Effect of Attacks on Dwt Based Spatial Image Watermarking

Manisha Bhardwaj [1], Er. Shaveta Sehgal S[2]
[1, 2] Dept of Computer Science Engineering
[1, 2] Asra College of Engineering and Technology, Bhawanigarh, Punjab

Abstract- *In this work, A DWT Arnold transform based robust watermarking technique is proposed which can use secret information from the same cover image whose data need to be hiding. In order to select the watermark, a cropping tool has been introduced which can allow the user to select the ROI from the host image which can further embedded in the cover image. To increase the security of the watermark, it is first scrambled through the use of Arnold transform. Then DWT is applied to watermark in which approximation coefficients are used as embedding bits as they contain the main content of the ROI. For embedding, cover image is divided into 8*8 non-overlapping blocks which are selected randomly for embedding. For each selected block, DWT is applied in order to get the first level detailed and approximation coefficients. Then absolute minimum rule is applied to select the coefficient places which are modified based on watermark bits. That approximation coefficient, which has least difference and is less than a chosen threshold, has been selected to embed the message. Two keys are generated in which first key notes the block number and second key notes the location of embedding bits. Many attacks has been applied on produced steago image and effective PSNR and NC values has been noted when performance evaluation has been carried out after watermark extraction.*

Keywords- compression, non-overlapping blocks, Arnold transform, PSNR, NC etc.

I. INTRODUCTION

Digital image watermarking is defined as the process to hide the information into host image, which is to be protected and extracted for copy right protection and its verification. There are two types of digital image watermarking schemes i.e. visible watermarking and invisible watermarking. The invisible watermarking requirements are imperceptibility and robustness. Similarly the requirements of visible watermarking should be visible that means easy to identify the hiding data [1]. Now a day the internet plays very important role in the human life. It is very useful for easy to share the data information in different forms like images, audio, & video. Due to this problem of security and authentication of digital information to provide sufficient security for multimedia information while providing protection against various forms of forgery in an efficient manner with respect to speed of verification process [1]. Two categories of digital watermarking algorithms are spatial domain (time domain) techniques & frequency domain techniques. The best example of spatial domain technique is LSB (least significant bit) which is directly perform the operation and modify the pixels. The frequency domain techniques transform the image into set of coefficients i.e. to perform operation on transform coefficients. The frequency domain techniques are DCT (Discrete cosine transform) DWT (Discrete Wavelet Transform), SVD (Singular Value Decomposition) etc. The frequency domain based watermarking is known as more robust and imperceptions (invisible) than background.

II. LITERATURE SURVEY

Digital watermarking can be categorized into fragile and robust watermarking based on the applications concerned. Generally, fragile watermarking can be used for authentication of the digital data and to further validate the integrity of the contents [2]. In contrast, the robust watermarking can be used for copyright protection purposes and therefore the presence of the watermark should be verified not only against common signal processing distortions but also against compression, geometric and counterfeit attacks [3]. Recently, numerous robust watermarking techniques have been proposed in the literature, where the majority of techniques are utilizing the transform domain representation for the watermarking. Generally, these techniques employs invertible transformations such as discrete Fourier transform (DFT), discrete cosine transform (DCT), discrete wavelet transform (DWT), singular value decomposition (SVD) and other transforms to embed the watermark [4][5]. Among these, wavelet based techniques get more attention because they enables to provide the description of a signal in different level of resolution. Another large group of techniques utilize the embedding directly in the spatial domain [6][7]. These techniques are simple when compared to the transform domain watermarking. However, these are having very limited robustness and hence cannot survive against majority of signal processing and geometric attacks. The transform domain techniques are more robust, which is due to the fact that the watermark is disseminated irregularly over the image pixels after the inverse transform, thus making manipulation and detection of the watermark more difficult for an attacker. Recently, a stochastic resonance (SR)-based watermarking technique is proposed [8]. The central idea of this technique is that the watermarking involves detecting weak signals (watermarks) in the presence of strong background interference (the intentional and unintentional distortions) and therefore the stochastic resonance is used to optimize the watermark extraction. Thereafter, a variety of watermarking schemes are proposed combining stochastic resonance with different existing philosophies [9]. In [9], a watermarking process for binary pulse amplitude modulation signals is proposed where underlying signal processor is based on aperiodic stochastic resonance. A more efficient watermarking technique based on dynamic stochastic resonance has been proposed in [10]. In the former technique, the watermark is embedded based on the pseudo random binary sequence in discrete cosine domain whereas a combination of multi-level wavelet and discrete cosine domain is used in the later. In both the cases, the extraction is done by the dynamic stochastic resonance. In [11], authors have combined the dynamic stochastic resonance with the singular value decomposition for the watermarking. The main drawback of these techniques is that they are having limited robustness. The technique in [11] is robust against a variety of distortions when compare to others but it suffers with the false positive problem. This is mainly due to the fact that only the singular values of the watermark are embedded into the host image, and one can extract an estimate of watermark from the host image using the singular vectors of non-existent watermark. This situation normally leads to the ambiguous state [12].

