Volume 5 Issue I, January 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Prevention of Geometric Attacks Using Image Watermarking Technique

Mr. K. Balasamy AP/IT[1], C. V. Swarnalakshmi[2], M. Aarthisri[3]
Information Technology Dr. Mhalingam College of Engineering Technology

Abstract: ***In this paper, a robust image watermarking algorithm which was based on singular value decomposition (SVD) and discrete wavelet transform (DWT) was proposed and simulated for protecting real property rights. To obtain this we divide the host image into four non- overlapping sub bands called sub images and then watermark is embedded in that sub images. Its embedding algorithm hide a watermark in sub-band blocks in the low–low (LL), low-high(LH), high-low(HL) and high-high (HH) sub-bands of a target non-overlapping block of the host image by modifying singular values (SVs) on SVD version of these blocks. The watermark extraction algorithm was designed to estimate the original coefficients. Then we will verify for various geometric and Gaussian attacks such as translation, scaling, reflection, noise, mean, median etc., and finally we will extract the attacked image and water marked image separately and will check for its robustness. Experimental results showed that the proposed scheme made significant improvements in terms of both transparency and robustness and was superior to the existing methods which were considered in this paper.***

I. INTRODUCTION

Image watermarking is an efficient solution for authentication and copyright protection of images in popular communication environments like Internet, which is susceptible to illegal usages. The basic procedure of image watermarking is to hide some data along with the cover image. Thus, the ownership or copyright of the multimedia can be provided by using the watermarked image. The most important properties of an efficient watermarking algorithm are imperceptibility (i.e., no visual difference between original and watermarked image) and robustness against various image manipulations called attack. The main attacks can be categorized as: (1) signal processing like JPEG compression, various types of noise, filtering, and blurring, etc; and (2) geometric attacks like rotation, scaling, cropping, translation ,and affine transformation, etc. In case, if image watermarking is performed in spatial or signal domains it can be done by watermarking by directly altering pixels ,leads to easy and low-cost implementation. Although the spatial domain schemes are not robust to affine transformations the signal processing attacks. Compared to the spatial domain, transform domain schemes, such as discrete wavelet transforms (DWT) , discrete cosine transforms (DCT) , and singular value decomposition (SVD) are more robust, especially against the signal processing attacks. This is due to the reality that watermark is embedded by modifying transform coefficients and when the image is inverse transformed, the watermark is distributed irregularly over the image, reducing effect of many kinds of image manipulations. Moreover, other interesting specifications are: (1) localization of both special and frequency domain (in case of DWT), (2) employing a mathematical technique for extracting geometric characteristics from an image (in case of SVD), and (3) high-energy compaction and low-computation cost (in case of DCT).In addition, combining two or more transformations can enhance the performance of watermarking . The robust image watermarking approach applied here is based on a combination of two transform domains; DWT and SVD. The SVD-based watermarking is one of the most powerful watermarking schemes. In the literature, watermarking algorithms based on SVD insert the watermark in different ways. The simplest embedding scheme consists in adding the SVs of the watermark image by modifying the SVs of the host image. It performs two times of the SVD transformation during embedding phase and hides the watermark in the SVs of the SVD-domain image. Although this method performs well on transparency and robustness but it still has two weaknesses. First, the method needs highly computational complexity due to two times of SVD during the watermark-embedding phase. Second, it requires original images during the watermark-extraction phase. Thus, the hybrid DWT-SVD domain watermarking scheme considering the properties of human visual system (HVS). After decomposing the host image into four sub-bands in the DWT domain, they applied SVD to each sub-band and embedded SVs of the watermark in the sub-bands. Thus the robustness were achieved using these techniques.

II. EXISTING SYSTEM

A. Dwt

One of the main challenges of the watermarking problem is in obtaining a better trade off between robustness and perceptivity.

DWT is highly preferred, because it provides both simultaneous spatial localization and frequency spread of the watermark within the host image. By applying the DWT, an image is decomposed into four sub-bands. The most important part of the image resides in the LL sub-band that includes low frequency wavelet coefficients. Edges and details are usually in the high frequency sub-bands. DWT is superior to other translations due to the characteristics of multi-resolution and excellent image localization, similar to HVS.

