Security and Watermarking of Color Images

Piyush .V. Gattani
Department of Computer Science and Engineering
Shri Ramdeobaba College of Engineering and Management
Nagpur, India
pgattani98@gmail.com

Dr. C. S. Warnekar
Principal (Former) Cummins College Pune
Sr. Prof Department of Computer Science and Engineering
Jhulelal Institute of Technology
Nagpur, India
cswarnekar@gmail.com

***Abstract*:** The burgeoning information transactions in the cyber world have necessitated the need of research aimed at developing different ways to secure the communication of digital multimedia documents like text, images, audio, and video; as they could be easily accessed, manipulated or tampered. A digital watermark is certain digital signal or a pattern embedded into the host document, such as an image or audio or video with a view to protect it.

This paper suggests a new invisible digital watermarking scheme for color images based on the amalgamation of wavelet transform (SWT2) with singular value decomposition (SVD), and advanced encryption scheme (AES). In this new approach, standard watermark is embedded into the three color channels (R, G, B) of the host image in order to increase the robustness of the watermark. The proposed method embeds the watermark without affecting the visual quality of the host document and also allows for reasonable compromise between robustness and invisibility of watermark. This research is an extension of our earlier work on gray-scale image to embed a color watermark into a color host based on the singular vector domain for all channels of RGB color space.

Keywords- *Digital Water Mark (DWM), Wavelet Transform SWT2, SVD, AES, PSNR, Gaussian, Histogram, Median, Average,*

*****

I. INTRODUCTION

A digital watermark is a digital signal or a pattern embedded into the host media to be protected, such as an image or audio or video file. There has been a phenomenal increase in the use and circulation of information in digital multimedia formats for various purposes. The paintings, photographs, newspapers, books, music etc., are available over the internet in multimedia format. The increasing necessity to protect the intellectual property rights of such digital content has led to considerable research in the area of Digital Watermarking

Digital watermark contains useful certifiable information for the owner of the host media, such as producer's name, company logo, etc. Digital watermark has two properties; first is Imperception and second is Robustness. Imperception deals with the visual quality of the host image and Robustness deals with the image distortions part. In other words, Imperception property provides perceptuality of the image and Robustness property provides a protection to the image against various common image processing operations like cropping, resize, image compression etc

. The image compression is classified into two categories: spatial domain and transform domain techniques. . In spatial domain technique the watermark embedding is achieved by directly modifying the pixel values of the host image. In transform domain technique the host image is first converted into frequency domain by transformation method such as the discrete cosine transform (DCT), discrete Fourier transform (DFT) or discreet wavelet transform (DWT) ,etc . then, transform domain coefficients are altered by the watermark. The inverse transform is finally applied in order to obtain the watermarked image. The frequency domain methods allow an image to be broken up into different frequency bands. Embedding the watermark in the low frequency increases the robustness with respect to image distortions. The high frequency band of an image is more prone to dropping due to quantization and it will be lost by compression or scaling attacks. The middle frequencies embedding of the watermark avoid the most visual important parts of the image and it is robust to compression and noise attacks; however it is less robust to low-pass filter.

II. PROPERTIES OF WATERMARKING

A. Imperceptibility

The watermark embedding should cause as little degradation to the host image. In other words, if we cannot distinguish between host image and the watermarked image called as imperceptibility.

B. Robustness

The watermark must be robust to common signal processing manipulations and attempts to remove or impair the watermark. In other words, if it is difficult to remove or destroy watermark from watermarked image then it is said to be robust.

C. Security

The embedded information must be secured against tampering via different attacks.

D. Capacity

The amount of embedded information must be large enough to uniquely identify the owner of the image.

III. DOMAINS OF WATERMARK

A. *Spatial Domain*

The Watermark embedding is achieved by directly modifying the (LSB of) pixel values of the host image.

