A Secure and Robust Image Watermarking System Using Normalization and Arnold Scrambling

Dharmalingam Vaishnavi and T. S. Subashini

(Corresponding author: Dharmalingam Vaishnavi)

Department of Computer Science and Engineering, Annamalai University
Annamalai Nagar, Chidambaram, Tamil Nadu, India

(Received Nov. 3, 2014; revised and accepted Jan. 16 & Mar. 4, 2015)

Abstract

This article proposes an image watermarking scheme to improve the robustness and security of watermark against several attacks. To achieve this, image normalization is utilized where affine transformation is applied on the image and which makes it as invariant to geometric transformations. The Lifting Wavelet Transform (LWT) and block based Discrete Cosine Transform (DCT) is applied to the cover image after normalizing an image. Then, the DC coefficients from all blocks are gathered and singular value matrix is constructed using Singular Value Decomposition (SVD). The watermark image is embedded in this singular value matrix after scrambling the image, which increases the security of the proposed scheme. The robustness and invisibleness of the proposed scheme is measured using Peak Signal to Noise Ratio (PSNR), Signal to noise Ratio (SNR) and Structural Similarity (SSIM). The comparison was made with existing schemes and it reveals that the proposed scheme provides high robustness than the existing one.

Keywords: Copyright protection, distortions, image watermarking, scrambling

1 Introduction

The marvelous growth in computer networks and the world wide web coupled with the exponential increase of computer performance, has facilitated the distribution of multimedia data [20]. The extraordinary technical revolution from analog to numerical technology was not achieved without generating anxiety in terms of the protection of the author's rights, since the digital media content, including audio, video and image can be quite easily duplicated, modified and illegally attacked by anyone, and without deterioration of the original image [10]. Thus, it came to be progressively imperative for creators of the computerized media archives to ensure themselves and secure interactive media reports as they were influenced by noteworthy income misfortunes.

Digital watermarks provide a solution to this issue and the exchange of multimedia documents has been since more secure. The digital watermarking was introduced at the beginning of the 1990s, as a second level of technical security protection after encryption. It consists of inscribing invisible secret data into the multimedia document to protect [12]. The key point of digital watermarking is to find the balance between the aspects such as robustness to various attacks and invisibleness. The invisibleness of watermarking is based on the intensity of embedding watermark and the better invisibleness is achieved for less intensity watermark. In general, there is a little compromise between the robustness and invisibleness. Increased robustness require a stronger embedding, which in turn increases the visual degradation of the images [19]. Under the human perception, the digital image watermarking scheme can be classified into two categories: visible and invisible. Visible watermarking in which, the information is obvious in the picture/video. For invisible watermarking, information is added as digital data audio, picture/video, but it cannot be perceived as such. Further, the invisible watermarks are categorized into watermarking techniques as fragile, semi fragile and robust. Fragile/semi-fragile watermark is applied to content authentication and integrity verification because of its sensitiveness to attacks. A robust method is generally used for copyright protection and ownership identification because they are designed to withstand attacks. But the geometric attacks are more complicated to deal with the other kinds of attacks. In this article, a watermarking method is proposed to alleviate the problem of distortion for geometric attacks. The rest of this paper is structured as follows: section 2 gives related works for solution to geometric distortion, section 3 gives the background details of the algorithms used, section 4 illustrates the proposed methodology, section 5 discusses the results and section 6 concludes the paper.

2 Related Works

The work in [4], the original image is transformed into Discrete Wavelet Transform (DWT) domain and a reference sub-image is formed using directive contrast and wavelet coefficient. Then the watermark is embedded by modifying the singular values of reference image using the singular values of the watermark. Many of the transform domain watermarking schemes are proposed by the authors in [3, 16, 23]. In [1] pseudorandom sequence of real number is used as watermark and genetic programming (GP) is used to structure the watermark for enhanced imperceptibility by reflecting the Human Visual System (HVS) aspects. The watermark is detected using correlation. The authors in [6], presented a robust and blind DWT based digital image watermarking scheme. The host image is transformed to wavelet domain and SVD is applied to each sub band. The watermark image is converted to form a new semi binary array and which is inserted into the selected values of SVs of decomposed host image's sub band.

The scheme in [12], the host image is normalized and Harris feature points are extracted to generate some non-overlapped circular regions. The watermark is embedded and extracted into classified regions using the DCT domain. In [9], Zernike transform is applied to the normalized host image to calculate Zernike moments. Dither modulation is adopted to quantize the magnitudes of Zernike moments according to the watermark bit stream. The quality degradation of watermarked image brought about by the embedded watermark is visually transparent.

The work in [8], the first SVs of adjacent blocks of the normalized host image are concatenated to form a singular value (SV) block. DCT is then carried out in these SV blocks. A watermark bit is embedded in the high frequency band of an SVD-DCT block by infringing a specific relationship between two pseudo randomly selected DCT coefficients. The authors in [13], offered a scheme based on logo embedding in DCT domain using image normalization techniques. A visual mask is developed to get maximum watermark embedding with least perceptual degradation. The watermarking structure is based on DCT transform. In [14], visually significant feature points are extracted by end-stopped wavelet. The watermark is embedded in the non-overlapping circular images which are determined by the feature points. These feature points can be used as synchronization marks between watermark embedding and detection. The work in [11], both the normalized host image and watermark image is divided into 8×8 sized block and DCT is applied on each block of host image. Then each watermark block is embedded in the transformed block respectively. The proposed scheme in [18], Blind Normalization Algorithm (BNA) is used to achieve affine invariant wavelet transform. In this, the first step is rotate and scale (RnS) that rotates the signal by a fixed angle θ followed by scale normalization. The second step is the computation of the orientation indicator index (OII). The normalized cover image is wavelet decomposed then the watermark is embedded in DC coefficients of a DCT transformed image. The watermarking schemes in [11, 18, 24, 25] were implemented in DCT and wavelet domains alone and the robustness achieved by these schemes were not that impressive. To improve the robustness further, the proposed scheme combines the LWT and DCT algorithms with Singular Value Decomposition.

