Volume 6, Issue 5, May 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Secure Digital Watermarking Scheme using DWT, SVD and Chaotic Scrambling

Ritu Bansal
M. Tech. Scholar, Department of CSE
MIET, Shahabad, Kurukshetra, Haryana, India

Shikha Sharma
Asst. Professor, Department of CSE
MIET, Shahabad, Kurukshetra, Haryana, India

Abstract: A secure digital watermarking algorithms using DWT, SVD and chaotic scrambling is described in this paper. Chaotic scrambling is used to encrypt the watermark image. DWT is used to decompose the original image upto two levels. After the first level decomposition, the three high frequency sub-bands (LH, HL and HH) are watermarked using the encrypted watermark. After the second level decomposition, all the sub-bands of the low frequency sub-band (LL), i.e. (LL1, LH1, HL1 and HH1) are encrypted. Thus the complete original image is watermarked with an encrypted watermarking image. Thus the technique is really robust and secure as compared to previously developed techniques.

Keywords: Chaotic Scrambling, Encryption, Digital Watermarking, DWT, SVD

I. INTRODUCTION

Digital Watermarking is defined as the process of inserting digital information which contains the identity of the owner, into other multimedia object such as image, audio, video etc. The digital information to be inserted is termed as watermark. This is basically done for copyright protection. Other applications of digital watermarking are Fingerprints, Image and content authentication, broadcast monitoring, copy and playback control, copy protection etc.

A no. of techniques has been proposed for embedding the watermark into other multimedia object. Some of these techniques use a combination of DCT-DWT [1], a combination of DWT-SVD [2], [4], a combination of DCT-DWT-SVD [3] and others.

To enhance the security without increasing the payload, chaotic scrambling is used to encrypt the watermark. After the watermark is encrypted, it is embedded into the DWT transformed image.

We define a logistic chaotic system:

$X_{k+1} = \mu x_k(1-x_k)$

Where μ is a system parameter and x_k is a mapping alternatives. And,

$X \in (0,1)$ and $\mu \in (1,4)$

Initial value x_0 and μ are used as key space $K(x_{0,}\ \mu)$ to generate chaotic sequences which scramble watermarks W. When $\mu \in (3.569945.4)$, the mapping is a real value chaotic sequence.

II. BACKGROUND REVIEW

In [5], a scheme has been described to create chaotic random sequence and watermark embedding and extraction.

To create a chaotic random sequence, the initial value x_0, y_0 is taken as a key to the sequence and $(x_0, x_1 \ldots\ldots x_{m-1})$, $(y_0, y_1 \ldots\ldots y_{n-1})$ is used as chaotic sequence, where m, n is the row and line no. of watermarking images. Then their orders are rearranged in ascending order such that a new sequence is obtained which is $(x_0', x_1', \ldots.. x_{m-1}')$, $(y_0', y_1', \ldots.. y_{n-1}')$

Then the scrambled image is scanned in the shape of word 'Z' and encoded by 0 and 1 to get a binary sequence which is an encrypted watermarking image.

To embed the encoded watermark, DWT and chaotic scrambling is used. The original image is divided into 8X8 blocks and every block is transformed using three-level DWT. Then the low frequency coefficient in the LL3 sub-band is chosen to embed the encoded watermark and then IDWT is applied to get the watermarked image.

To extract the watermarking image, the key sequence x_0, y_0 of chaotic sequence must be known and the reverse process of watermark embedding is done.

III. PROPOSED APPROACH

The proposed watermarking scheme uses the combination of DWT, SVD and Chaotic scrambling to watermark the original image. This method is different from previously described techniques in the sense that all the four sub-bands i.e. LL, LH, HL, HH of the original image are watermarked with a portion of watermarking image rather than watermarking only the low frequency sub-band (LL).

The Watermark Embedding Scheme:

Step 1- Encrypt the watermark by chaotic scrambling [4]. Let us have x_0=0.6 and μ= 3.570043 to obtain a scrambled watermark W' from W.