B. *Transform Domain*

The host image is first transformed to frequency domain using say Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discreet Wavelet Transform (DWT) or Singular Vector Domain (SVD) etc. Then the Watermark is embedded in the coefficients of transform function. In Transform Domain, the transform techniques help in locating the most Significant Portion of the Host Image.

A cursory survey of the work done so far in the related areas is given in the sequel.

Miyara et al. [13] proposed a new digital watermarking method of three bands RGB color images based on PCA. This consists of embedding the same digital watermark into three RGB channels of the color image based on PCA Eigen-images. Piva et al. [14] introduced another color image watermarking scheme based on the cross-correlation of RGB-channels. Here DCT transformation is first performed separately on each color channel. A set of coefficients is then selected from each color channel, which is used to embed the watermark by modifying these coefficients. Zhang and Du [4] proposed an algorithm based on the RGB color space. They proposed to embed color watermark into a color host image. It fully uses he characteristics of HVS, fulfills the self-adaptive embedding of watermarking, and balances the imperceptions and robustness. Cheng et al. [10] proposed algorithm based on embedding the watermark image three times in different frequency bands that are low, medium and high; result of that the watermark can not be totally destroyed by either low pass, medium or high pass filter. The concept of using more than one watermark has also been suggested by Raval and Rege [11], in which multiple watermarks are embedded in LL and HH bands after application of a DWT. Gorodetski et al. [12] used SVD domain for watermarking a RGB image by quantized the singular value of each channel. But, this is shown to resist only for JPEG compression.

IV. METHODS USED

Considering the aforesaid points, a new invisible digital watermarking scheme for color images based on the amalgamation of wavelet transform (SWT2) with singular value decomposition (SVD), and advanced encryption scheme (AES) is suggested here. Details & results are presented below.

A. *SWT2:-*

It performs a multilevel 2-D stationary wavelet decomposition using a specific orthogonal wavelet decomposition filters.

Syntax:-SWC=swt2(X,N,'*wname*')
[A,H,V,D] = swt2(X,N,'*wname*')

Perform SWT decomposition of X at level 3 using sym4.
[ca,chd,cvd,cdd] = swt2(X,3,'sym4');

B. *SVD(Singular Value Decomposition):-*

The SVD is the optimal matrix decomposition in a least square sense that it packs the maximum signal energy into as few coefficients as possible . SVD is a stable and an effective method to split the system into a set of linearly independent components, each of them bearing own energy contribution

The SVD transform of a digital Image X of size MxN, with M≥N, is given by :

$$[X]^{N}_{M} = {}_{M}[U]^{M}\,[S]^{N}_{M}\,[V]^{N\,T}_{N}$$

$$U=[u_1, u_2, \ldots, u_m], \qquad V=[v_1, v_2, \ldots, v_n],$$

$$S=\begin{bmatrix}\sigma_1 & & & \\ & \sigma_2 & & \\ & & O & \\ & & & \sigma_n\end{bmatrix}$$

Fig. 1 Representation of SVD

Where U is an MxM orthogonal matrix, V is an NxN orthogonal matrix, and S is an MxN matrix with the diagonal elements represents the singular values.

The columns of the orthogonal matrix U are called the left singular vectors, and the columns of the orthogonal matrix V are called the right singular vectors. The left singular vectors (LSCs) of X are eigenvectors of XX^T and the right singular vectors (RSCs) of X are eigenvectors of X^TX. Each singular value (SV) specifies the luminance of an image layer while the corresponding pair of singular vectors (SCs) specifies the geometry of the image .

C. *AES(Advanced Encryption Scheme):-*

AES is based on a design principle known as a substitution-permutation network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. AES operates on a 4×4 column-major order matrix of bytes. The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext.

10 cycles of repetition for 128-bit keys,12 cycles of repetition for 192-bit keys,14 cycles of repetition for 256-bit keys.

Each round consists of several processing steps, each containing four similar but different stages, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

Description of the algorithm:

1. KeyExpansion—round keys are derived from the cipher key using Rijndael's key schedule. AES

 ISSN: 2321-8169
1465 – 1470

requires a separate 128-bit round key block for each round plus one more.