3 Background Details

3.1 Discrete Cosine Transform(DCT)

DCT is used to convert the Time domain/spatial domain signal into the frequency domain signal. It is widely used algorithm, due to its compaction and de-correlation properties. The DCT of a given matrix gives the frequency coefficients in the form of another matrix and it is scattered into two: DC and AC coefficients. The left top corner element (zero frequency) is called as DC coefficient which is perceptually significant and which aids to enhance the robustness of the watermark [26].

3.2 Lifting Wavelet Transform (LWT)

LWT with standard 4-tap ortho normal filter with two vanishing moments is used for digital image watermarking. This algorithm consists of following three steps and is given by [21].

1) Split: It splits an input signal $x(n)$ into even and odd samples:

$$x_e(n) = x(2n), x_o(n) = x(2n+1) \tag{1}$$

2) Prediction: It denotes high frequency components of $x(n)$. It takes a difference, between the prediction value of even sample and the original value of odd sample and is denoted as detail signal $d(n)$.

$$d(n) = x_o(n) - P[x_e(n)] \tag{2}$$

where P is prediction operator.

3) Update: Update: It updates the even samples using $d(n)$ and it denotes low frequency components of $x(n)$ and is denoted as $c(n)$.

$$c(n) = x_e(n) + U[d(n)] \tag{3}$$

where U is update operator.

In comparison with general wavelets, reconstruction of image by lifting wavelet is flawless because, it increases smoothness and reduces aliasing effects. It reduces loss of information, increases intactness of the embedded watermark in the image and helps to increase the robustness of the watermark [23].

3.3 Singular Value Decomposition (SVD)

SVD is an optimal matrix decomposition technique and it packs the maximum signal energy into as few coefficients as possible. It has the ability to adapt to the variations in local statistics of an image [5]. The main features of SVD under the perspective of image processing are as follows:

- The quality of the reconstructed image will not degrade a considerable measure, even if ignoring the small SV's in the reconstruction of images.
- The SVs have very good stability, i.e. When a small annoyance is added to an image, the SVs do not vary rapidly.

An image of a real matrix with the size of m×n can be decomposed as: $A = U * S * V'$. Where U is a m×m unitary matrix, S is a m×n matrix with nonnegative numbers on the diagonal and zeros on the off diagonal, and V' denotes the conjugate transpose of V is a n×n unitary matrix. The unitary matrix U and V represent the geometry of an image. The nonnegative components of S represents the luminance value of the image.

3.4 Image Normalization

Image normalization is used to perform watermark embedding and extraction in its original coordinate system by affine transforming the image. The transform parameters are estimated from the geometric moment of the image. Therefore, the image which is invariant to any affine distortions of the image [2, 15]. It will ensure the integrity of watermark, even if, the watermarked image undergoes affine geometric attacks and which increases robustness of watermark [7]. The normalization procedure is composed of the following steps [13].

Step 1: To obtain the translation invariance, shifting the cover image to its central point, image center for $f(x,y)$ is determined by the equation $\begin{pmatrix} x_a \\ y_a \end{pmatrix} = A\begin{pmatrix} x \\ y \end{pmatrix} - d$, where, $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $d = \frac{d_1}{d_2}$ with: $d_1 = \frac{m_{10}}{m_{00}}, d_2 = \frac{m_{01}}{m_{00}}$. Where m_{00}, m_{01}, m_{10} are geometric moments of an image and let $f_1(x,y)$denotes the resulting center image.

Step 2: Apply shearing transform on $f_1(x,y)$ in the X-direction with matrix denoted $A_x = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}$ by $f_2(x,y) = A_x[f_1(x,y)]$. The value of β can be calculated using following equation $\mu_{30} = \mu_{30} + 3\beta\mu_{21} + 3\beta\mu_{12} + \beta^3$.

Step 3: Apply transform to $f_2(x,y)$ in the Y-direction with the matrix is denoted $A_y = \begin{pmatrix} 1 & 0 \\ \gamma & 1 \end{pmatrix}$ by $f_3(x,y) = A_y[f_2(x,y)]$. The value of γ can be calculated using following equation $\mu_{11} = \gamma\mu_{20} + \mu_{11}$.

Step4: Apply Scale $f_3(x,y)$ in both X and Y directions such that $A_s = \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix}$ andthe resulting image is denoted by $f_4(x,y) = A_s[f_3(x,y)]$. The value of parameters α and δ are determined by its moments $\mu_{50} > 0, \mu_{05} > 0$ respectively.