Step 2- Apply DWT to the 256x256 host image and decompose it to 2nd level.
Step 3- Take 4x4 blocks of coefficients from each sub band leaving the lowest frequency LL sub band. Then decompose each block with SVD, later sort the singular values in descending order, let each block be I_g .
Step 4- Set a quantization step which is marked as step;
Step 5- Get the norm of singular value vector V^λ :

$$Norm(V^\lambda) = \sqrt{\sum_{i=1}^{r} \lambda_i^{\,2}}$$

where, r is the rank of singular value matrix, λ_i is the singular value.
Step 6- Quantify the norm based on quantization step:

$$N = floor\,[\frac{Norm(V^\lambda)}{step}];$$

Step 7- Embed the watermark bit according to the following concept:

if (bit = = 1) and if ($floor\left(\frac{N}{2}\right) \sim= (\frac{N}{2})$) then $N' = N + 1$;
else $N' = N$;
else
if (bit= =0) and if ($floor\left(\frac{N}{2}\right) \sim= (\frac{N}{2})$)
then $N' = N$; else $N' = N + 1$;

Step 8- Calculate the norm of singular value matrix which has been updated:
$Norm(\overline{V^\lambda}) = (N' + 0.5) * step$;
Step 9- Calculate the singular value matrix which has been updated:
$\overline{V^\lambda} = V^\lambda * Norm(\overline{V^\lambda}) / Norm(V^\lambda)$;
Step 10- Calculate the new values of image blocks after the watermark bits have been embedded: $I'_g = UM_{\overline{V^\lambda}}V'$, where $M_{\overline{V^\lambda}}$ is the singular value matrix .
Step 11- Get the watermarked image after calculating all blocks. Calculate the value of Peak Signal to Noise Ratio (PSNR) between the watermarked and Host image. If the value is not between 40 and 50, then go to (4); else end.

The Watermark Extracting Scheme:
Step 1- Take the IDWT of the image data up to level two.
Step 2- Divide the sub bands except the lowest frequency one into blocks with 4×4, make SVD to each block, sort the singular values in descending order: $\lambda 1, \lambda 2, \lambda 3, \ldots\ldots \lambda r$;
Step 3- Get the norm of the singular matrix vector V^λ :

$$Norm(V^\lambda) = \sqrt{\sum_{i=1}^{r} \lambda_i^2}$$

Step 4- Calculate the value of quantization:

$$N = floor\,[\frac{Norm(V^\lambda)}{step}]$$

Step 5- Extract the watermark bit based upon the following rules:

If ($floor\left(\frac{N}{2}\right) == (\frac{N}{2})$) then bit = 1;
else bit = 0;

Step 6- Repeat above steps (2) to (4), until all the watermark bits are extracted.

The Watermark Embedding Scheme for second level:
The low frequency sub band from first level is again decomposed in 2nd level decomposition and hence we are left with four sub bands of 64x64 each. The idea is to pick 64x64 binary watermarks and divide it into four 32x32 size watermarks.
Consider the original watermark matrix, we are compartmenting [1:32, 1:32] of it, to be embedded in lowest frequency sub band of second level, then[1:32, 33:64] of it, to be embedded in to LH of second level, then [33:64, 1:32] of it, to be embedded in HL and finally [33:64, 33:64] of it, to be embedded in HH sub band of second level. Assigning the names, W1, W2, W3 and W4 to each watermark respectively.
Step 1- Let

$$s = \left(\sum_{i=0}^{nm-1} c_i\right)_{Mod2}$$

And $c_{min} = Min\{|c_i|\}$, where c_i is the coefficient in a2×2block.
If an input bit is 1 and s=1, then do nothing; otherwise, add the coefficient c_{min} to 1.
Else if input bit is 0 and s=0, then do nothing otherwise, subtract the coefficient. c_{min} from 1.

The Watermark Extracting Scheme for second level:

Step 1- Compute

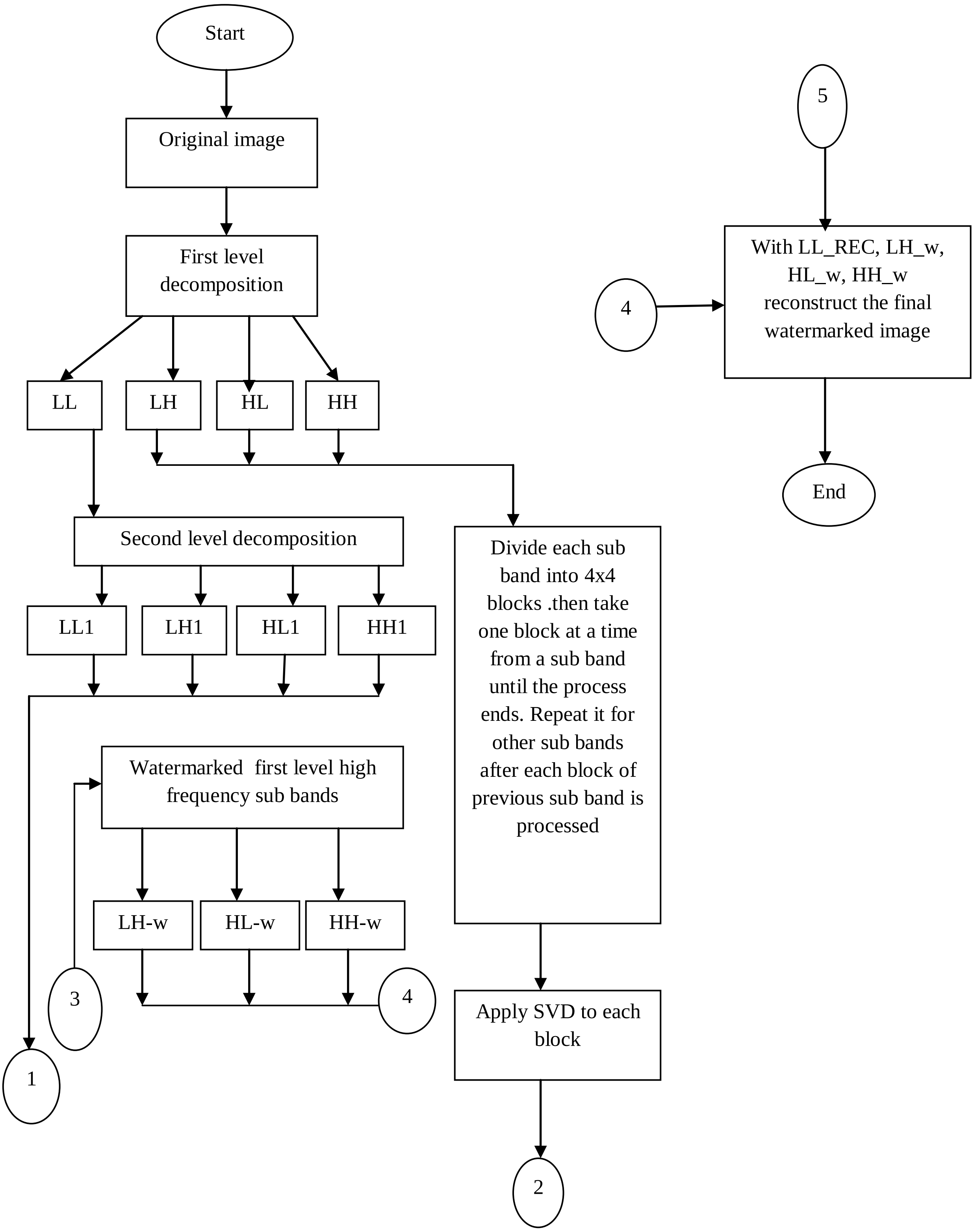
$$s^{i} = \left(\sum_{i=0}^{nm-1} c_j\right)_{Mod2}$$