2. InitialRound
    1. `AddRoundKey`—each byte of the state is combined with a block of the round key using bitwise xor.
3. Rounds
    1. `SubBytes`—a non-linear substitution step where each byte is replaced with another according to a lookup table.
    2. `ShiftRows`—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
    3. `MixColumns`—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
    4. `AddRoundKey`
4. Final Round (no `MixColumns`)
    1. `SubBytes`
    2. `ShiftRows`
    3. `AddRoundKey`.

V. PROCEDURE IMPLEMENTED:

1) Take the Image and Watermark.

2) Apply SWT2 classical version of DWT to the image and the watermark, for getting HH, HL, LH, LL part of both the image and the watermark.

3) Apply SVD Singular Value Decomposition to both the LL part of image and the watermark.

4) Embed the watermark in the image with the help of scaling factor lamda. This lamda is multiplied with the singular matrix of watermark and get added to the singular matrix of the image.

5) Now we get the new singular matrix after the above operation and we get new embedded watermarked image. Apply AES Encryption to the Watermarked Image for providing security.

6) Apply Decryption at the receiving end and extract the watermark.

7) We can also apply different noise attacks at the time of decryption.

8) Now calculate the PSNR and normal cross co-relation values.

9) Compare the extracted watermark with the standard watermark through psnr values. If the values of the psnr of the standard watermark are same with the extracted one then the transaction is safe, otherwise the transaction is manipulated.

VI. EXPERIMENTAL RESULTS

Fig..2 For gray images

FOR GRAY IMAGES:

Table 1. For Gray Image:- where lamda value=0.20

Sr.no	Host	Watermark	Attack	Embedding time(min)apox	Extraction time(min)apox	Psnr value(db)	Normalized corelation
1	Lena	Parrot	No attack	2.5	2.5	52.4478	0.9999
2	Lena	Parrot	Histogram	2.5	2.5	11.4657	0.8123
3	Lena	Parrot	Gaussian	2.5	2.5	22.2462	0.9015
4	Lena	Parrot	Median	2.5	2.5	29.6711	0.9784
5	Lena	Parrot	Average	2.5	2.5	22.7924	0.8941

 ISSN: 2321-8169
1465 – 1470

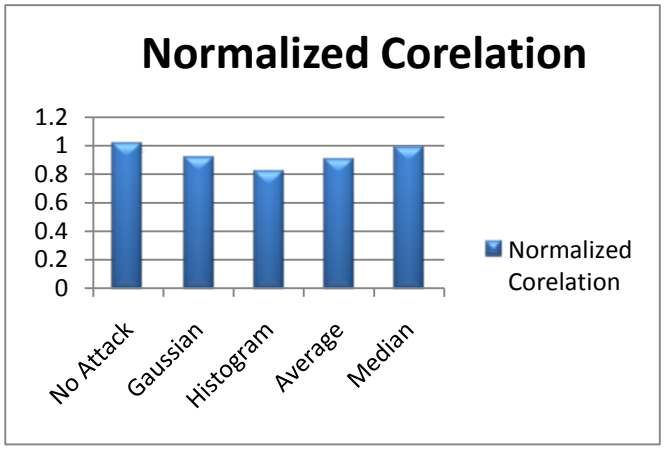

Fig.3 Normalized Corelation values of attacks on gray image

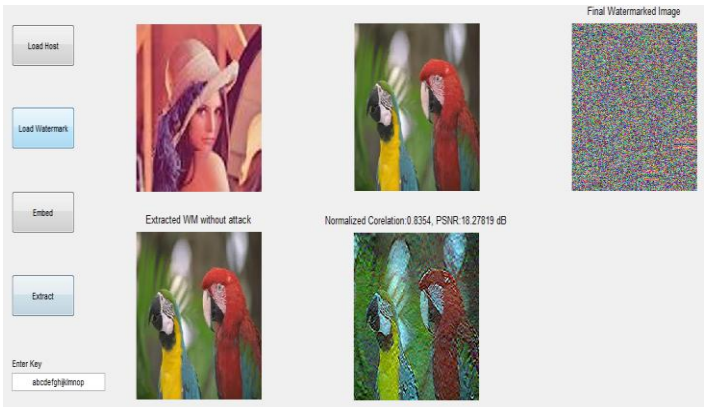

Fig..4 For Color Images:

Table 2. For Color Image:- where lamda value=0.20

Sr.no	Host	Watermark	Attack	Embedding time(min)apox	Extraction time(min)apox	Psnr value(db)	Normalized corelation
1	Lena	Parrot	No attack	7.5	7.5	47.3893	0.9916
2	Lena	Parrot	Histogram	7.5	7.5	10.3148	0.6929
3	Lena	Parrot	Gaussian	7.5	7.5	18.2782	0.8354
4	Lena	Parrot	Median	7.5	7.5	29.0171	0.98
5	Lena	Parrot	Average	7.5	7.5	24.3119	0.9501

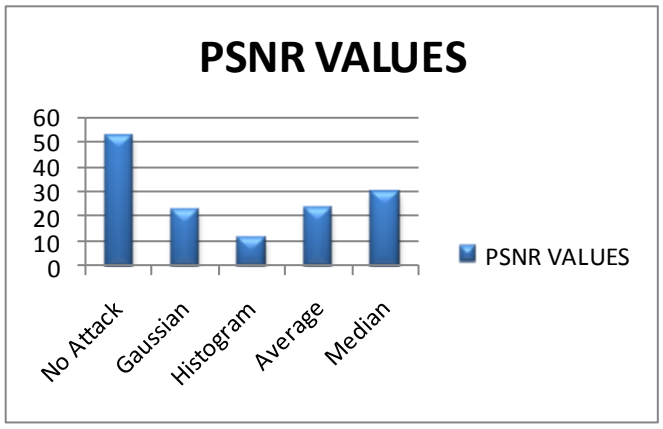

Fig. 5 Psnr values of attacks on gray image

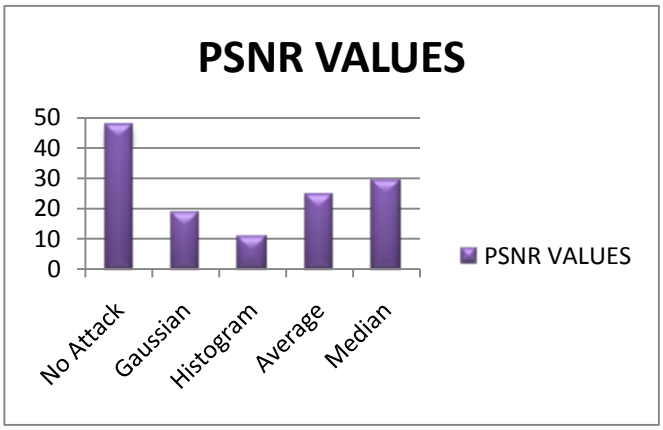

Fig. 6 Psnr values of attacks on Color image

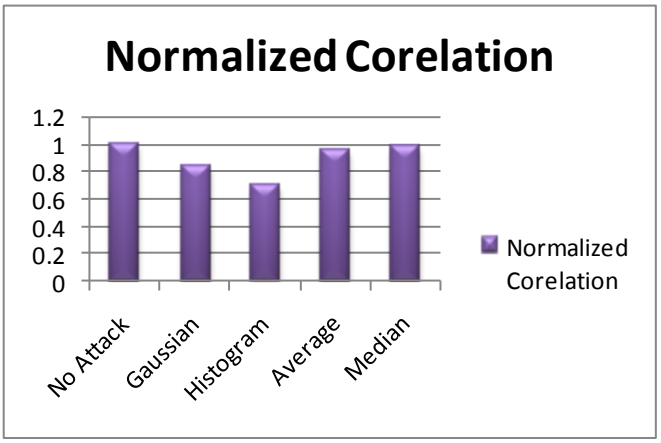

Fig. 7 Normalized Corelation values of attacks on Color image

VII. CONCLUSION :

The Procedure was applied to recognize the effect of AES encryption over the SVD transform of the image. From the above discussion it is clear that applying the swt2 technique via SVD reduces distortion and the AES ensures the security of the image.

