [4], and it should identify and embed the watermark in most significant features of the original image.

In visible watermarking, watermark is visible, because the watermark is overlaid on the original image. The watermark needs to be overlaid in a way that it has to be difficult to remove the watermark which can be a text or logo. In invisible watermarking the watermark is embedded imperceptibly into the original image. One of the simple invisible watermarking schemes is modifying the LSB plane of the original image with the message bits that need to be embedded [5].

THE IIOAB JOURNAL
ISSN: 0976-3104

Spatial domain watermarking is simple and has advantages of easy implementation, low complexity. Generally the spatial domain techniques are not robust, they are fragile. Different variations and improvements of this method are also available. In spatial domain watermarking, the embedded watermark can't resist image processing operations or attacks. The Frequency domain watermarking is performed by inserting the watermark into the magnitude of the coefficients in the frequency domain. Existing transform domain watermarking techniques include: FFT (Fast Fourier Transform), DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform), SVD (Singular Value Decomposition) and hybrid (Combination of the above transforms).

In Transform domain watermarking techniques, DWT [6, 12-19, 21-23] and SVD [7, 20] watermarking techniques have been proposed. Another watermarking technique using principal component analysis (PCA) has been discussed in [8], where the watermark is embedded in the highest energy coefficients (most significant features). DCT domain watermarking is classified into global and block-based DCT watermarking. In the global DCT scheme, a watermark is embedded in perceptually significant portion of the original image [9] and the watermarking schemes based on DCT and its variations has been discussed in [24-28]. A hybrid watermarking technique using a combination of both DWT and SVD transforms for user authentication in biometrics is proposed in [10]. DWT and the SVD watermarking scheme is proposed in [29]. An image adaptive watermarking scheme that uses wavelet for watermarking, where the watermark is embedded in the portion of the image that exhibits high tolerance towards the modification is discussed in [11]. The rotation, scale and translation invariant watermarking of a digital image with log polar mapping and phase correlation is proposed in [30]. Another reversible transform used for watermarking is Walsh-Hadamard Transform (WHT) and this technique has been presented in [31, 32].

Several digital image watermarking methods have been proposed previously. In [25], DCT watermarking method for sub bands of a digital image has been proposed. In the DWT watermarking scheme, the watermarking method is same as in DCT, the difference is in the process of transforming the original image in its frequency domain [36]. Different DWT watermarking schemes have been proposed. One of those is [13], at multiple resolutions the watermark is embedded in all high pass bands in a nested manner. In order to consider HVS factor, [14, 15] improved this technique by adding HVS factor. A dual domain watermarking technique for image authentication and compression is presented in [37], where the watermark is generated using DCT domain, and DWT domain is used to insert the watermark.

If the watermark is embedded in low frequency components of the image, then it is robust to low pass filtering, lossy compression and geometric distortions and if the watermark is embedded in the high frequency components of the image then it is robust to contrast and brightness adjustments, gamma correction, histogram equalization and cropping. In order to achieve the overall robustness of the watermarked image, multiple watermarks are embedded in low and high frequency components of the DWT transform [18]. Optimal wavelet based watermarking scheme is presented in [38], where a binary logo is used as watermark and it is inserted in all four sub bands of DWT transform with variable scaling factors in different sub bands i.e., high scaling factor for an LL sub band and low scaling factor for other three sub-bands. In [39], an improved watermarking scheme is proposed where the watermark is embedded in the SVD domain of four sub bands (LL, LH, HL, HH) of DWT transformed image.

The DFT domain watermarking technique utilizes a circular symmetric watermark to embed in the 2-D DFT domain of the original image [41]. As the watermark is circular in shape, it is robust to geometric rotation attack. Here it discusses that the scaling in spatial domain leads to inverse scaling in the frequency domain and rotation in spatial domain leads to the same rotation in the frequency domain. DFT is resistant to translation and cropping [40], Circular shifts in spatial domain do not have an effect on the magnitude of the Fourier spectrum. In above both papers, watermarking the low frequency components have some visible effect in spatial domain, and high frequency components will be removed during JPEG compression. So, embedding the watermark in mid frequencies will be better. In DFT watermarking, the watermark can be embedded either in magnitude or phase information. A DFT watermarking technique which uses phase information for embedding the watermark presented in [43], is robust to image contrast operation. Another DFT watermarking in which multiple watermarks have been embedded in low and high frequency bands are discussed in [42]. A RST resilient watermarking is presented in [44], in which watermark is embedded in the magnitude information of the re-sampled Fourier spectrum by log-polar mapping. This is not robust to cropping and weak robust to JPEG compression. Hadamard Transform based watermarking that modifies the high frequency Hadamard coefficients for embedding the watermark is proposed in [45]. A watermarking technique that uses a multi-resolution transform and Complex-Hadamard transform is presented in [46]. The multi resolution Hadamard transform is applied first, then Complex Hadamard transform is applied and the watermark is embedded in the phase component as it is more robust to

THE IIOAB JOURNAL
ISSN: 0976-3104

noise compared to amplitude modulation. An improved watermarking technique for JPEG images has been presented in [47].

In case of image watermarking, illegal tampering of the watermark should not destroy or transfer the watermark to another valid signature and it should maintain the quality of the image as well. So, in [48] two perceptual based watermarking techniques are proposed: Block-based DCT and Multi resolution wavelet framework and it provides good results for image transparency and robustness, which are the basic requirements of an effective watermarking scheme. Multi Resolution WHT (MR-WHT) and SVD based robust watermarking scheme for copyright protection is presented in [49], the image is first decomposed into sub-bands using MR-WHT and the middle singular values of the high frequency band at the coarsest and finest level are modified by the singular values of the watermark.

A new watermarking scheme with the combination of Fast WHT (FWHT) and DCT has been proposed in [50]. An adaptive image watermarking technique based on just-noticeable difference (JND) and Fuzzy Interference System (FIS) optimized with Genetic Algorithm (GA) is presented in [51]. To embed the watermark it utilizes the JND profile of the image and to improve watermark extraction performance FIS with optimized GA is used. It is robust to image manipulation attacks. In the image watermarking one of the key problems is how to hide the robust gray scale or color watermarks which is discussed in [52]. A block based watermarking scheme using SVD, where the watermark is inserted in right singular values of each block of the original image is proposed in [53].