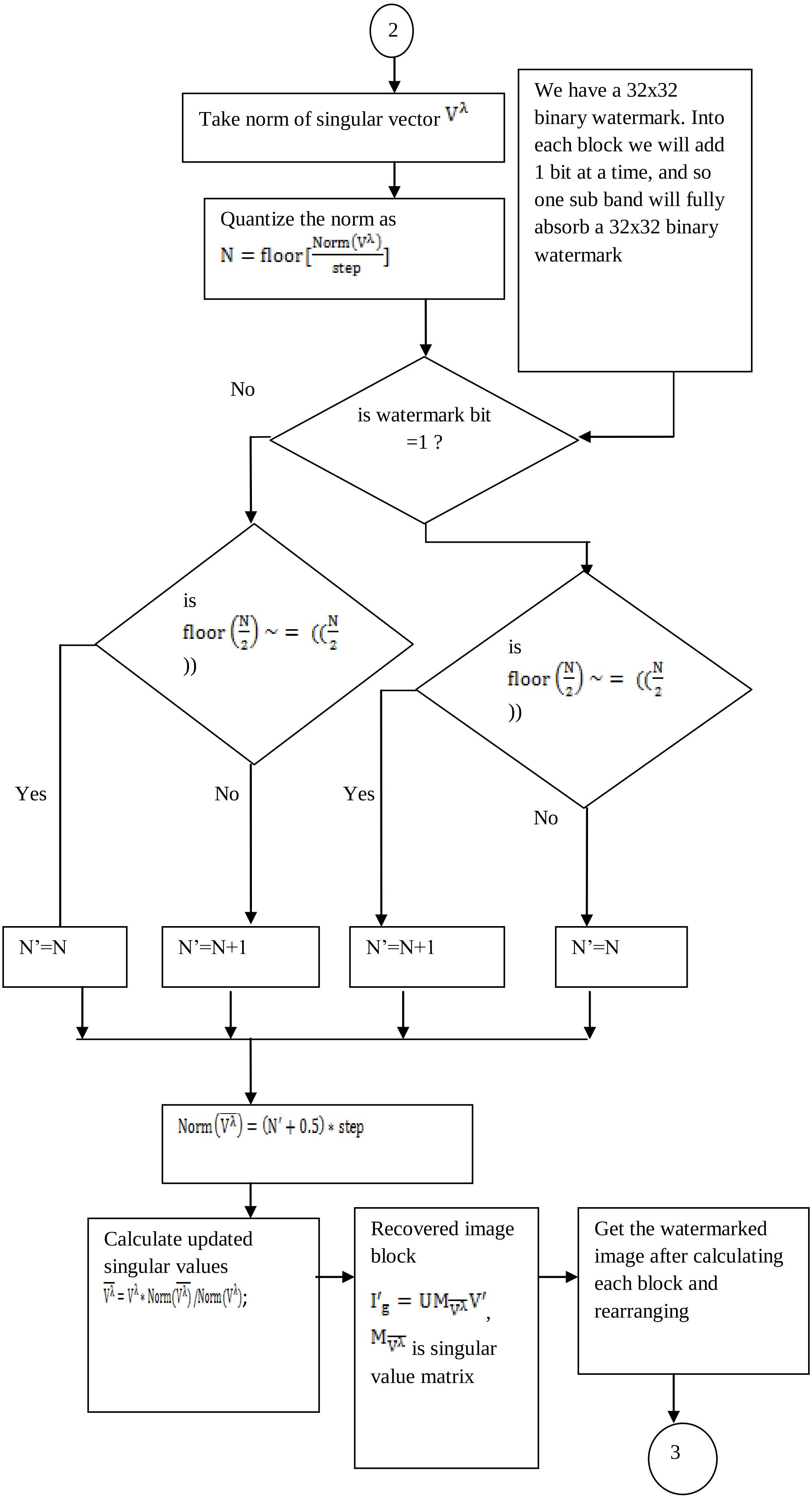
With c_j being the coefficients in a hidden block.