B. Svd

The singular value decomposition of a matrix is a factorization of the matrix into a product of three matrices. Given an m×n matrix A, where m ≥ n, the SVD of A is defined as

$$A = U\Sigma V^{T} \quad ---[1]$$

where U is an m×n column-orthogonal matrix whose columns are referred to as left singular vectors; Σ =diag (σ1, σ2, . . . , σn) is an n×n diagonal matrix whose diagonal elements are nonnegative singular values arranged in descending order; V is an n×n orthogonal matrix whose columns are referred to as right singular vectors.

SVD efficiently represents intrinsic algebraic properties of an image, where singular values correspond to brightness of the image and singular vectors reflect geometry characteristics of the image. Since slight variations of singular values of an image may not affect the visual perception, watermark embedding through slight variations of singular values in the segmented image has been introduced as a choice for robust watermarking.

The existing system is a combination of DWT-SVD based technique. Initially the cover images and the water mark image have been obtained by MATLAB environment. Then, after this the water mark is embedded in that cover image using the hybrid scheme. That is the entire image is divided into four images then the watermark is embed into four copies of four different segments of the host image. These segments can be listed as up-left, up-right, bottom-left, and bottom-right. Although the decomposition is exactly that of described for detecting four corners of an image (previous section),the operations and objectives are obviously different and completely independent. In the watermarking procedure explained in this section, the decomposition is due to insertion of the watermark into the four different places, reducing cropping effect. Here, each segment of the host image is called sub image. Likewise the existing system had overcome the cropping, scaling and translation attack.

C. Algorithm

Using Haar filter, one-level DWT is applied on sub-image S H1 to obtain four sub-bands: LL, LH, HL, and HH. Each one will be of size M/4 × N/4.

The sub-bands LH and HL are partitioned into 8 × 8 nonoverlap-ping blocks and
each block is transformed by the DCT operation.

$$LH = \bigcup_{m=1}^{M/32} \bigcup_{n=1}^{N/32} LH(m,n) \quad --[2]$$

$$HL = \bigcup_{m=1}^{M/32} \bigcup_{n=1}^{N/32} HL(m,n) \quad --[3]$$

Only the first two AC coefficients (according to the Zig–Zag order) of each 8 × 8 DCT transformed block are selected to put in a rectangular matrix A. The two DCT coefficients are located at coordinate (1,2) and (2,1) in each 8 × 8 block.

In fact, each 8 × 8 DCT transformed block provides two elements of the matrix A. Therefore, the number of elements in the matrix A is calculated as M/32 × N/32 × 4. So, its dimensions can be M/16 × N/16. In our scheme, there is no need to specific rule for the placement regularity of the DCT coefficients from different 8 × 8 blocks in the matrix A. However, it is obvious that the placement regularity used in this step must be the same as the placement regularity used in the rest of the procedure as well as the extraction phase. The SVD operation is applied on the matrix A, getting three sub-matrices:

$$[U\,S\,V] = SVD(A) \quad ---[4]$$

Matrix S of size M/16 × N/16 that contains singular values, is used to embed the watermark. Watermark matrix W1 is scrambled by the Arnold transform to obtain matrix WScr . Matrix S of size M/16 × N/16 is modified to embed the matrix WScr.

$$SW = S + \sigma WScr \quad --[5]$$

where σ is the scaling factor. It is clear that the watermark matrix must be the same size as the matrix S. Again, the SVD operation

Volume 5 Issue I, January 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

is applied on the modified singular values, as given below:

$$[\,U' S'_W\, V'] = \text{SVD}(S_W) --[6]$$

Modified matrix A W is calculated as:

$$A_W = U S'_W V^T --[7]$$

In fact, the matrix A W contains altered AC coefficients.