In SVD watermarking technique the scaling factor of the watermark is maintained constant [33]. In [34], it is suggested that multiple scale factors can be considered because using constant scale factor may not be efficient in some cases. In [20], a digital watermarking scheme based on singular value decomposition and a Tiny genetic algorithm (for finding optimum scale factors) is proposed. In this paper, an SVD watermarking scheme that uses Tabu search, which is a meta-heuristic approach to find optimal scale factors to watermark the singular values of the original image is proposed.

MATERIALS AND METHODS

In this section, basic SVD based watermarking is explained in detail. Then the concept of Tabu search is discussed and how it is used to determine proper multiple scale factors for the singular values of the original image is described.

SVD based watermarking

In most of the image processing applications, image can be perceived as a matrix with non-negative scalar values. The SVD of an image F of size M x M is calculated as, $F = U\ S\ V^T$, where U and V are orthogonal matrices of size M x M and M x M respectively, and S is a diagonal matrix of size M x M i.e., S = diag (ei) where ei 's are the singular values arranged in decreasing order with i = 1, 2, 3, ..., M. Singular values of an image will have most of the energy concentrated in the beginning of the diagonal matrix as they are arranged in decreasing order. It contains the luminance values of the image and the slight modification done to the singular values will not affect the original image visual quality. So, for SVD watermarking the singular values are used for embedding the watermark. SVD of image F can be written as:

$$F = \sum_{i=1}^{r} u_i\ s_i\ v_i^T$$

Here r specifies the rank of the matrix F, ui and vi are left and right singular vectors respectively. From [7], The SVD watermarking is as follows: First, the SVD operation is performed on the original image, F resulting in three matrices U, S and V. Then, a watermark is embedded in diagonal matrix, S as S' = S + α W, where α is used to scale the watermark strength and SVD operation is employed on S' obtain three matrices U_W, S_W and V_W. The watermarked image, F_W is obtained by multiplying three matrices U, S_W and V^T.

$F = U\ S\ V^T$;
S' = S + α.W, where α.W is point wise multiplication, i.e., $\alpha\ W = (\alpha_1 W_1, \alpha_2 W_2, .. \alpha_n W_n)^T$;
$S' = U_W\ S_W\ V_W^T$;
$F_W = U\ S_W\ V^T$;

By performing the inverse operation of the watermarking, watermark extraction can be done. F_W^* is possibly modified watermarked image.

$F_W^* = U^*\ S_W^*\ V_T^*$;
$D^* = U_W\ S_W^*\ V_W^T$;

THE IIOAB JOURNAL
ISSN: 0976-3104

W* = (1/ α) (D* - S);
The verification of the watermark can be done by correlating with the inserted watermark.

The scaling vector α plays an important role in obtaining robustness. Choosing the optimal vector α using Brute-Force technique requires an exponential amount of time. Hence, it is better to use soft computing technique to find optimal or close to optimal in polynomial time. [20] uses Genetic Algorithms (GA) to find optimal vector α to get best robustness. In this paper, we use Tabu Search to find optimal vector α and the experiment done on the standard data set shows that Tabu Search gives more robustness than the GA in watermarking.

Tabu-search

Tabu Search was created by Fred W. Glover in 1986. It is a meta heuristic algorithm used for solving combinatorial optimization problems. In this paper, Tabu Search is used for optimizing the scaling factors. In [20], the authors have used Tiny GA (Genetic algorithm) for optimizing the scaling factors with small population size (ten chromosomes), little number of generations and simple fitness.

When Tabu Search is used to solve the problem, the following need to be considered: 1) Representation of solution for the problem, 2) Initial Solution, 3) Generating Candidate solutions, 4) Fitness evaluation function, 5) Tabu List to store the solutions for reducing cycles and 6) Termination criteria. Tabu Search usage can reduce the effort of computation required to generate the optimized scaling factors for watermark embedding.

Representation of the Solution: The solution, which is a vector of scaling factors to embed the watermark in the diagonal matrix can be represented as vector a = (a_1, a_2, a_3. . . a_n), where $a_i \in [0, 1]$, $1 \le i \le n$ and n x n is the dimension of diagonal matrix.

Initial Solution: Randomly generated vector of scaling factors is given as initial solution. It is assumed as the best solution (S_{best}) available till better solution is obtained.

Candidate Solutions generation: Given initial random solution, a = (a_i), where $a_i \in [0, 1]$, $1 \le i \le n$ and n x n is the dimension of diagonal matrix. Candidate solutions (CS_i) are generated as follows:

CS_i = (a_1, a_2, . . ., max (a_i, a_{i+1}), k_i , a_{i+2}, ... , a_{n-1}) ; where $a_i \in [0, 1]$; $1 \le i \le n-1$. The value of k_i is determined by the following Algorithm1, Scale (a_i, a_{i+1}) i.e., k_i = Scale (a_i, a_{i+1}) as follows:

Algorithm 1 Scale(a_i, a_{i+1})

```
initialize w=0.2
if a_i < a_{i+1} then
  lc = w.a_i + (1-w). a_{i+1}
else
  lc = w.a_{i+1} + (1-w). a_i
end if
if lc ≤ 0.2 then
  k_i=1-lc
else
  if lc ≥ 0.8 then
    k_i= lc
  else
    if 0.2 < lc ≤ 0.4 then
      lc = lc-0.2
      k_i= 1-lc
    else
      if 0.6≤ lc ≤ 0.8 then
        lc = lc + 0.2
        k_i = lc
      else
        lc = lc - 0.4
        k_i = 1- lc
      end if
    end if
  end if
end if
```

The candidate solution CS_i generated in the i^{th} iteration from the candidate solution in the previous iteration by changing i^{th} element a_i with the maximum of a_i and a_{i+1} i.e. max(a_i,a_{i+1}) and $(i+1)^{th}$ element by k_i = Scale(a_i, a_{i+1}). The algorithm that computes Scale(a_i,a_{i+1})

THE IIOAB JOURNAL
ISSN: 0976-3104

uses a parameter w, and w is initialized 0.2. The objective of Scale() function is to find the convex linear combination of a_i and a_{i+1} and the resultant value k is to be a high value in the range [0, 1]. The k found by the algorithm is more than 0.8 and less than 1.If different w is chosen, then steps in the algorithm needs to be modified so that $0.8 \leq k \leq 1$. The reason why we need to keep k in the range [0.8, 1] is that high value of k gives more robustness.