Where, μ is central moment & m is the geometric moment of an image with $p+q$ order and $p, q = 0, 1, 2, ...$

3.5 Arnold Scrambling

Scrambling is a pretreatment stage of watermarking and which makes the meaning full image as meaningless one. It is an essential issue to have the spatial correspondence decreased between the host image and the embedded watermark [22]. The 2-dimensional Arnold scrambling transformation is defined as:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} modN \qquad (4)$$

$$x, y \in 0, 1, 2, ...N-1$$

Wherein, x and y is the pixel coordinates of the original space: x' and y' is the pixel coordinates, after iterative computation scrambling; N is the size of the image, also referred to as a step number. By the above formula the corresponding inverse transform formula can be obtained:

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} x' \\ y' \end{pmatrix} modN \qquad (5)$$

$$x', y' \in 0, 1, 2, ...N-1$$

It is easy to restore the original initial state according to the corresponding iterations [17]. Arnold transformation is cyclical, when iterate to a step, it will regain original image. It is not able to restore the image without knowing about the cycle and iterations. Thus it makes security of the embedded watermark strongest.

4 Proposed Method

The watermarking scheme consists of watermark embedding and extraction processes. These two processes of proposed scheme are illustrated in the following subsections.

4.1 Watermark Embedding

The basic idea of invisible image watermark is to embed the watermark on the cover image without damaging its visual content. The proposed watermark embedding process is shown in Figure 1 and the steps involved in it are as follows:

Step 1: The normalization procedure is applied to the cover image.

Step 2: Normalized cover image is converted into four sub bands (LA, LH, LV& LD) of wavelet coefficients by applying single level LWT with Haar wavelet scheme.

Step 3: The wavelet coefficients of sub band is selected and divided as 8×8 non-overlapping sub blocks.

Step 4: Then the forward DCT is applied to each non overlapping block. Then, DC coefficient from each DCT transformed block is retrieved to form a matrix of DC's and Singular values are extracted using SVD.

Step 5: The watermark image is embedded on the matrix of singular values using controlling parameter called gain factor (g), after applying the Arnold scrambling.

Step 6: The modified SVs are replaced with original DC coefficients of each DCT transformed block and then inverse DCT is applied to each sub blocks.

Step 7: The all 8×8 non-overlapping sub blocks are organized as a single block matrix and the image is reconstructed using Inverse LWT with one modified and other three unmodified sub bands.

Step 8: The inverse normalization procedure is applied to get the watermarked image.

4.2 Watermark Extraction

The steps involved in the watermark extraction process are as follows:

Step 1: First, the normalization procedure is applied to the watermarked image then it is decomposed using single level LWT to get the sub bands of coefficients.

Step 2: The sub band, which has chosen for embedding process is selected and divided as 8×8 non-overlapping sub blocks to transform it to DCT coefficients.

Step 3: The DC coefficients from each DCT transformed block is retrieved and SVD is applied to extract the scrambled watermark coefficients.

Step 4: Then the inverse scrambling procedure is applied to obtain a meaning full recovered watermark image.

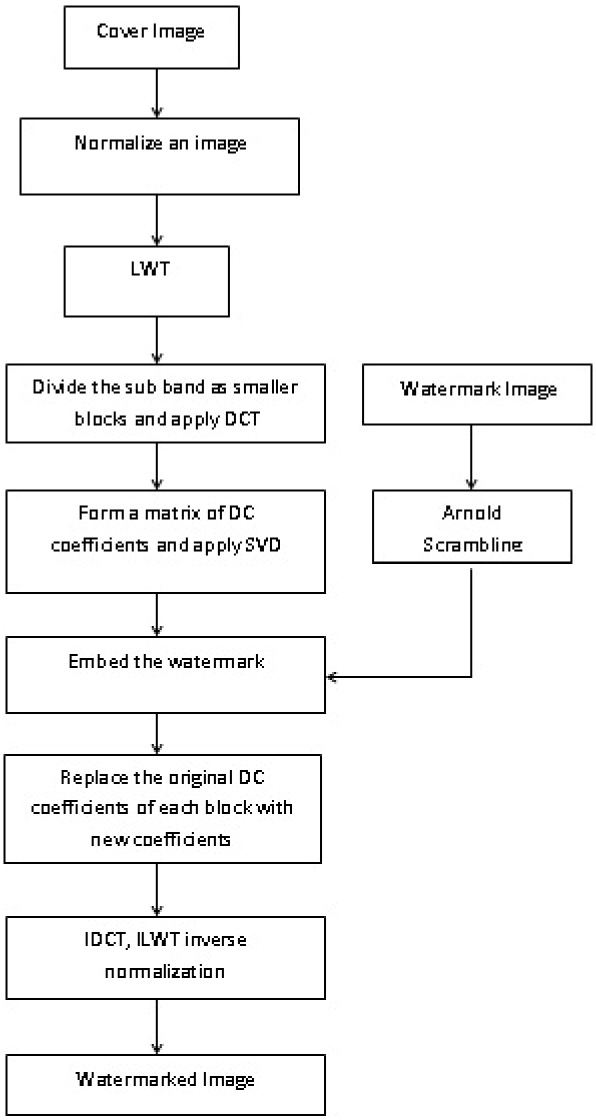
Cover Image
Normalize an image
LWT
Divide the sub band as smaller blocks and apply DCT
Watermark Image
Form a matrix of DC coefficients and apply SVD
Arnold Scrambline
Embed the watermark
Replace the original DC coefficients of each block with new coefficients
IDCT, ILWT inverse normalization
Watermarked Image

Figure 1: The Proposed scheme

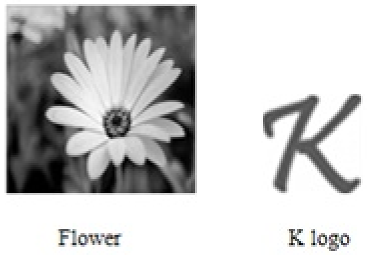

Figure 2: Sample Cover and Watermark images

5 Results and Discussions

The experiment was done by Mathworks MATLAB version 12b. The single level LWT with Haar wavelet is applied to an input image. The watermark is embedded into the wavelet of each sub band. The input of cover and watermark images are taken as a grayscale image whose resolution is 256×256 and 32×32 respectively. Figure 2 shows the sample cover image flower and the watermark K logo. Figure 3 shows watermarked flower image and the recovered K logo watermark.