These altered AC coefficients are put back to relevant positions in 8 × 8 blocks. In other word, the first two AC coefficients from each 8 × 8 DCT transformed block that compose the matrix A, are replaced by corresponding elements of matrix A_W, achieving watermarked and DCT transformed blocks.

Inverse DCT operation is applied on 8 × 8 blocks to get water-marked sub-bands as follows:

$$LH\_W = \bigcup_{m=1}^{M/32} \bigcup_{n=1}^{N/32} LH\_W(m,n) --[8]$$

$$HL\_W = \bigcup_{m=1}^{M/32} \bigcup_{n=1}^{N/32} HL\_W(m,n) --[9]$$

Inverse DWT is performed by using two non-modified sub-bands (i.e., LL and HH) and two modified sub-bands (i.e., LH_W and HL_W), obtaining watermarked sub-image SH_W.

The aforementioned steps are similarity repeated for embed-ding other three copies of the watermark into other three sub-images of the host image H. The resultant will be watermarked image H W. As a result from discussion above, using the proposed scheme, a host gray-scale image of size M × N can be used to embed a watermark matrix of size M/16 × N/16.

Next the PSNR value is computed. To evaluate imperceptibly, we use the Peak-Signal-to-Noise-Ratio (PSNR), which is defined as follow: With higher PSNR value, the watermarked image is more invisible. psnr - compute the Peak Signal to Noise Ratio,defined by :

$$PSNR(X,Y) = 10 * log10\left(\frac{\max(\max(x),\max(y))^2}{|x-y|^2}\right) --[10]$$

C. Watermark extraction algorithm

The watermarked image H_W may be corrupted by different attack. Firstly the geometric distortion correction technique is applied on the possibly distorted water-marked image. Then, the restored watermarked image H_W* is partitioned into four sub-images (i.e., S_H1*, S_H2*, S_H3*, and S_H4*), similar to embedding phase. The following steps describe how a possibly distorted watermark matrix W1* is extracted from a sub-image S_H1* of size M/2 × N/2.

Using Haar filter, one-level DWT is applied on sub-image S_H1*to obtain four subbands: LL*, LH*, HL*, and HH*. Each one will be of size M/4 × N/4.

The sub-bands LH*and HL*are partitioned into 8 × 8 non over-lapping blocks and each block is transformed by the DCT operation as given below:

$$LH^* = \bigcup_{m=1}^{M/32} \bigcup_{n=1}^{N/32} LH^*(m,n) --[11]$$

$$HL^* = \bigcup_{m=1}^{M/32} \bigcup_{n=1}^{N/32} HL^*(m,n) --[12]$$

Only the first two AC coefficients (according to the Zig–Zag order) of each 8 × 8 DCT transformed block are selected to put in a rectangular matrix A*. Similar to step 3 of embedding phase, the two DCT coefficients are located at coordinate (1,2) and (2,1)in each 8 × 8 block.

The SVD operation is applied on the matrix A, getting three sub-matrices:

$$[U^*\ S^*\ V^*] = SVD(A^*) --[13]$$

Matrix S^*_Wcan be computed as given below:

$$S^*_W = U'\, S^* V'^T --[14]$$

The aforementioned steps are similarity repeated for extracting other three copies of the watermark (i.e., W2*, W3*, and W4*) from

Volume 5 Issue I, January 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

other three sub-images (i.e., S_H2*, S_H3*, and S_H4*). The redundancy in different regions of the image can decrease impact of cropping attack. At the end, the final extracted watermark W*can be obtained as

$$W^* = \frac{W1^* + W2^* + W3^* + W4^*}{4} \quad [15]$$

If the watermark is a binary matrix, because of the embedding and extracting procedures, the elements of the extracted matrix may be turned to the fractional numbers between zero and one.

III. PROBLEM DEFINITION

Though there are lots of signal processing and geometric attacks such as mean attack, median attack, noise attack, cropping, scaling, rotation, reflection, shearing and translation , the existing system is robust only against translation, shearing, rotation. This will not make the image to be robust against all such attacks. So in order to overcome that, in addition to the existing technique, we are going to analyze all such attacks, such as mean attack, median attack, noise attack, cropping attack in our proposed technique.