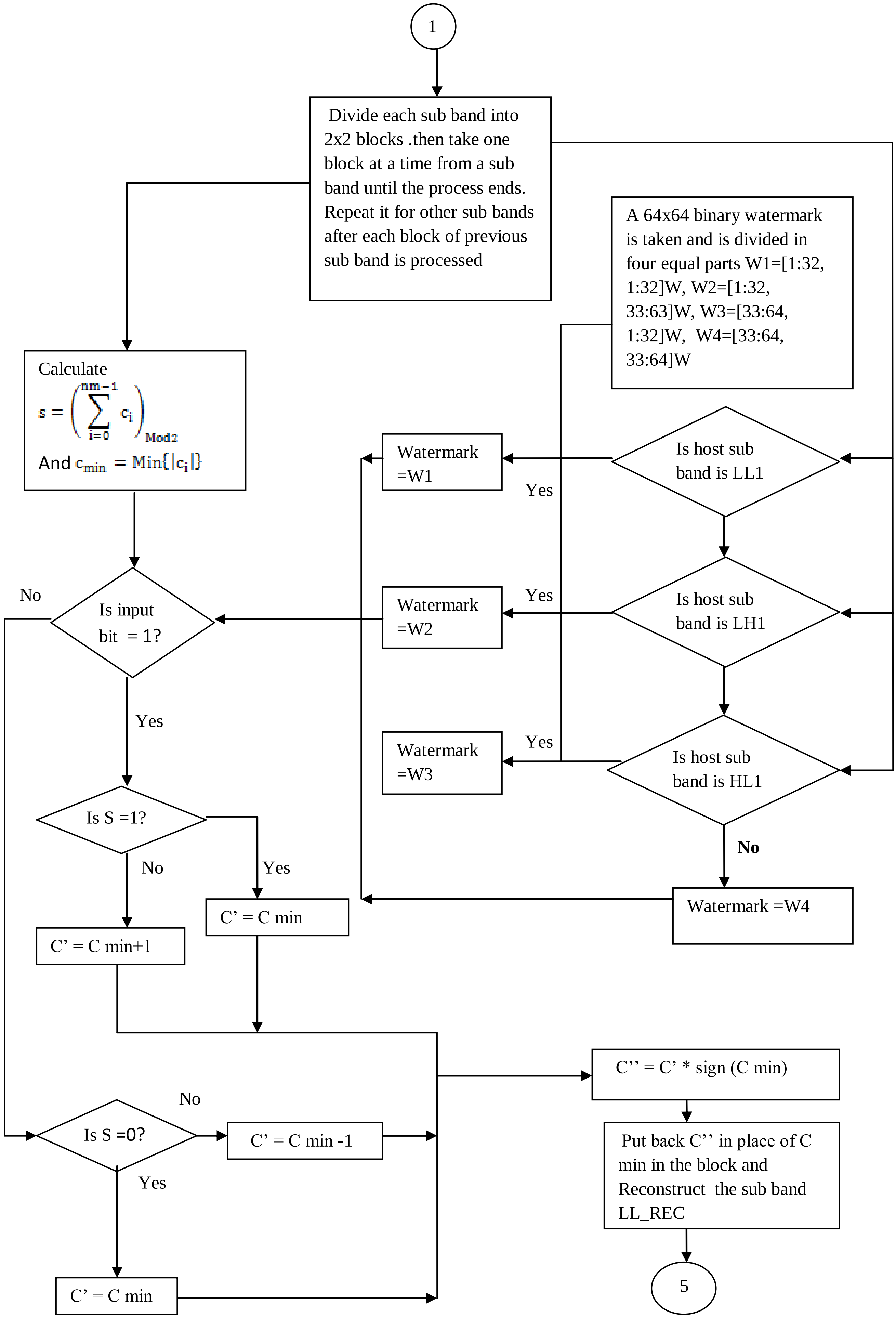
If s^{i}=1, then a data bit 1 is obtained else a data bit 0 is obtained.

The procedure is repeated until all data bits have been extracted and after we extract watermarks from each of the second level sub bands as W_1', W_2', W_3' *and* W_4' we de-compartmentalize them to get a final reconstructed watermark.

IV. FLOW CHART FOR THE PROPOSED APPROACH




2
Take norm of singular vector V^{λ}
We have a 32x32 binary watermark. Into each block we will add 1 bit at a time, and so one sub band will fully absorb a 32x32 binary watermark
Quantize the norm as $N = floor[\frac{Norm(V^{\lambda})}{step}]$
No
is watermark bit =1 ?
is $floor\left(\frac{N}{2}\right) \sim = ((\frac{N}{2}))$
is $floor\left(\frac{N}{2}\right) \sim = ((\frac{N}{2}))$
Yes
No
Yes
No
N'=N
N'=N+1
N'=N+1
N'=N
$Norm(\overline{V^{\lambda}}) = (N' + 0.5) * step$
Calculate updated singular values
$\overline{V^{\lambda}} = V^{\lambda} * Norm(\overline{V^{\lambda}}) / Norm(V^{\lambda});$
Recovered image block
$I'_g = UM_{\overline{V^{\lambda}}}V'$,
$M_{\overline{V^{\lambda}}}$ is singular value matrix
Get the watermarked image after calculating each block and rearranging
3


1
Divide each sub band into 2x2 blocks .then take one block at a time from a sub band until the process ends. Repeat it for other sub bands after each block of previous sub band is processed
A 64x64 binary watermark is taken and is divided in four equal parts W1=[1:32, 1:32]W, W2=[1:32, 33:63]W, W3=[33:64, 1:32]W, W4=[33:64, 33:64]W
Calculate
$s = \left(\sum_{i=0}^{nm-1} c_i\right)_{Mod2}$
And $c_{min} = Min\{|c_i|\}$
Is host sub band is LL1
Yes
Watermark =W1
Is host sub band is LH1
Yes
Watermark =W2
Is host sub band is HL1
Yes
Watermark =W3
No
Watermark =W4
Is input bit = 1?
No
Yes
Is S =1?
No
Yes
C' = C min+1
C' = C min
Is S =0?
No
C' = C min -1
Yes
C' = C min
C'' = C' * sign (C min)
Put back C'' in place of C min in the block and Reconstruct the sub band LL_REC
5

V. EXPERIMENTAL RESULTS

To explain the performance of proposed approach, the original image named as "Househill" of size 256X256 (fig 1(i)) and watermarking image named as "Mathworks" of size 64X64 (fig 1(ii)) was taken which was embedded in CA band after second level of decomposition (Chaotic scrambling was used to watermark the image at first level of decomposition). Fig 1(iii) shows the watermarked image. A high degree of robustness is achieved as there is no perceptual difference between the original and watermarked image. Fig. 1 (iv) shows the extracted watermark from first level of watermarking and fig 1(v) shows the watermark extracted from second level of watermarking.