In order to test the fidelity and robustness of proposed method, the metrics such as Peak Signal-to-Noise Ratio (PSNR), Structural Similarity (SSIM) and Signal-to-Noise Ratio (SNR) are calculated by Equations (6)-(9). Here, O & W represents the Original and Watermarked

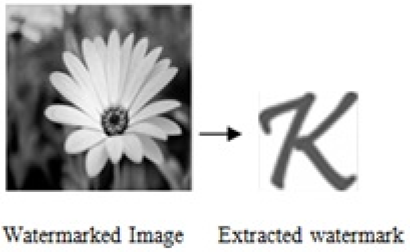

Figure 3: Watermarked image and Extracted watermark

and or recovered images.

$$PSNR = 10log_{10}\left(255^2/MSE\right) \quad (6)$$

$$MSE = \frac{\sum[O(m,n) - W(m,n)]}{M \times N} \quad (7)$$

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad (8)$$

where,

- μ_x, μ_y is the average of x,y respectively;
- σ_x^2, σ_y^2 is the variance of x and y;
- $\sigma_{x,y}$ is covariance of x and y;
- $c_1 = (k_1L)^2, c_2 = (k_2L)^2$ are two variables to stabilize the division with weak denominator;
- L is the dynamic range of the pixel values $k_1 = 0.001$ *and* $k_2 = 0.03$ by default.

$$SNR = \frac{\sum_{i=o}^{M-1}\sum_{j=0}^{N-1}[O(i,j)^2]}{\sum_{i=o}^{M-1}\sum_{j=0}^{N-1}[(O(i,j)^2 - W(i,j))^2]} \quad (9)$$

To experimentally ascertain the robustness and fidelity, the proposed approach is assessed with the watermarked image against the following attacks: Rotation, Scaling, Translation, X-Shearing, Y-shearing, noise, Contrast Increment (Cont Inc) and Histogram Equalization (Hist Eq) and the results are exposed in the Figure 4 & Figure 5. It depicts that the proposed system is resilient to all the attacks.

The fidelity and robustness of proposed scheme subject to different sub bands for the flower image is embedded with k logo watermark, is measured by PSNR calculation and is given in Table 1. It shows that the PSNR value of robustness is greater in LD sub band when compared with the other sub bands. Further, Table 2 displays the robustness of the proposed system using PSNR, SSIM and SNR measures for LD sub band subjecting to the geometric and other kinds of attacks for the gain factor of 0.5. It shows that the robustness (PSNR value) acheived is excellent for the geometric attacks scaling (46.6051), rotation (46.6092), and translation (46.6204), X- shearing (59.9161) and Y-shearing (60.1973).

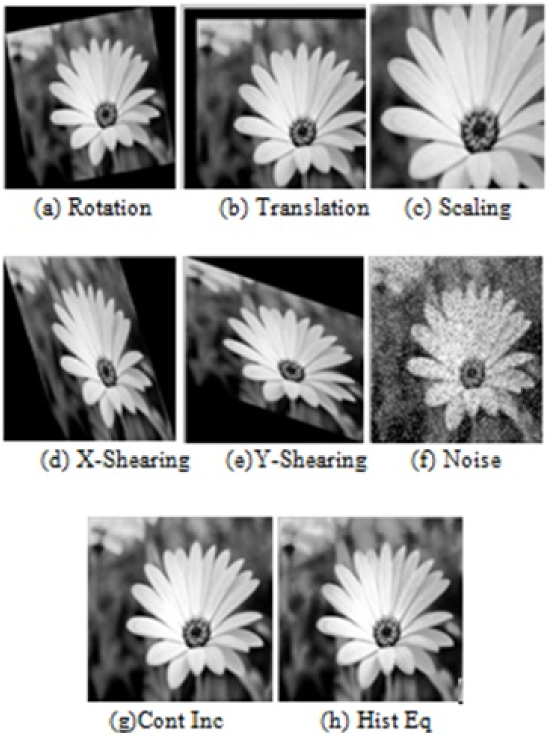

Figure 4: Flower image embedded with K logo watermark subjected to various attacks a) rotation, b) translation, c) scaling, d) X-Shearing, e) Y-shearing, f) noise, g) Cont. Inc and h) Hist Eq

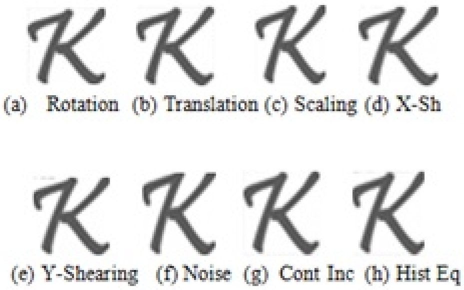

Figure 5: K logo watermark extracted from flower image after subjecting it to various attacks a) rotation, b) translation, c) Scaling, d) X-Shearing, e) Y-shearing, f) noise, g) Cont Inc and h) Hist Eq.