A. System design

Digital watermark Allows users to embed SPECIAL PATTERN or SOME DATA into digital contents without changing its perceptual quality.

When data is embedded, it is not written at HEADER PART but embedded directly into digital media itself by changing media contents data

Watermarking is a key process for the PROTECTION of copyright ownership of electronic data.

IV. PROPOSED SYSTEM

The proposed technique will also use the same algorithm and technique as that of existing system. But the robustness against various types of attack will be more in our technique compared to the existing technique.

It is a combination of DWT-SVD based technique. Initially the cover images and the water mark image have been obtained by MATLAB environment. Then, after this the water mark is embedded in that cover image using the hybrid scheme. That is the entire image is divided into four images then the watermark is embed into four copies of four different segments of the host image. These segments can be listed as up-left, up-right, bottom-left, and bottom-right. Then after applying signature embedding, signature extraction, watermark embedding and watermark extraction technique we will obtain two curves such as “Gaussian curve” and “ROC” along with the watermark embedded image. Then after this we will check for the various kinds of attacks with the already taken cover and watermarked image. In the existing system they calculated for Translation, Scaling, Rotation + Scaling. In addition to that, we are going to calculate for mean, median, noise, shearing and cropping attack. Then we will extract the attacked image and watermarked image separately, and finally we are going to verify those observed values with our experimental results.

A. Watermarking embedding extraction steps

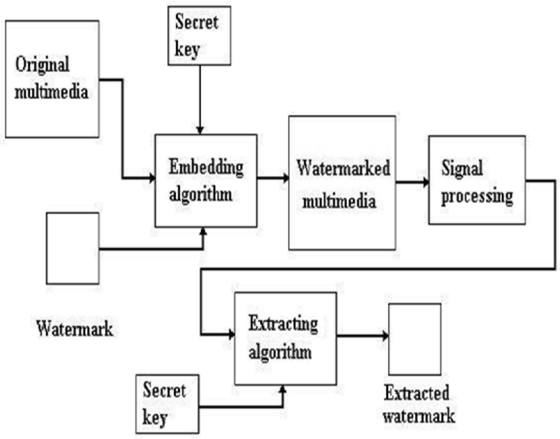

Fig 1: watermarking embedding extraction steps block diagram

Initially the original multimedia and watermark image is embedded with embedding algorithm along with secret key, then we will

Volume 5 Issue I, January 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

get the watermarked multimedia. Then with that watermarked multimedia, we will apply the signal processing, watermark extraction algorithm along with the secret key where we will obtain the extracted watermark.

B. Working procedure

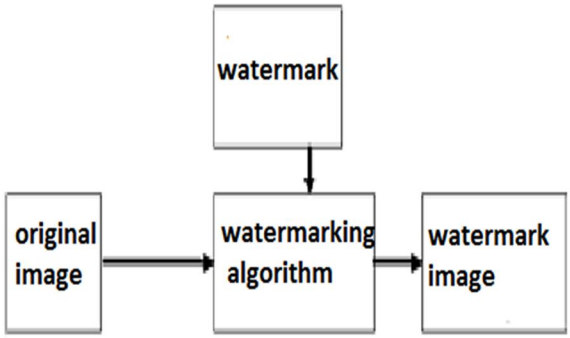

Fig 2: Working procedure block diagram

The original image is embedded with another image is using DWT-SVD where it is divided into 4 sub blocks, and then watermarking algorithm is applied where we will obtain the watermarked image .Then we will check for the various kinds of attacks with the already taken cover and watermarked image. In the existing system they calculated for Translation, Scaling, Rotation + Scaling. In addition to that, we are going to calculate for mean, median, noise, shearing and cropping attack. Then we will extract the attacked image and watermarked image separately, and finally we are going to verify those observed values with our experimental results.