Fitness Evaluation: Fitness function is defined as a function of imperceptibility and robustness. It is used to balance the main requirements of watermarking i.e., imperceptibility and robustness.

$$Fitness = f(Imperceptibility, Robustness)$$

Fitness is measured for all the candidate solutions generated, F = (f_1, f_2, f_3, ..., f_{n-1}) and fitness for the initial solution is also measured, F_{best}. Candidate solution with minimum fitness (F_{min}) is selected as solution for the next iteration. If the fitness F_{min} is less than the best fitness, F_{best} then the candidate solution with F_{min} is selected as the best solution.The imperceptibility is measured as a normalized correlation between the original image and the watermarked image to determine the visual quality of the watermarked image. Robustness means that when the watermarked image is attacked, the inserted watermark has to be extracted with some distortion. Imperceptibility and robustness are defined by formulas as follows [20]:

$$Imperceptibility = NC(F, F_w)$$

$$Robustness = \frac{N}{\sum_{i=1}^{N} NC(W,W_i^*)}$$

$$NC(X, X^*) = \frac{\sum_i \sum_j X(i,j)X^*(i,j)}{\sqrt{\sum_i \sum_j X(i,j)^2}\sqrt{\sum_i \sum_j X^*(i,j)^2}}$$

where X and X* are the original and processed watermarked image respectively;
W, W_i* are the inserted and the extracted watermarks; N is the number of attacks considered;
F and F_W are the original and watermarked image.

Tabu list: Tabu list is used to store the candidate solutions that are best and used as the solution for the next iteration. If the candidate solution to be updated for the next iteration is already present in tabu list, then the next candidate solution with minimum fitness is selected for the next iteration. Tabu list is used to for removing cycles in the solutions, by neglecting the updated solutions in Tabu List. The solutions in the Tabu List are updated in a FIFO manner.

Termination criteria: If the number of iterations is met or if the same fitness value is being repeated for some number of iterations, then the algorithm is terminated.

Proposed work

The proposed watermarking algorithm is as shown in **Figure-1**. SVD transform is applied to the original image F i.e. $F = U S V^T$, where U and V are orthogonal matrices and S is a diagonal matrix. The diagonal matrix, S is modified by the watermark image with the initial scaling factor, $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_N)$, where N x N is the size of the diagonal matrix as follows:

$S' = S + \alpha.W$, where $\alpha.W$ is point wise multiplication, i.e., $\alpha W = (\alpha_1 W_1, \alpha_2 W_2, .. \alpha_n W_n)^T$.

Apply SVD on S' and the resulted matrices are U_W, S_W and V_W, i.e. $S' = U_W S_W V_W^T$, where U_W, V_W are orthogonal matrices and S_W is a diagonal matrix with embedded watermark. Now Watermarked image, F_W is obtained by multiplying three matrices U, S_W and V^T, i.e. $F_W = U S_W V^T$. From the attacked versions of the watermarked image F_W*, a watermark is extracted as follows. Apply SVD on possibly modified watermarked image resulting three matrices U*, S_W* and V^{*T}.

$$F_W^* = U^* S_W^* V^{*T}$$

And then calculate

$$D^* = U_W S_W^* V_W^T$$

The extracted watermark W* is

$$W^* = (1/\alpha)(D^* - S).$$

The normalized cross correlation between inserted and extracted watermark (NC (W, W*)) is calculated . Then fitness for the watermarked image is calculated as a function of imperceptibility and robustness by using Tabu search as explained under Tabu-

THE IIOAB JOURNAL
ISSN: 0976-3104

search. For the initial random set of scaling factors, original image is watermarked and the fitness value is calculated for the attacked watermarked images. The set of scaling factors with minimum fitness value is utilized for generating candidate solutions as explained under Tabu-search. The candidate solution having minimum fitness value is selected for generating next set of scaling factors. If the Candidate solution already exists in Tabu list, pick the next candidate solution having minimum fitness. If the termination condition is met, then stop the operation. Otherwise, the new set of the scaling factor is used to generate the candidate solutions until the termination criteria is met.