Figure 6: Cover image man and watermark CS logo image

5.1 Comparison of Proposed Scheme with BNA Scheme

In order to justify the results, the proposed scheme is compared with the existing system Blind Normalization

Table 1: Fidelity and robustness (PSNR value) of the flower image watermarked with K logo watermark in different sub bands

Gain Factor	LA	LH	LV	LD
Fidility				
0.1	38.9936	39.5433	39.6337	39.8160
0.5	31.2529	34.6081	35.1472	37.2655
1	26.2422	30.1644	31.1007	33.6606
Robustness				
0.1	20.9747	37.9505	35.1736	49.7414
0.5	17.9527	39.8228	46.3689	65.6337
1	24.9196	37.3635	46.3348	71.2505

Table 2: Robustness of extracting K logo watermark for gain factor=0. 5

Attacks	PSNR	SNR	SSIM
Rotation	46.6092	59.3065	0.9996
Translation	46.6204	62.4176	0.9998
Scaling	46.6051	58.0547	0.9996
X-Shearing	59.9161	58.3359	0.9996
Y-Shearing	60.1973	59.3065	0.9996
Noise	34.7532	32.8918	0.9996
Cont. Hist.	66.2200	64.3586	0.9996
Hist Eq.	62.1603	60.2989	0.9996

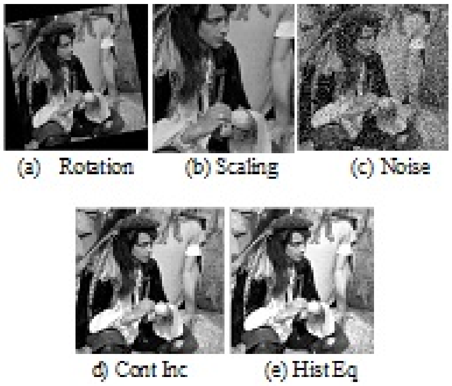

Figure 7: Cover image man embedded with CS logo watermark with various attacks a) Noise, b) Rotation, c) Cont Inc, d) Hist Eq, e)Scaling

Algorithm (BNA) based DWT- DCT watermarking[21]. The sample images in the BNA method namely man and CS logo is used as the benchmark image to do the comparative study about the performance of the proposed method and is shown in Figure 6. The Figure 7 displays the watermarked man image after the geometric attacks (Rotation & scaling) and other attacks (Noise, Cont Inc & Hist Eq).

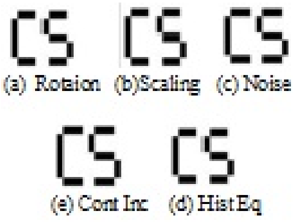

Figure 8: CS logo watermark extracted from Man image after subjecting it to various attacks a) Noise, b) Translation, c) cont Inc, d) Histogram Equalization, e) Scaling

Figure 8 displays the extracted watermark CS logo subjecting to the attacks. For comparison purpose, the proposed system is tested with the same gain factors namely 0.1, 0.5 and 1. Table 3 & Table 4 showing the comparison of fidelity and robustness of proposed method with BNA method for different sub bands with gain factors. It demonstrates that the robustness as well as the fidelity of the proposed method is far better compared to the BNA method. The improved PSNR and SNR values of the proposed method show that the proposed method is highly robust. It also shows that the LD sub band gives better PSNR and SNR values out of four sub bands. The results also depict that the watermark can be embedded in the LD sub band without any deterioration in the image quality (fidelity) and as well as it is robust to any kind geometric attacks. Further, the Table 3 also reveals that the fidelity is better for smaller gain factor.

The Figures 9-12 graphically shows that the comparison of robustness of the proposed system with BNA method for the different wavelet sub bands. Table 5 also gives a better robustness for LD sub band for the attacks with 0.5 gain factor and which is graphically shown in the Figure 13. It also shows that proposed method is highly improved compared to BNA method.

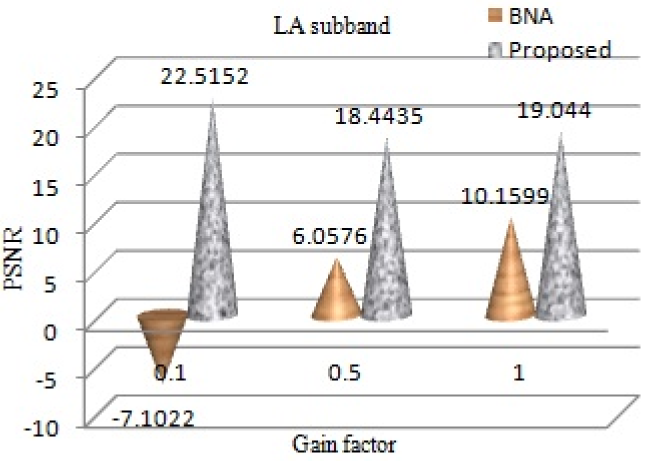

Figure 9: Gain factor vs PSNR (Robustness) for LA sub band of cover image man embedded with CS logo watermark

5.2 Robustness Against Multiple Attacks

The robustness of the proposed system is also tested to ascertain how it handles multiple geometric attacks at a