(i) (ii) (iii) (iv) (v) (vi)

Fig 1. (a) original image (b) watermarking image (c) watermarked image (d) Extracted watermark from first level of watermarking (e) Extracted watermark from second level of watermarking (f) Extracted watermark ("mathworks" image) after Gaussian noise attack on watermarked image.

As a measure of the quality of watermarked image, the peak signal-to-noise ratio (PSNR) was used. To evaluate the robustness of proposed approach, the watermarked image was tested against Gaussian Noise attack. Correlation coefficient was used to compare the original and watermarked image. Some values between 0.05 and 20.0 were taken as the scale factor or step size. The results are shown in Tables I and II.

The tables I & II shows that as the value of step size are increased, the correlation and PSNR values between the original watermark and the extracted watermark from attacked images varies randomly and these values are very low. The effect of Gaussian noise attack on watermarked image can be seen in fig 1(vi) which shows the extracted watermark i.e. "Mathworks" image after the watermarked image was attacked by Gaussian noise.

The value of step size =15 can be taken to have good results. Higher value of step size increases the energy of the watermark. At the step size value above 30 the watermarked picture quality becomes poor and it can be easily determined by anyone that picture has some degraded perceptual quality

Table I Correlation Coefficient Values of Extracted Watermarks from Gaussian Noise Attack

S.NO.	Step size (α) or Scale Factor	Normalized Correlation Coefficient (CC) in Gaussian Attack
1	0.05	0.7174
2	1	0.7153
3	5	0.7186
4	10	0.7190
5	15	0.7149
6	20	0.7128

Table II PSNRr Values of Extracted Watermarks from Gaussian Noise Attack

S.NO.	Step size (α) 0r Scale Factor	PSNR Value
1	0.05	20.0820
2	1	20.1175
3	5	20.0904
4	10	20.1231
5	15	20.1214
6	20	20.1206

Similar experiments can be performed against other kinds of attacks, such as noising, rotation, cropping, denoising, average filtering, scaling, compression and others.

VI. CONCLUSIONS

The work is done on implementing the Integer Wavelet domain with Digital Watermarking. As wavelet has hierarchical nature so its multi resolution analysis helps to embed the watermark in n no. of levels. Watermark encryption before embedding gives added security to the algorithm and hence chaotic scrambling has proved to be a deserved answer to it.

Embedding watermark in Integer Wavelet Domain assures more reversibility of data than any other domain. As it maps integers to integers so adding binary watermark to IWT decomposed image comes in good compatibility. We have seen that increasing the step size increases the depth of watermark embedding and so its energy to withstand regular signal processing attacks. But the method gives bad response against Gaussian Noise attack as the values of correlation coefficients is very low at different step size. So the procedure requires improvements in this regard.

REFERENCES

[1] Mei Jiansheng, Li sukang and Tan xiaomei, "*Digital Watermarking Algorithm based on DCT and DWT* ," Nanchang power supply company and Nanchang institute of technology", Nanchang, China 2009

[2] Emir Ganic and Ahmet M. Eskicioglu, "*Robust Embedding of Visual Watermarks using DWT-SVD*" , Journal of Electronic Imaging, Volume 14, issue 2

[3] Mohammad Ibrahim Khan, Md. Maklachur Rahman and Md. Iqbal Hasan Sarker, "*Digital Watermarking for Image Authentication on Combined DCT, DWT and SVD transformation*", 2013

[4] Chih-Chin Lai, Member, IEEE, and Cheng-Chih Tsai, "*Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition*" IEEE Transaction on Instrumentation and Measurement, Vol. 59, No. 11, November 2010

[5] Huang Hui-fen, "*Digital Watermarking Algorithm Based on DWT and Chaotic Scrambling*", In Proc, of 14th Youth Conference on Communication, 2009