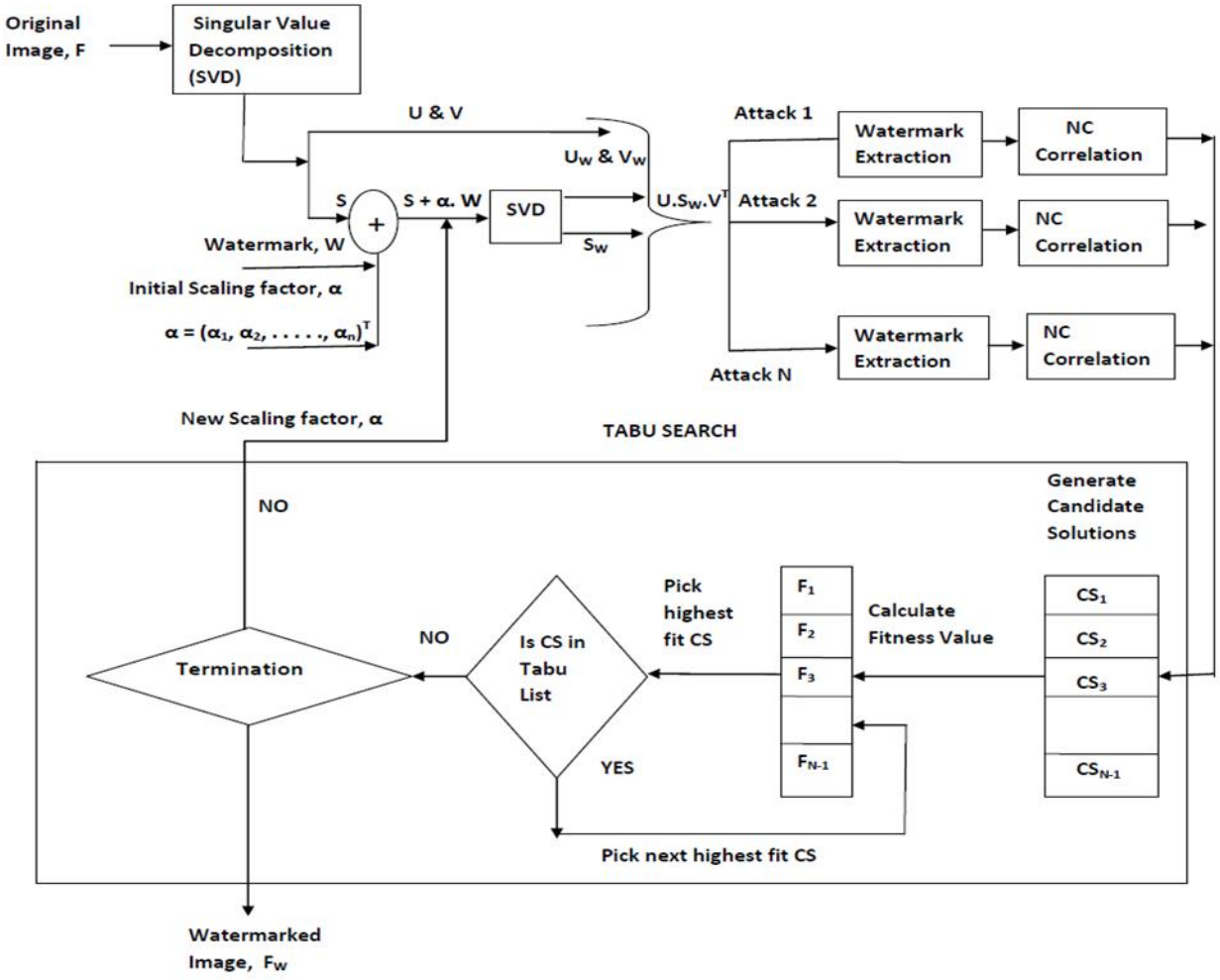

Fig: 1. Block diagram for the proposed watermarking algorithm

Block-wise SVD watermarking

In order to capture the local properties of image in watermarking, Block-Wise SVD can be considered.
Block-Wise SVD watermarking algorithm is explained in the **Fig: 2.**
The Original image F is of size M x N and Watermark image W is of size a x b.

1) Divide F into blocks of size 8 x 8, then there will be M/8 x N/8 blocks.

2) A watermark W is linearized in row major fashion, say W' is of size 1 x ab, W'(i) is the ith value of W, using row major scheme.

3) F has M/8 x N/8 blocks, linearize the blocks in row major fashion as B (i), $1 \leq i \leq$ M/8 x N/8 .

THE IIOAB JOURNAL
ISSN: 0976-3104

Case- I: Considering highest singular value in each 8 x 8 block for watermarking

In this case, highest singular value in each 8 x 8 block is considered for watermarking as it has high energy concentration.

1) Calculate $T = \frac{ab}{(\frac{M}{8})^2}$, where ab is number of linearized watermark coefficients, in order to compute how many watermark coefficients needs to be inserted in each of the 8 x 8 blocks. .

2) If T ≤ 1, then the size of the linearized watermark W' is less than the number of blocks. So,W'(i) is inserted into B(i), 1 ≤ i ≤ ab .

3) If T > 1, we can insert more than one watermark coefficient in each 8 x 8 block. So, $\lceil T \rceil$ number of watermark coefficients need to be insertyed in each 8 x 8 block.

4) The strength of the watermark, W'(i) ,1 ≤ i ≤ ab, is modified by set of scaling factors α = (αi) ,1 ≤ i ≤ ab.

5) The SVD is performed for each 8 x 8 block individually and arranged linearly in row major order.

6) The first singular value of the SVD of each block is modified by adding watermark coefficients with some strength i.e. scaling.

7) This set of scaling factors is determined by Tabu search algorithm. This technique is robust to cropping and average filtering attacks.