Table 3: Comparison of Fidelity for watermarked man image for different wavelet sub bands

Sub Band	Gain Factor	**Fidility**			
		BNA Method		**Proposed Method**	
		PSNR	**SNR**	**PSNR**	**SNR**
LA	**0.1**	13.7642	1.3316	34.1176	21.7089
	0.5	13.7528	1.3316	29.9730	17.5492
	1	13.6901	1.2948	26.0615	13.0445
LH	**0.1**	33.9066	-0.0668	34.2859	21.8650
	0.5	32.1404	-0.0852	18.5312	18.5312
	1	29.6951	-0.1007	29.7522	15.9511
LV	**0.1**	33.8943	-0.0672	32.7276	20.3010
	0.5	32.0385	-0.0847	31.8376	19.4194
	1	29.6203	-0.0995	29.9251	17.5330
LD	**0.1**	33.9892	-0.0668	34.7744	19.3031
	0.5	32.4560	-0.0864	32.7048	17.2510
	1	30.2078	-0.1022	29.2401	15.0430

Table 4: Comparison of Robustness of the proposed method with BNA method for different wavelet sub bands

Sub Band	Gain Factor	**Fidility**			
		BNA Method		**Proposed Method**	
		PSNR	**SNR**	**PSNR**	**SNR**
LA	**0.1**	-7.1022	-43.9509	22.5152	4.4709
	0.5	6.0576	-26.9779	18.4435	9.2920
	1	10.1599	-24.0186	19.0440	7.7655
LH	**0.1**	13.5618	-4.9816	31.5569	19.9601
	0.5	13.5498	4.1096	43.5801	34.3042
	1	13.4536	7.3074	42.0741	32.8275
LV	**0.1**	13.6057	-3.9755	37.6449	27.3884
	0.5	13.5384	3.8456	51.1598	41.9306
	1	13.4780	7.3965	58.7038	49.4626
LD	**0.1**	13.4157	1.1388	46.2885	37.0577
	0.5	13.4139	12.1995	57.9158	48.6794
	1	13.3901	14.4298	66.2543	57.0100

Table 5: Comparison of robustness (LD sub band) of proposed method with BNA method for different attacks (g=0.5)

Methods	**BNA Method**		**Proposed Method**	
Attacks	**PSNR**	**SNR**	**PSNR**	**SNR**
Noise	13.3336	4.9786	35.4550	26.2351
Rotation	13.4263	10.9554	39.3071	49.7238
Cont. Inc.	13.4329	10.1274	55.5388	46.3165
Hist. Eq.	13.4643	8.3710	55.1915	45.9938
Scaling	13.4925	7.5581	39.2162	44.8618

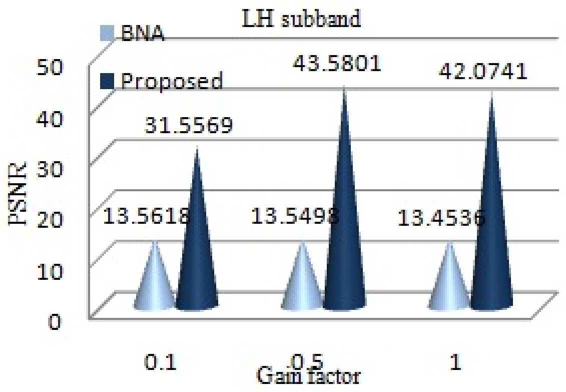

Figure 10: Gain factor vs PSNR (Robustness) for LH sub band of cover image man embedded with CS logo watermark

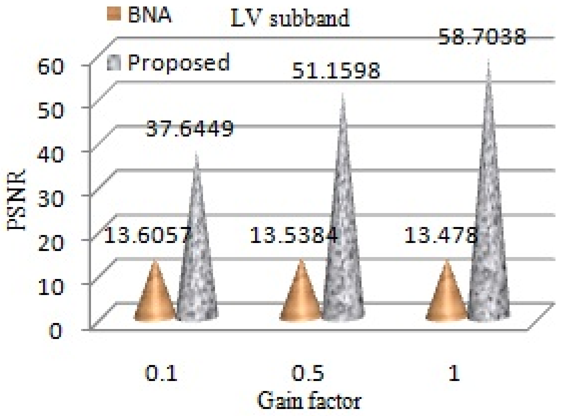

Figure 11: Gain factor vs PSNR (Robustness) for LV sub band of cover image man embedded with CS logo watermark

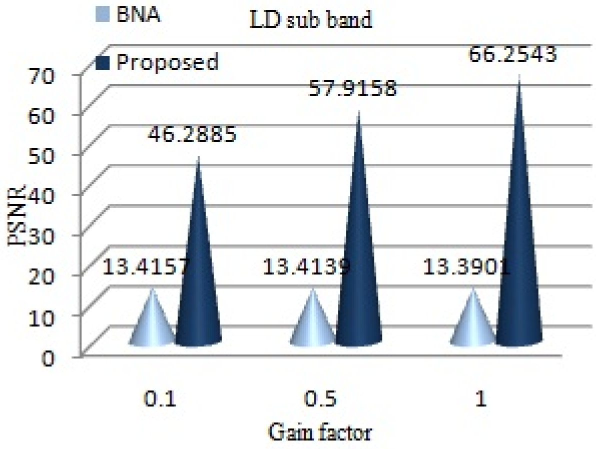

Figure 12: Gain factor vs PSNR (Robustness) for LD sub band of cover image man embedded with CS logo watermark