III. SYSTEM MODULE

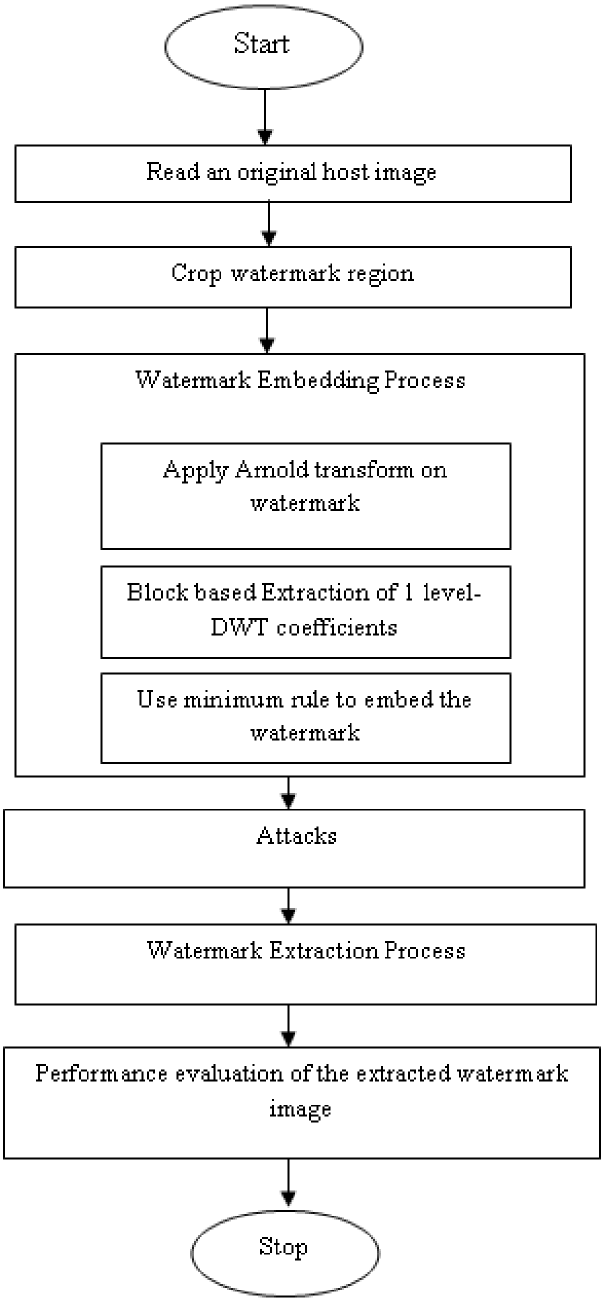

Start
Read an original host image
Crop watermark region
Watermark Embedding Process
Apply Arnold transform on watermark
Block based Extraction of 1 level-DWT coefficients
Use minimum rule to embed the watermark
Attacks
Watermark Extraction Process
Performance evaluation of the extracted watermark image
Stop