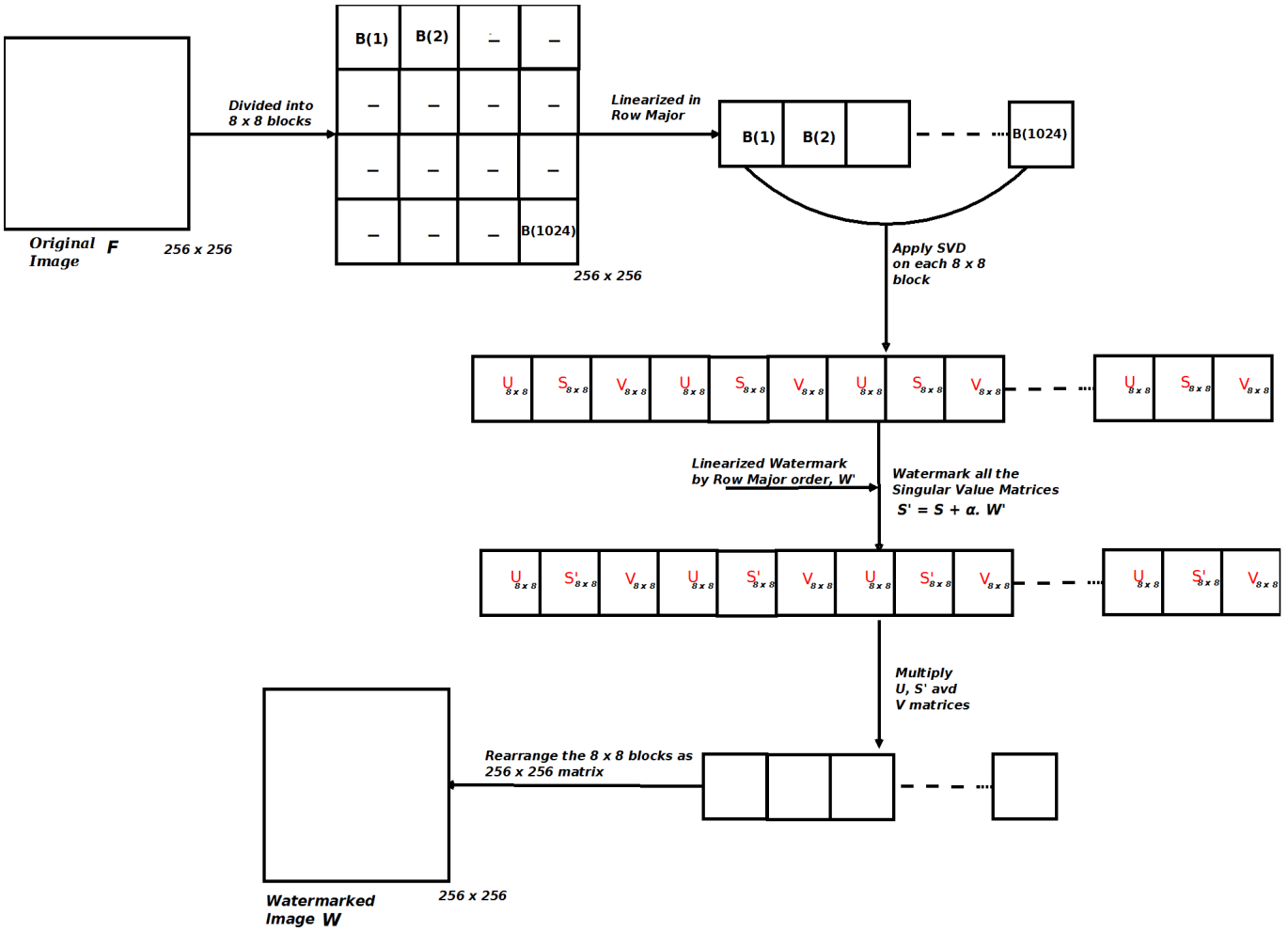

Fig: 2. Block diagram for the block-wise SVD watermarking algorithm

THE IIOAB JOURNAL
ISSN: 0976-3104

Block-wise SVD watermarking

Case II: Considering all the singular values for watermarking

In this case, all the singular values of each 8 x 8 block are considered for watermarking. Details are given below:

1) For example, the size of an original image F is 256 x 256 and the size of watermark image W is 32 x 32.

2) The original image is divided into 8 x 8 blocks, i.e. 1024 blocks of size 8 x 8 are available.

3) These blocks are organized linearly using row major fashion, i.e. B(i), $1 \leq i \leq 1024$, where i corresponds to one 8 x 8 block.

4) The watermark is also linearized in row major order, i.e. W'(i), $1 \leq i \leq 1024$.

5) If SVD is performed on B, then 8192 singular values will be available. In order to watermark all the singular values, the linearized watermark W' is expanded by a factor of 8 (8 copies of W').

6) The expanded watermark ,We (8 copies of W' that is of size 1 x 8192) is used for watermarking. Here for every 8 x 8 block two orthogonal matrices U & V and one diagonal matrix S will be available after performing SVD.

7) For 1024 blocks, U and V matrices are stored in a linear fashion.

8)The number of singular values available is 8192 and the size of expanded watermark, We is 1x 8192. So, all the singular values of diagonal matrix S are watermarked in order to incorporate watermark in all 8 x 8 blocks and the modified Singular value matrix is S'. For Case II, the watermark W' needs to be replaced by We, in **Figure-2.**

9) The strength of the watermark is modified by a set of scale factors $\alpha = (\alpha i)$, where $1 \leq i \leq 8192$. This set of scaling factors is determined by Tabu search algorithm. Then Watermarked image is obtained by multiplying all three matrices U, S' and VT and rearranging to the image of size 256 x 256 as shown in **Figure-2**.

RESULTS

The proposed watermarking scheme has been verified with the following attacks: Cropping, Rotation, Gaussian Noise, Average Filtering, Histogram equalization and JPEG compression. The experimental results have been compared with the results presented in [20] as shown in **Table−1**. For doing comparison between the inserted and extracted watermarks, 2D normalized correlation (NC) was used. If NC is closer to 1 then extracted watermark is closer to the inserted watermark. By considering multiple scaling factors for embedding the watermark we can achieve good improvement on robustness. More the strength of the scaling factor, better the robustness. On the dataset given in [54], the proposed technique is implemented and the average NC values are listed in **Table−2**. The original image, watermark and the extracted watermarks after attacks have been shown in **Figure− 3.**

The watermarked image is cropped for different rows and columns and the NC values are listed in **[Table−3]**. JPEG compression with different quality factors have been performed on the watermarked image and the NC between the inserted and extracted watermark is calculated and listed in **[Table−4]**. NC values for different rotated versions of the watermarked image is computed and compared with the algorithm presented in [20]. The cropped, average filtered and rotated version of the watermarked image is as shown in **Figure− 4.**

Table: 1. NC values of the extracted watermarks from different attacks for the image given in Fig: 2 (a)

Attack	NC for proposed	NC for SVD+GA[20]
Crop	0.9996	0.9996
Rotation	0.9932	0.9701
Gaussian Noise	0.9089	0.9069
Average Filtering	0.9804	0.9795
Histogram Equalization	0.9314	0.9286
JPEG Compression	0.9535	0.9415

THE IIOAB JOURNAL
ISSN: 0976-3104

Table: 2. Average NC values of the extracted watermarks from different attacks on images given in [54]

Attack	NC for proposed	NC for SVD+GA[20]
Crop	1(with 5 decimations)	0.99952
Rotation	0.994	0.9939
Gaussian Noise	0.885	0.888
Average Filtering	0.983	0.9817
Histogram Equalization	0.903	0.904
JPEG Compression	0.957	0.953