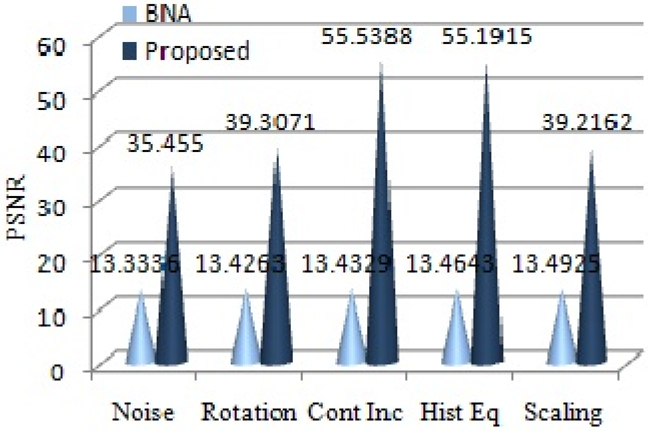

Figure 13: Robustness under the attacks for LD sub band for cover image man embedded with CS logo watermark

time. Hence, the various combinations of geometric attacks were applied to watermarked images and the watermark was recovered after the attacks. The images are taken from the standard image processing database which was embedded with the watermark shown in Figure 2. The watermark was recovered after the attacks and results are shown in Figure 14. The experiment is repeated with 20 images from the database and the mean quality measures such as PSNR and SNR tabulated in Table 6. Table 6 reveals that the proposed method is resilient to combination of various attacks also.

Table 6: Robustness for combination of geometric attacks for gain factor 0.5

Combination of Attacks	**Quality Metrics**	
	PSNR	**SNR**
Rotation +Translation	50.2126	38.5376
Translation + Scaling	41.6941	29.1566
Rotation+Scaling	46.3957	34.6203
Rotation+Translation+Scaling	46.1827	34.1939
X&Y directional Shearing	49.3310	37.8248
Rotation+Translation +X & Y Directional Shearing	50.4827	39.0628
Translation+Scaling +X & Y Directional Shearing	40.8880	28.1711
Rotation+Scaling +X & Y Directional Shearing	45.3821	33.6296
Rotation+Translation+Scaling +X & Y Directional Shearing	41.3514	28.6097

6 Conclusion

In this paper, a secure and robust watermarking scheme is developed for geometric distortion and other several attacks using image normalization. The robustness of wa-

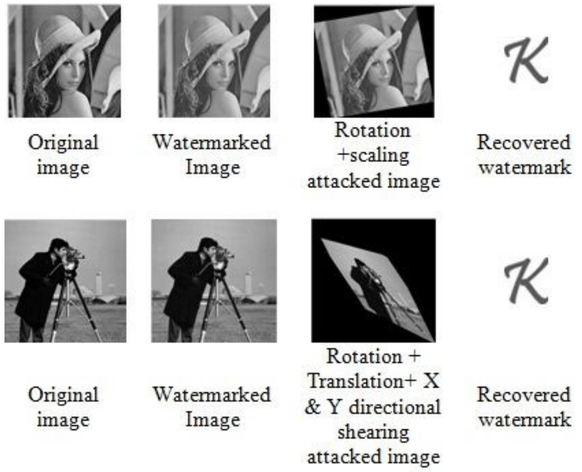

Figure 14: Results of Combination of Gometric Attacks

termark is improved by combining the algorithms namely LWT & DCT with Singular Value Decomposition. The security of proposed scheme is also achieved by scrambling the watermark image. Then, the proposed method was tested in different wavelet sub bands and various gain factors. The results from the test illustrates that the watermark embedded in the LD sub band is highly robust to geometric and various kinds of attacks. The performance of the proposed system is also compared with the results of the BNA method for various gain factors and it also reveals that the proposed system is superior and LD sub band is highly to the attacks.

References

[1] A. Abbasi, W. C. Seng, and I. S. Ahmad, "Multi block based image watermarking in wavelet domain using genetic programming," *International Arab Journal of Information Technology*, vol. 11, no. 6, pp. 582–589, 2014.

[2] Y. S. Abu-Mostafa and D. Psaltis, "Image normalization by complex moments," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. PAMI-7, no. 1, pp. 46–55, 1985.

[3] M. S. Arya, R. Siddavatam, and S. P. Ghrera, "A hybrid semi-blind digital image watermarking technique using lifting wavelet transformsingular value decomposition," in *IEEE International Conference on Electro/Information Technology (EIT'11)*, pp. 1–6, 2011.

[4] G. Bhatnagar and B. Raman, "A new robust reference watermarking scheme based on DWT-SVD," *Computer Standard & Interfaces*, vol. 31, pp. 1002–1013, Sept. 2009.

[5] D. S. Chandra, "Digital image watermarking using singular value decomposition," in *The 45th IEEE Midwest Symposium on Circuits and Systems (MWSCAS'02)*, vol. 3, pp. III–264, 2002.

[6] H. Danyali, M. Makhloghi, and F. A. Tab, "Robust blind DWT based digital image watermarking using singular value decomposition," *International Journal of Innovative Computing Information and Control*, vol. 8, no. 7, pp. 4691–4703, 2012.