Figure 1: Overall Architecture

Proposed system uses discrete wavelet transform to decompose the image so that datacan be hide in approximation coefficients. To make it robust from attacks and to secure secrte information, Arnold transform has been used. The techniques used are briefed as below

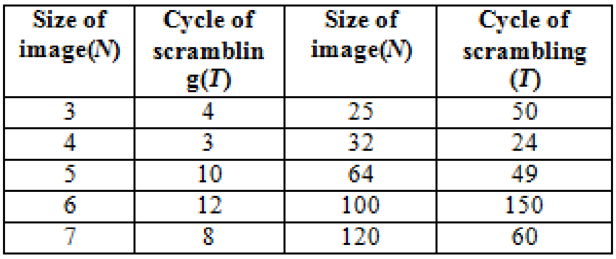
A. Discrete wavelet transform

Discrete wavelet transform is a mathematical tool, used to decompose a function into a set of basic functions called wavelets. Wavelets are created by translation and dilation of a fixed function, called the mother wavelet. Wavelet provides frequency as well as time information of a function. Wavelet transforms are able to provide multi resolution analysis of digital images. This transform is used to overcome the drawbacks of exists basic image like Fourier transform, short term Fourier transform, Fourier series etc with the functionality of scaling & wavelet concept. By using DWT the image is transformed into sub bands (like LL, LH, HL & HH). This is the first level discrete wavelet transform. The second level process the LL band is decomposed into (LL1, LH1, HL1 &HH1). Continuing the process up to nth level a pyramid is obtained [1].

B. Arnold Transform Based Digital Image Scrambling

The digital image can be seen as a two-dimensional matrix. When the size of the image is N, then I have N × N elements, the subscript x, y stand for the position of pixel, x, y ∈ {0, 1, 2..., N-1}. Let x, y corresponds to the x, y of Arnold scrambling, for each pair x, y, after all do Arnold scrambling, become x' and y', which equivalent to the original image of the point from (x, y) move to the = (x ', y'), so realized the movement of pixels in the image, the image with Arnold scrambling traverse all the points to complete a picture of Arnold scrambling. The cycle of Arnold scrambling is relate to the size of the image, but not directly proportional. If size is 128 × 128 pixel image of Arnold scrambling cycle is 96, size 240 × 240 pixel image of Arnold scrambling for 60 cycles. Table 1 shows the relationship between different N values and the cycle T of Arnold scrambling.

Table 1: Arnold scrambling algorithm cycle



Size of image(*N*)	Cycle of scramblin g(*T*)	Size of image(*N*)	Cycle of scrambling (*T*)
3	4	25	50
4	3	32	24
5	10	64	49
6	12	100	150
7	8	120	60

C. Scrambling Recovery in Arnold Scrambling Algorithm

Arnold scrambling recovery has two ways: one is the application of its periodicity, and the other is the pursuit of its inverse matrix to the inverse transformation [13]. It is very natural to leverage the periodicity of Arnold scrambling method. By research of it before, we can come to this conclusion: For the digital image of N × N pixels, as long as meet non-1 positive integer N, The Arnold scrambling has periodicity. Extend to an arbitrary Scrambling time of n, you need to proceed (m^{N-n} mod m^N) times Arnold scrambling transformation. However, the times of scrambling are relate to the order of N, in general, if N is the number of higher-order cases, the cycle is relatively long.