Table: 3. NC values of watermarked image for different cropped versions for image given in Fig: 3 (a)

Number of Rows Cropped (Out of 256)	Number of columns cropped (Out of 256)	NC for proposed	NC for SVD+GA[20]
0	First 20 and last 6 columns	0.9996	0.9999
0	First 50 and last 6	0.9978	0.999
0	First 50 and last 56	0.9926	0.9937
0	First 20 and last 256	0.9956	0.9935
First 50	First 50	0.9911	0.999
First 100	First 50	0.9913	0.994
First 150	First 150	0.9743	0.9736
First 100	First 100	0.9895	0.9887

Table: 4. NC values of JPEG compression for different quality factors for image given in Fig: 2 (a)

JPEG quality factor	NC for proposed	NC for SVD+GA[20]
50	0.9799	0.9798
75	0.9856	0.9851
90	0.9881	0.9872
95	0.9886	0.9876

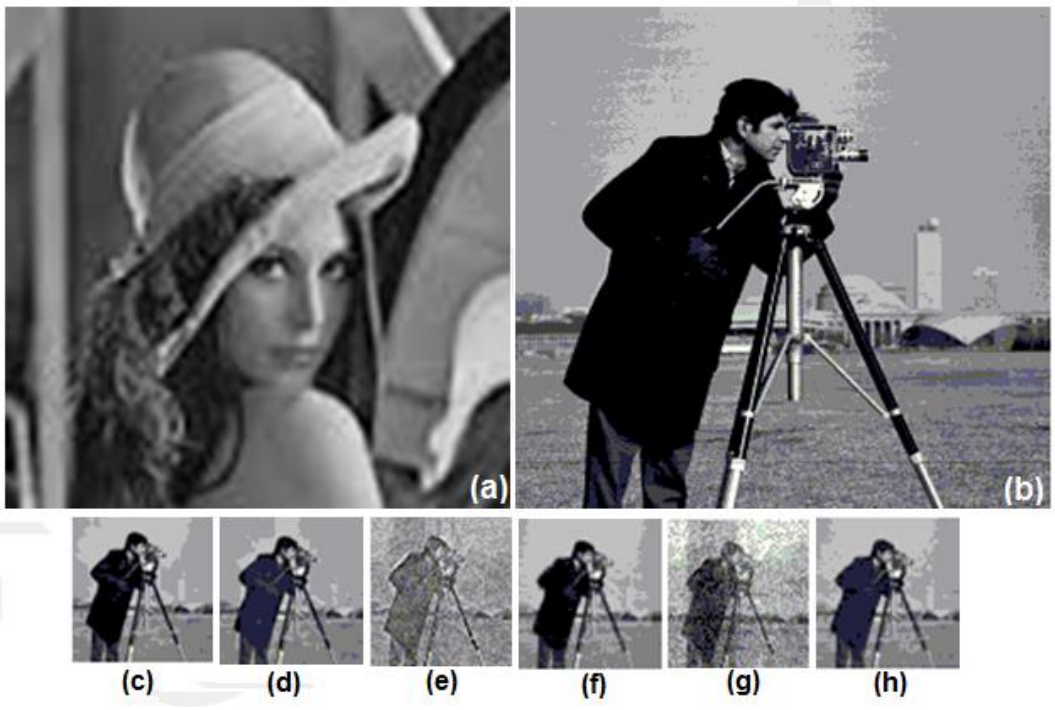

Fig: 3. (a) Original image, **(b)** watermark, **(c)** Extracted watermarks after cropping, **(d)** Rotation, **(e)** Gaussian noise, **(f)** Average filtering, **(g)** Histogram equalization and **(h)** JPEG compression attacks respectively

THE IIOAB JOURNAL
ISSN: 0976-3104

Table: 5. NC values of Watermarked image for rotation of the image given in Fig: 3 (c)

Rotation (in degrees)	NC for proposed	NC for SVD+GA[20]
-45	0.9785	0.9775
-15	0.9902	0.9901
-5	0.9985	0.9985
-2	0.9995	0.9996
2	0.9989	0.9988
5	0.9957	0.9954
15	0.9851	0.9851
45	0.9785	0.9775

Fig: 4. (a) Cropped, **(b)** Average filtered and **(c)** Rotated version of watermarked image respectively

DISCUSSION

In order to evaluate the performance of the proposed watermarking scheme, experiments have been conducted on all the images from the dataset [54]. The robustness of the proposed scheme have been evaluated with different attacks such as rotation, cropping, JPEG compression, Histogram equalization, Average filtering and Gaussian noise and compared with the algorithm presented in [20]. The strength of the watermark will modify the quality of the singular values of the image. So, instead of maintaining constant scaling factor for all the singular values, multiple scaling factors are used that are optimal for each singular value of the image. The proposed Watermarking algorithm uses Tabu Search for finding optimal scaling factors with anti-cycling memory, which will avoid the search of generating a set of scaling factors that has been already generated in the previous steps. So, at every step, a new set of scaling factor, better than the previous set will be generated, providing better robustness and imperceptibility of the watermarking algorithm.

CONCLUSIONS

A digital image watermarking scheme based on SVD and Tabu search has been proposed in this paper. Multiple scaling factors are used to embed the watermark in the diagonal matrix instead of one constant value. Tabu search is used to optimize multiple scaling factors for different singular values of the diagonal matrix to embed the watermark. The proposed method performs successfully during the attacks and the watermark can be extracted with very less degradation. During the attacks, the correlation between the extracted and inserted watermark is closer to 1 (means similar) and it performs better than the other similar works. It is observed that the proposed method is more robust compared to the algorithm that used Genetic algorithm for finding optimal scaling factors.

.

CONFLICT OF INTEREST

Authors declare no conflict of interest.

ACKNOWLEDGEMENT

None.

FINANCIAL DISCLOSURE

No financial support was received to carry out this project.

THE IIOAB JOURNAL
ISSN: 0976-3104

REFERENCES

[1] Rafael C Gonzalez, Richard E Woods, Digital image processing, Third edition, Pearson Publishers, 842−852.