V. RESULTS AND DISCUSSIONS

To demonstrate the efficiency of the proposed scheme, we selected some earlier geometrically robust works and the result shave been compared in terms of the robustness and imperceptibility. For each related work, we used its case study with similar specifications to establish a fair comparison. The experiments were coded by MATLAB R2103and implemented on a PC with CPU Intel Pentium 3.

Image in the first set of our experiments, we consider the geometrically robust watermarking scheme based on DWT, SVD, and Zernike Moments, reported by Li and Zhu, where a binary image of size32 × 32 as watermark is used to embed into the gravy-scale Lena image of size 512 × 512 as host. The selection of the image sizes in meets the watermark capacity of the proposed scheme (i.e., M = N = 512, M/16 = N/16 = 32). Then the image is verified against different kinds of geometric attacks such as rotation, shearing, cropping, mean, median, noise attacks.

To evaluate imperceptibly, we use the Peak-Signal-to-Noise-Ratio (PSNR), which is defined as follow. With higher PSNR value, the watermarked image is more invisible.

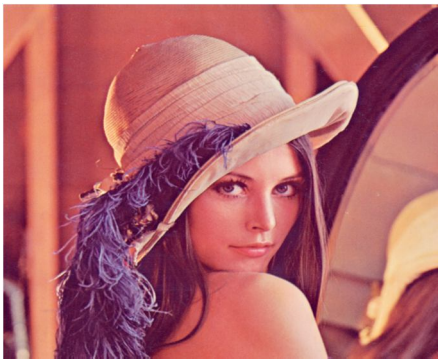

Fig 3: original image

Volume 5 Issue I, January 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Fig 4: watermark image

Fig 5: watermarked image

After applying Attack: For example 'crop attack'