[7] P. Dong, J. G. Brankov, N. P. Galatsanos, Y. Yang, and F. Davoine, "Digital watermarking robust to geometric distortions," *IEEE Transactions on Image Processing*, vol. 14, pp. 2140–2150, 2005.

[8] S. W. Foo and Qi Dong, "A normalization-based robust image watermarking scheme using SVD and DCT," *International Scholarly and Scientific Research & Innovation*, vol. 4, no. 1, pp. 753–758, 2010.

[9] S. W. Foo, Qi Dong, "A normalization-based robust watermarking scheme using zernike moments," *World Academy of Science, Engineering and Technology*, vol. 35, pp. 508–513, 2009.

[10] Li C. Huang, L. Yu Tseng, and M. S. Hwang, "The study of data hiding in medical images.," *International Journal of Network Security*, vol. 14, no. 6, pp. 301–309, 2012.

[11] A. Kumar, A. Kr Luhach, and D. Pal, "Robust digital image watermarking technique using image normalization and discrete cosine transformation," *International Journal of Computer Applications*, vol. 65, no. 18, pp. 5–13, 2013.

[12] K. Loukhaoukha, J. Y. Chouinard, and M. H. Taieb, "Optimal image watermarking algorithm based on LWT-SVD via multi-objective ant colony optimization," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 2, no. 4, pp. 303–319, 2011.

[13] F. K. Mohamed and R. Abbes, "RST robust watermarking schema based on image normalization and DCT decomposition," *Malaysian Journal of Computer Science*, vol. 20, no. 1, pp. 77, 2007.

[14] I. Nasir, F. Khelifi, J. Jiang, and S. IPSON, "Robust image watermarking via geometrically invariant feature points and image normalisation," *IET Image Processing*, vol. 6, no. 4, pp. 354–363, 2012.

[15] S. C. Pei and C. N. Lin, "Image normalization for pattern recognition," *Image and Vision Computing*, vol. 13, no. 10, pp. 711–723, 1995.

[16] C. Sharma and D. Prashar, "Visible and invisible watermarking methods for quality loss of data," *International Journal of Advanced Research in Computer Science and Electronics Engineering*, vol. 1, no. 3, pp. 57–63, 2012.

[17] C. Song, S. Sudirman, and M. Merabti, "Recent advances and classification of watermarking techniques in digital images," in *Proceedings of Post Graduate Network Symposium*, pp. 1–6, 2009.

[18] T. Sridevi and V. V. Kumar, "A robust watermarking algorithm based on image normalization and dc coefficients," *International Journal of Computer Science Issues*, vol. 8, no. 5, pp. 226–232, 2011.

[19] S. S. Sujatha and M. M. Sathik, "A novel DWT based blind watermarking for image authentication," *International Journal of Network Security*, vol. 14, no. 4, pp. 223–228, 2012.

[20] B. Surekha and G. N. Swamy, "Sensitive digital image watermarking for copyright protection," *International Journal of Network Security*, vol. 15, no. 2, pp. 113–121, 2013.

[21] W. Sweldens, "The lifting scheme: A custom-design construction of biorthogonal wavelets," *Applied and Computational Harmonic Analysis*, vol. 3, no. 2, pp. 186–200, 1996.

[22] V. Prasad, R. Kurupati, "Secure image watermarking in frequency domain using arnold scrambling and filtering," *Advances in Computational Sciences and Technology*, vol. 3, no. 2, pp. 236–244, 2010.

[23] D. Vaishnavi and T. S. Subashini, "A novel approach to improve invisibleness and robustness of a digital watermark in copyrightprotection," *International Journal of Computer Applications*, vol. 71, pp. 7–13, June 2013.

[24] D. Vaishnavi and T. S. Subashini, "A robust image watermarking for geometric distortion using dc coefficients," *International Journal of Applied Engineering Research*, vol. 9, no. 21, pp. 4895–4800, 2014.

[25] D. Vaishnavi and T. S. Subashini, "An image watermarking scheme resilient to geometric distortions," in *Power Electronics and Renewable Energy Systems*, LNCS 326, pp. 1225–1233, Springer, 2015.

[26] B. Wang, J. Ding, Q. Wen, X. Liao, and C. Liu, "An image watermarking algorithm based on DWT, DCT and SVD," in *IEEE International Conference on Network Infrastructure and Digital Content (IC-NIDC'09)*, pp. 1034–1038, 2009.

Dharmalingam Vaishnavi received her BE (IT) degree in the year 2009 and ME (CSE) degree in the year 2011 from Annamalai University. She was worked as Assistant Professor at Anjalai Ammal Mahalingam Engineering College, Thiruvarur District, Tamil nadu, India. Currently, she is pursuing Doctor of philosophy in Annamalai University. Her area of research is Image watermarking and digital forensics. She has published 9 International Journals and Conferences.

T. S. Subashini received her B.E (CSE) degree in the year 1991 from Bharath Engineering College, Chennai. In the same year she was appointed as Hardware Service Engineer in Sterling Computers Chennai and in 1996 she joined Annamalai University. She was sponsored by the University under Quality Improvement Programme (QIP), to pursue ME (CSE) at Anna University, Chennai 2001. She gained her doctoral degree in Computer Science and Engineering from Annamalai University in 2011. Her area of doctoral research is Medical Image Analysis. She has published over 35 research papers in international journals and conferences. She is now working on UGC sanctioned research project worth Rs. 11.4 lakhs on Breast Cancer. Her research interests include Image and Video processing, Computer Vision and Pattern Classification.