D. Algorithm used

Steps in the watermark embedding process

The steps of watermark embedding have been briefed as follows:

1. Read the cover image which needs to be watermarked and select a region of interest (ROI) for self-embedding process in which $R_1 \, and \, C_1$ is the number of rows and columns of the ROI region.
2. Apply discrete wavelet transform to the cropped watermark image by selecting first level of decomposition. DWT decomposition gives three detailed coefficients named as vertical, horizontal and diagonal coefficients and one approximation coefficients
3. Select the approximation sub band coefficients apply Arnold transform for 10 times to get the scrambled matrix A_s in order to secure the information in secret watermark which need to be embed in cover image
4. Convert the matrix A_s into a one dimensional array $Watermark_j = [e_1, e_2, . . ., e_M]$, where $sizeM = (R_1 \times C_1 / 4)$ is the number of components to be embedded.
5. Divide the Cover image into blocks B_i of size 8*8 where i = 1, 2,…,N and N is the number of blocks. Each component ($Watermark_j$) of Watermark matrix is embedded into a selected block of the image. Selecting the block is explained in next step.
6. Initially loop parameter i is set to one. Comparison is started from the first in which selected block B_i has been scrambled using Arnold transform to get the scrambled block ($Block_{scrambled}$).
7. Then, first level discrete wavelet transform is applied on the block $Block_{scrambled}$. Then approximation coefficients are extracted of size 4 × 4 and convert into 1 × 16 array $Array_i$ and Then absolute distance is taken between $watermark_j$ and coefficients of $Array_i$, giving a new array.
8. In this step, minimum value $Value_{\min}$ and its position $Position_{\min}$ in the resultant array has been evaluate as defined

by formula $[Value_{\min}, Position_{\min}]$ = min (abs($Array_i - Watermark_j$)),. If there are several identical minimum values, the first one found is chosen. If the minimum value $Value_{\min}$ is smaller than a threshold value Thresh, go to the next step. Otherwise, set i = i + 1 and go back to step 6.

9. Selection of the coefficients located in $Position_{\min}$ of the array $Array_i$ .is carried out in this step. This coefficient has the least difference with the component $Watermark_j$. In other words, it is the nearest to $Watermark_j$. The location of the selected coefficient and that of the block $Block_{scrambled}$ are saved as keys Key_2 and Key_1, respectively by putting them in two columns of same key.

10. Then Replacement of the selected coefficient of the block is carried out with $Watermark_j$, giving the embedded block for watermarked image.

11. Then inverse discreet wavelet transform is applied to the embedded block to obtain the scrambled watermarked block $Block_{scrambled\ watermark}$

12. Then implementation of Arnold transform is done for $(f - 10)$ times on the scrambled watermarked block in which f is the Arnold transform period of the block.

13. When all the elements of $Watermark_j$ are embedded, the watermarked image $\mathrm{Im}\,age_{watermarked}$ is produced.

In order to embed the next components of W, the already embedded blocks is not considered in the comparison procedure in previous work which results in decrease in embedding capacity but in proposed work , we have ignored that location in the block which has been used previously hence using the same block for next embedding as threshold is the only parameter to slip a block. It results in more ROI that can be embedded. The extraction process is reverse of the embedding process.

V. RESULTS AND DISCUSSIONS

Watermarking algorithms are generally grouped into spatial and frequency domain algorithm. Although spatial algorithms have low complexity and they are easy to implement, they can embed little information and they are not robust against attacks and common signal processing operations. The frequency domain that is similar to spread spectrum communication embeds the watermark by modification of the magnitude coefficient of the digital content according to the embedding algorithm.