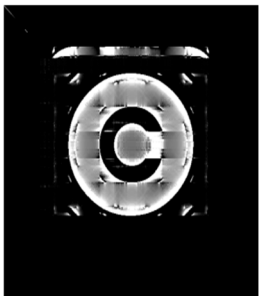

Fig 6: Attacked image Fig 7: extracted watermark

Next we will obtain two Curves

A. Roc curve

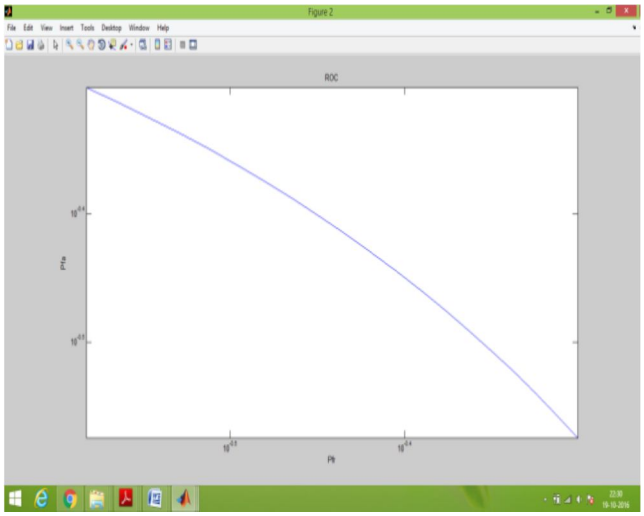

Fig 8: ROC curve

Volume 5 Issue I, January 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

B. Gaussian curve

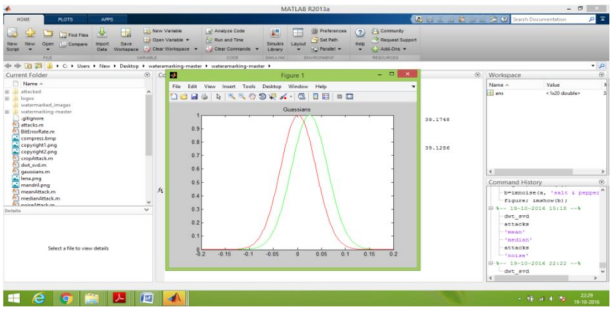

Fig 9: Gaussian curve

VI. CONCLUSION

Increasing robustness against geometrical distortions was addressed in this project. We suggested that watermark is independently embedded in four different sub-images of host image, to resist cropping attack. Furthermore, we demonstrated that other geometrical attacks such as rotation, translation, cropping, shearing, mean, median, noise and affine trans-formations generate a margin around desired image. The margin can lead to detect four corners of the desired image to perform recovering process. The proposed watermarking scheme is based on a new combination of DWT, DCT, and SVD domains, in which the attempt is based on usage of middle frequency components, establishing a trade-off between imperceptibility and robustness. Some earlier geometrically robust schemes were selected to compare with the proposed scheme. In the first related work, a binary image is used as watermark and in the other works, 1D binary sequences with different lengths are used as watermark. Also, we used error correction techniques, where length of the watermark sequence is lesser than the capacity of the proposed scheme. Experimental simulations demonstrated that the proposed scheme yields a considerable robustness, especially against geometrical attacks. In addition, generally, our scheme is superior or comparable to the other related schemes This paper has presented a SVD-DWT scheme, which was a semi-blind block-based watermarking technique for protecting real property rights of images. In this method, first, watermark and host images were taken to discrete wavelet transform domain and then HH and LL sub-bands of the host image were blocked and SVD was applied to each block of the host image. Afterward, LL sub-band blocks of the watermark image were embedded in the singular values of the blocks of the host image and a different SF was used for each block.

REFERENCES

[1] R. Liu, T. Tan, An SVD-based watermarking scheme for protecting rightfulownership, IEEE Trans. Multimedia 4 (1) (2002) 121–128.
[2] B. Lei, I.Y. Soon, F. Zhou, Z. Li, H. Lei, A robust audio watermarking scheme basedon lifting wavelet transform and singular value decomposition, Signal Process.92 (9) (2012) 1985–2001.
[3] C. Singh, S.K. Ranade, Geometrically invariant and high capacity image water marking scheme using accurate radial transform, Opt. Laser Technol. 54 (30)(2013) 176–184.
[4] M. Cedillo-Hernández, F. García Ugalde, M. Nakano Miyatake, H.M. Pérez Meana, Robust hybrid color image watermarking method based on DFT domainand 2D histogram modification, Signal Image Video P. 8 (2014) 49–63.
[5] E. Chrysochos, V. Fotopoulos, M. Xenos, A.N. Skodras, Hybrid watermarkingbased on chaos and histogram modification, Signal Image Video P. 8 (5) (2014)843–857.
[6] V. Aslantas, S. Ozer, S. Ozturk, Improving the performance of DCT-based fragilewatermarking using intelligent optimization algorithms, Opt. Commun. 282(2009) 2806–2817.
[7] D. Yu, F. Sattar, B. Binkat, Multiresolution fragile watermarking using com-plex chirp signals for content authentication, Pattern Recognit. 39 (2006)935–952. Z. Wenyin, F.Y. Shih, Semi-fragile spatial watermarking based on local binarypattern operators, Opt. Commun. 284 (2011) 3904–3912.
[8] A. Mishra, C. Agarwal, A. Sharma, P. Bedi, Optimized grayscale image water marking using DWT–SVD and firefly algorithm, Expert Syst. Appl. 41 (2014)
[9] D. Kundur, D. Hatzinakos, Toward robust logo watermarking using multi reso lution image fusion principles, IEEE Trans. Multimedia 6 (2004) 185–198.
[10] A. Briassouli, M.G. Strintzis, Locally optimum nonlinearities for DCT watermark detection, IEEE Trans. Image Process. 13 (2004) 1604–1617.
[11] C. Das, S. Panigrahi, V.K. Sharma, K.K. Mahapatra, A novel blind robust imagewatermarking in DCT domain using inter-block coefficient correlation, Aeu Int.J. Electron. C. 68 (2014) 244–253.
[12] A.A. Mohammad, A. Alhaj, S. Shaltaf, An improved SVD-based watermarking scheme for protecting rightful ownership, Signal Process. 88 (2008)2158–2180.