[2] Potdar, Vidyasagar M., Song Han, and Elizabeth Chang [2005] "A survey of digital image watermarking techniques" in IEEE 3rd IEEE International Conference on Industrial Informatics, 709−716.

[3] Cox, Ingemar J, Joe Kilian, F Thomson Leighton, and Talal Shamoon.[1997] Secure spread spectrum watermarking for multimedia, IEEE Transactions on Image Processing, 6(12): 1673−1687.

[4] Cao JG, James E Fowler, and Nicholas H Youman, [2001] An image-adaptive watermark based on a redundant wavelet transform, in the proceedings of *IEEE International Conference on Image Processing*, 2: 277−280.

[5] Joshi, Vaibhav and MilindRane. [2014] Digital Watermarking using LSB replacement with Secret key insertion Technique.

[6] Xia, Xiang-Genm Charles G Boncelet, and Gonzalo R Arce. [1997] A Multi resolution Watermark for digital Images, in the proceedings *of IEEE International Conference on Image Processing*, 1: 548551.

[7] Liu Ruizhen, and Tieniu Tan. [2002] "An SVD based Watermarking Scheme for Protecting rightful ownership, *IEEE Transactions on Multimedia* 4(1): 121−128.

[8] Wang Shuo-zhong. [2000] Watermarking based on principal component analysis, *Journal of Shanghai University (English Edition)* 4(1): 22−26.

[9] Cox Ingemar J, and Matt L Miller. [1997] Review of Watermarking and the importance of perceptual Modeling, in *Electronic Imaging, International Society for Optics and Photonics*, 92−99.

[10] Majumder Swanirbhar, Kharibam Jilenkumari Devi, and Subir Kumar Sarkar, [2013] Singular Value Decomposition and Wavelet based IRIS biometric Watermarking, *IET Biometrics*, 2(1): 21−27.

[11] Kaewkamnerd N, and K R Rao. [2000] Wavelet based Image Adaptive Watermarking Scheme, *Electronics Letters*, 36(4): 312−313.

[12] Kundur D, Hatzinakos D. [1998] Digital Watermarking using Multiresolution Wavelet Decomposition, Proc. IEEE Int. Conf. On Acoustics, Speech and Signal Processing, Seattle, Washington, 5: 2969−2972.

[13] Zhu W, Xiong Z, and Zhang YQ. [1999] Multiresolution Watermarking for Images and Video, in *IEEE Trans. on circuit and System for Video Technology*, 9(4): 545−550.

[14] Kaewkamnerd N, Rao KR. [2005] Multiresolution based image adaptive watermarking scheme, in EUSIPCO, Tampere, Finland, (Available online www.ee.uta.edu/dip/paperfEUSIPCO water.pdf).

[15] Kaewkamnerd N, Rao KR. [2000] Wavelet based image adaptive watermarking scheme in *IET Electronics Letters*, 36(4): 312−313.

[16] Xie L, Boncelet, G, Acre, GR. [1998] Wavelet transform based watermarking for digital images, *in Optics Express*, 3(12): 497−511.

[17] Hsu CT, Wu JL. [1998] Multiresolution Watermarking for Digital Images, in IEEE Transactions on Circuits and Systems - II: Analog and Digital Signal Processing, 45(8): 1097−1101.

[18] Raval MS, Rege PP. [2003] Discrete wavelet transform based multiple watermarking scheme, Conference on Convergent Technologies for Asia-Pacific Region, TENCON 2003, 3: 935−938.

[19] Kundur D, Hatzinakos D. [1998] Digital Watermarking using Multiresolution Wavelet Decomposition, in Proc. *IEEE Int. Conf On Acoustics, Speech and Signal Processing, Seattle*, Washington, 5: 2969−2972.

[20] Lai, Chih-Chin.. [2011] A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm, *Digital Signal Processing*, 21(4):522−527.

[21] Ayesha Sk, VM Manikandan, and V Masilamani. [2015] A Combined SVD-DWT Watermarking Scheme with Multi-level compression Using Sampling and Quantization on DCT Followed by PCA, In Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014, *Springer International Publishing*, 141−149.

[22] Lee C, Lee H. [2005] Geometric attack resistant watermarking in wavelet transform domain, in Optics Express 13(4): 1307−1321.

[23] Zhu W, Xiong Z, Zhang Y-Q. [1999] Multiresolution Watermarking for Images and Video, in *IEEE Trans*. on circuit and System for Video Technology, 9(4): 545−550.

[24] Tao B, Dickinson B. [1997] Adaptive Watermarking in DCT Domain, in Proc. *IEEE International Conference* on Acoustics, *Speech, and Signal Processing*, 4: 1985−2988.

[25] Fotopoulos V, Skodras AN. [2000] A Subband DCT Approach to Image Waternarking, in Proceedings of *X European Signal Processing Conference*, Tampere, Finland.

[26] Choi Y, Aizawa K. [2002] Digital Watermarking Technique using Block Correlation of DCT Coe*fficients, in* Electronics and Communications, Japan, Part 2 85(9): 23−31.

[27] Suhail M, A Obaidat, MS. [2003] Digital Waternarking Based DCT and JPEG Model, in *IEEE Transactions on Instrumentation and Measurement*, 52(5): 1640−1647.

[28] Golikeri A, Nasiopoulos P. [2005] A Robust DCT Energy Based Watermarking scheme for Images, *Journal of proceedings of IEEE* (Available Online: www.ece.ubc.ca/~adarshg/DCT_Watermark.pdf).

[29] Ganic Enir, and Ahmet M Eskicioglu, [2004] Robust DWT-SVD domain image watermarking: embedding data in all frequencies, in proceedings of the *ACM Workshop on Multimedia and Security*, 166−174.

[30] Zheng Dong, Jiying Zhao, Abdulmotaleb El Saddik, [2003] RST – Invariant digital Image watermarking based on log-polar mapping and phase correlation, *IEEE Transactions on Circuits and Systems for Video Technology*, 13(8): 753−765.