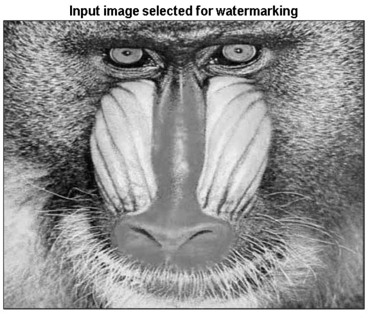


Figure 2: Baboon Image selected as host image for watermarking

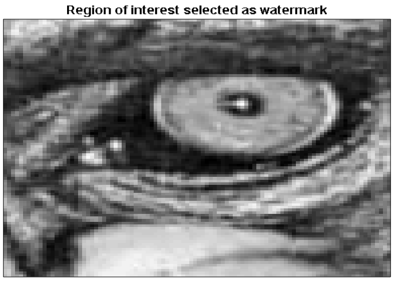


Figure 3: Region of interest cropped from the host image as secret information

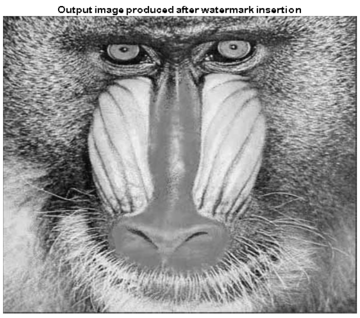
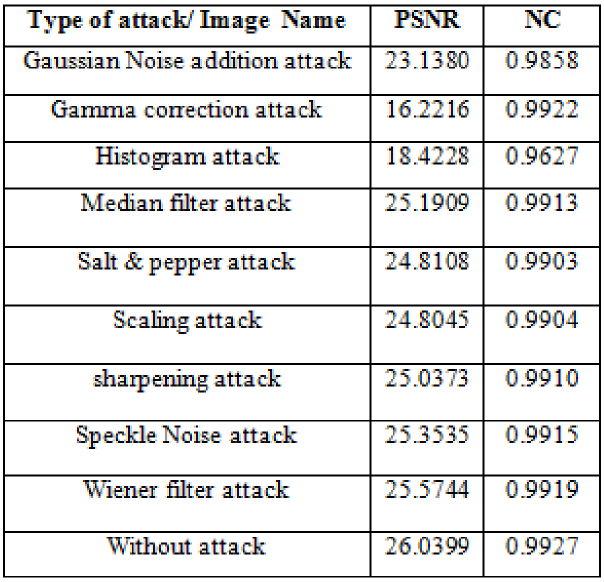


Figure 4: Output image produced after watermark insertion

The results for quality assessment has been given below

Table 2: PSNR and NC values at different attacks for Baboon image



Type of attack/ Image Name	PSNR	NC
Gaussian Noise addition attack	23.1380	0.9858
Gamma correction attack	16.2216	0.9922
Histogram attack	18.4228	0.9627
Median filter attack	25.1909	0.9913
Salt & pepper attack	24.8108	0.9903
Scaling attack	24.8045	0.9904
sharpening attack	25.0373	0.9910
Speckle Noise attack	25.3535	0.9915
Wiener filter attack	25.5744	0.9919
Without attack	26.0399	0.9927