VIII. FUTURE SCOPE :

To try some other techniques which can reduce the embedding and extracting time of the watermark.

ACKNOWLEDGMENT

I express my sincere gratitude to Dr. M. B. Chandak Sir, Head Department of CSE, for his valuable guidance and advice. Also I would like to thanks to my guide Dr.. C .S. Warnekar and the faculty members for their continuous support and encouragement.

REFERENCES

[1] R.Agrawal, M.S.Santhanam, K.Venugopalan on "Multichannel Digital Watermarking of Color Images Using SVD",,International Conference on Image Information Processing(ICIIP 2011).

[2] I.Nasir, Y.Weng, J.Jiang on "Novel Multiple Spatial Watermarking Technique in Color Images", 5th International Conference on Information Technology 2008.

[3] R.Agarwal , K.Venugopalan on "Digital Watermarking of Color Images in the singular Domain" ,IJCA Special Issue on "Computational Science – New Dimensions & Perspectives" NCCSE 2011.

[4] T.Zhang, Yi Du on "A Digital Watermarking Algorithm for Color Images Based on DCT" supported by the Innovation Program of Shanghai Municipal Education Commission.2009.

[5] R.Agarwal, M.S.Santhanam on "Digital Watermarking in the Singular Vector Domain" Physical Research Laboratory, Navrangpura, Ahemdabad 2006.

[6] M.Kamlakar, C.Gosavi, A.Patankar on " Single Channel Watermarking for Video using Block Based SVD" International Journal of Advances in Computing and Information Researches.ISSN:2277-4068,Volume1-no.2,April 2012.

[7] C.Jain, S.Arora, P.Panigrahi on"A Reliable SVD based Watermarking Scheme" (IISER) Kolkata.

[8] C.Gosavi, Dr. C.S.Warnekar "Study of Multimedia Watermarking Techniques" (IJCSIS) Internatinal Journal of Computer Scince & Imformation Security, Vol.8, No.5, August 2010.

[9] Eric Tyler Hansen "Analysis of the singular value decomposition in data hiding" Iowa State University Ames, Iowa 2007.

[10] L. M. Cheng, L. L. Cheng, C. K. Chan, and K. W. Ng, "Digital watermarking based on frequency random position insertion," Presented at Control, Automation, Robotics and Vision Conference, vol. 2, pp. 977-982(2004).

[11] M. S. Raval and P. P. Rege, "Discrete wavelet transform based multiple watermarking scheme," Int. Conference on Convergent Technologies for Asia-Pacific Region, vol. 3, pp. 935-938 (2003).

[12] V. I. Gorodetski, L. J. Popyack, V. Samoilov, and V. A. Skormin, "SVDbased Approach to Transparent Embedding Data into Digital Images," International Workshop on Mathematical Methods, Models and Architectures for Computer Network Security (MMM-ACNS 2001), pp. 21- 23 (2001).

[13] K. Miyara, T. Hien, H. Harrak, Y. Nagata, and Z. Nakao, "Multichannel color image watermarking using PCA eigenimages," Advances in Soft Computing, Springer-Verlag, vol. 5, pp. 287-296, 2006.

[14] A. Piva, F. Bartonlini, V. Cappellini, and M. Barnni, "Exploiting the cross- correlation of RGB-channels for robust watermarking of color image," Proceedings of the IEEE International Conference on ImageProcessing, vol. 1,pp. 306-310 (1999).