[31] Ho Anthony TS, Jun Shen and Soon H Tan. [2003] Robust Digital Image-in-image watermarking algorithm using the fast Hardamard Transform, in International Symposium on Optical Science and Technology, *International Society for Optics and Photonics*,76−85.

[32] Zheng, Peijia and Jiwu Hauns, [2013] Walsh Hadamard Transform in the homomorphic encrypted domain and its applications in Image watermarking, in Information Hiding, *Springer Berlin Heidelberg*, 240 – 254.

THE IIOAB JOURNAL
ISSN: 0976-3104

[33] Mohan B Chandra, and S Srinivas Kumar [2008] A Robust Image Watermarking Scheme using Singular Value Decomposition, *Journal of Multimedia* 3(1): 7−15.

[34] Bao Paul, Xiaohu Ma. [2005] Image Adaptive Watermarking using Wavelet domain Singular Value Decomposition, *IEEE Transactions on Circuits and Systems for Video Technology*, 15(1): 96 − 102.

[35] Cox Ingemar J, Mathew L Miller, Jeffrey Adam Bloom and Chris Honsinger, [2002] Digital Watermarking, Vol. 53, San Francisco, Morgan Kaufmann.

[36] Hao Yin, QiuFeng Lin Chuang, and Ding Rong. [2005] A Survey of Digital Watermarking" *Journal of Computer Research and Developmen*t, 42(7): 1093−1099.

[37] Zhao Y, Campisi, P, Kundur D. [2004] Dual Domain Watermarking for Authentication and Compression of Cultural Heritage Images, in *IEEE Transactions on linage Processing*, 13(3): 430−448.

[38] Tao P , Eskicioglu, AM. [2004] A Robust Multiple Watermarking Scheme in the Discrete Wavelet Transform Domain, in Symposium on Internet Multimedia Management Systems V, Philadelphia, 133−144.

[39] Ganic E, Eskicioglu, AM. [2004] Robust digital watermarking: Robust DWT-SVD domain image waternarking: embedding data in all frequencie", Proceedings of the multimedia and security workshop on Multimedia and Security, 166 – 174.

[40] Pereira S, Pun T. [2000] Robust Template Matching for Affine Resistant Image Watermarks, in *IEEE Transactions on Image Processing*, 9(6): 1123−1129.

[41] Solachidis V, Pitas I. [2001] "Circularly Symmetric Watermark Embedding in 2-D DFT Domain, in IEEE Transactions on Image Processing, 10(11): 1741−1753.

[42] Ganic E, Dexter SD, Eskiciogl, AM. [2005] Embedding Multiple Watermarks in the DFT Domain Using Low and High Frequency Bands, IS&T/SPIE's 17th Annual Symposiun on Electronic lmaging, Security, Steganography, and Watermarking of Multitnedia Contents VII Conference, San Jose, CA.

[43] Ruanaidh JJK O, Dowling WJ, Borland FM. [1996] Phase watermarking of digital images, in Proc. *IEEE Int. Conf: Image Processing*, 239−242.

[44] Lin C-Y, Wu M, Bloom JA, Cox U, Mille, ML &Lui, YM. [2001] Rotation, Scale and Translation Resilient Watermarking for Images, *IEEE Transactions on Image Processing*, 10(5): 767−782.

[45] Gilani AM. Skodras AN. [2001] Watermarking by Multi-resolution Hadamard Transform, in Proceedings *Electronic Imaging & Visual Arts (EVA 2001*), 73−77.

[46] Falkowski BJ, Lim LS. [2000] Image Waternarking Using Hadamard Transforms", in IEE Electronics Letters, United Kingdom, 36(3): 211−213.

[47] Noore A. [2003] An improved digital watermarking technique for protecting JPEG images in *IEEE International Conference on Consumer Electronics*, Morgantown, WV, USA, 222−223.

[48] Podilchuk Christine I, and WenjunZeng. [1998] Image-adaptive watermarking using visual models, Selected Areas in Communications, *IEEE Journal*, 4;. 525−539.

[49] Bhatnagar, Gaurav, and Balasubramanian Raman. [2009] Robust watermarking in multiresolution Walsh-Hadamard Transform, In *IEEE International Conference on Advance Computing*, 894−899.

[50] Marjuni Aris, RajasvaranLogeswaran, and MF Ahmad Fauzi. [2010] An image watermarking scheme based on FWHT-DCT", In *IEEE International Conference on Networking and Information Technology (ICNIT)*, 289−293.

[51] Tsai, Hung-Hsu, and Shih-Che Lo. [2014] JND-based watermark embedding and GA-based watermark extraction with fuzzy inference system for image verification, *Informatica* 25(1) 113−137.

[52] Boland FRANCIS MORGAN, JJK O Ruanaidh, and C Dautzenberg. [1995] Watermarking digital images for copyright protection", In Fifth IET International Conference on Image Processing and its Applications, 326−330.

[53] Basso, Alessandro, Francesco Bergadano, Davide Cavagnino, Victor Pomponiu, and AnnamariaVernone. [2009] A novel block-based watermarking scheme using the SVD transform, *Algorithms* 2(1):46−75.

[54] http://lear.inrialpes.fr/jegou/data.php#copydays (May 2014).

[55] http://sipi.usc.edu/database/

ABOUT AUTHORS

Ayesha Shaik *received the B.Tech degree in Electronics and Communications Engineering in 2008 and M.Tech degree in VLSI design in 2013 from JNTU Anantapur. Currently, she is a research scholar in the Department of Computer Engineering, Indian Institute of Information Technology, Design and Manufacturing (IIITD&M) Kancheepuram. Her research interests include Digital Image Processing, Watermarking, and Hardware implementation of image security algorithms.*

Masilamani V. *is currently Assistant Professor in the Indian Institute of Information Technology,Design and Manufacturing, Kancheepuram, India. He is currently faculty in the department of Computer Science. He received his M.Tech degree from Indian Institute of Technology, Kharagpur, India. He completed his Ph.D. from Indian Institute of Technology, Madras, India. His research interest includes Image Processing and theoretical computer science. He has teaching experience of 10 years and research experience of 8 years. He has a number of international journal and conference publications.*