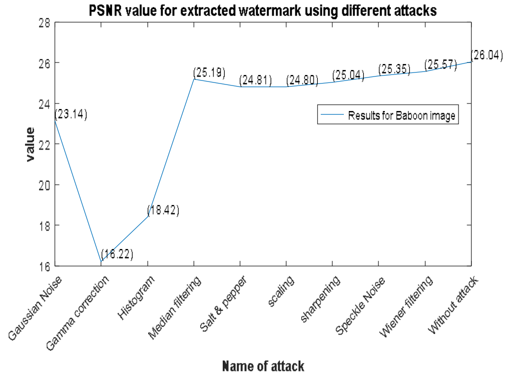


Figure 5: PSNR value of extracted watermark using applied attacks on Baboon

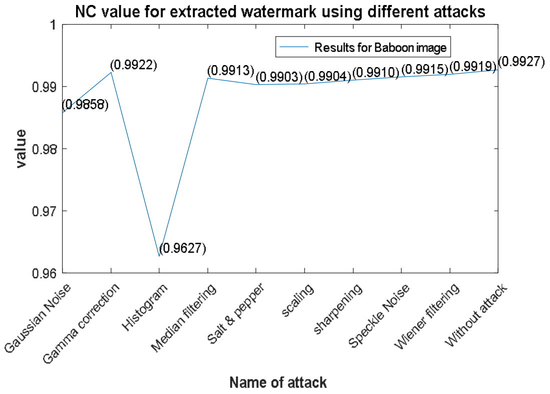


Figure 6: NC value of extracted watermark using applied attacks on Baboon image

V. CONCLUSION

Wavelet Transform has been used in this work to decompose host image. The low frequency of cover image decomposed coefficients has been proposed for embedding watermarking contents. The PSNR is high in this paper with resisting many kinds of attacks which indicates embedded image has a great quality without serious distortion. Minimum Absolute difference between watermark and cover block approximation coefficients has been adopted in this work for detection and extraction of watermarking information, which has advantages of efficient and easy for implementation of watermarking detection and extraction proceeding. In addition, we have provided a great deal of practical experience and cropping ROI based idea for watermarking research in which user oriented ROI can be selected from the host image as secret information. The experimental results show that the proposed scheme preserves not only the high perceptual quality, but also is robust against various attacks. This performance is verified by the extracted watermark results, which demonstrate that the algorithm can maintain the quality of the watermarked image after embedding. The PSNR and NCvalues of image quality measurement also confirm this result.

REFERENCES

[1] Maruturi Haribabu, Ch.Hima Bindu, K.Veera swamy,"A Secure & Invisible Image Watermarking Scheme Based on Wavelet Transform in HSI color space." published in 6th International Conference On Advances In Computing & Communications, ICACC 2016, 6-8 September 2016, Cochin, India

[2] S. Ababneh, R. Ansari, A. Khokhar, Iterative compensation schemes for multimedia content authentication, J. Vis. Commun. Image Represent. 20 (5) (2005) 303–311.

[3] F.Y. Shih, Y.T. Wu, Robust watermarking and compression for medical images based on genetic algorithms, Inf. Sci. 175 (3), 2005, 200–216.

[4] W. Wu, Z. Lin, SVD-based self-embedding image authentication scheme using quick response code features, J. Vis. Commun. Image Represent. 38 (2016) 18–28.

[5] X. Qi, X. Xin, A singular-value-based semi-fragile watermarking scheme for image content authentication with tamper localization, J. Vis. Commun. Image Represent. 30 (2015) 312–327.

[6] K. Choi, C. Pun, Robust lossless digital watermarking using integer transform with Bit plane manipulation, Multimedia Tools Appl. 75 (11) (2016) 6621–6645.

[7] A.M. Abdelhakim, H.I. Saleh, A.M. Nassar, A quality guaranteed robust image watermarking optimization with

Artificial Bee Colony, Expert Syst. Appl. 72 (2017) 317–326.

[8] G. Wu, Z. Qiu, A novel watermarking scheme based on stochastic resonance, in: Proceedings of IEEE 8th International Conference on Signal Processing, vol. 2, 2006, pp. 1–4.

[9] S. Sun, B. Lei, An aperiodic stochastic resonance signal processor and its application in digital watermarking, Signal Process. 88 (8) (2008) 2085–2094.

[10] R.K. Jha, R. Chouhan, P.K. Biswas, K. Aizawa, Dynamic stochastic resonance-based improved logo extraction in discrete cosine transform domain, Comput. Electrical Eng. 40 (6) (2014) 1917–1929.

[11] R. Chouhan, R.K. Jha, A. Chaturvedi, T. Yamasaki, K. Aizawa, Robust watermark extraction using SVD-based dynamic stochastic resonance, in: Proceedings of IEEE International Conference on Image Processing, 2011, pp. 2745–2748.

[12] Y. Wu, On the security of an SVD-based ownership watermarking, IEEE Trans. Multimedia 7 (4) (2005) 624–627. [923] S. Tao, W. Ruli, Y. Yixun, Generating

[13] Wang Lulu, Zhang Chong.: Arnold Scrambling Based On Digital Image Encryption Technique. J. National Defense Technology Base. 10, (2010)