International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 01 | Jan -2017 www.irjet.net p-ISSN: 2395-0072

A ROBUST IMAGE WATERMARKING USING SVD AND DIFFERENTIAL EVOLUTION IN DWT DOMAIN

Mr.K.Balasamy[1], S.Priyanka[2], N.Kavya[3] , A.Abinaya Shruthi[4]

[1]K.Balasamy, Assistant Professor,
[2]S.Priyanka - Student, [3]N.Kavya- Student, [4]A.Abinaya Shruthi - Student,
Dept. of Information Technology, Dr.Mahalingam College of Engineering and Technology, Pollachi, TamilNadu, India

---

Abstract - *A robust image watermarking using SVD and Differential Evolution algorithm in DWT domain. The original image is partitioned into wavelets and they are transformed into DWT domain. The DW coefficients from each wavelet is collected to construct a low-resolution approximation image and apply SVD on this approximation image. After that watermark is embedded by modifying the scaling factor with the singular values of the watermark. The role of DE algorithm is to identify the best multiple scaling factors for embedding process in order to achieve the best performance in terms of robustness without compromising with the quality of the image. To enhance the security, watermark is scrambled by Arnold transform before embedding. Experimental results show that the proposed scheme maintains a satisfactory image quality and watermark can still be identified from a seriously distorted image.*

Key Words: **Discrete Wavelet Transform, Singular Value Decomposition, Differential Evolution Algorithm, Peak Signal to Noise Ratio, Arnold Transform, etc.**

1. INTRODUCTION

Watermarks was designed to prevent counterfeiting and is still used today. Today, digital watermarks are also added to photos, films and audio files to show a copyright by the owner of the object. A watermark, in presentation software, is frequently used in a slightly different manner. A watermark is often a faded image or text used as a background of a slide. Watermarks are sometimes used in the form of a logo, discreetly placed on a slide to brand the presentation Technique used to hide a small amount of digital data in a digital signal in such a way that it can't be detected by a standard playback device or viewer.

1.1 Requirements of Watermarking Algorithm

Watermarking is only supported for image formats processed by the Image Magick and IMagick media processing plugins. Watermarking is not supported with GD. If you are having trouble getting watermarking to work make sure your system is actually using Image Magick / IMagick.

LL, LH, HL, HH regions are generated. The LL region of the wavelet is initially selected for watermarking process. The SVD (Single Value Decomposition) technique is applied [u, s, v] =svd (image) to LL regions of all three colour image plane namely Red, Green and Blue. A watermark image is first splitted into 8 ×8 square wavelets by means of DWT

In general a digital watermark must be robust to transformations that include common signal distortions as well as Digital – Analog or Analog - Digital conversion and lossy compression, unless the media is altered to the point of no value. There are two major problems when trying to guaranty robustness; the watermark must be still present in the media after the transformation or it must be still possible for the watermark detector to detect it. When a signal is distorted, its fidelity is only preserved if its perceptually significant regions remain intact, while perceptually insignificant regions might be drastically changed with little effect on fidelity.

1.2 Classification of watermarking technique

Watermarks are embedded into images by changing some bits in representation. Some methods operate on least significant bits, while others embed information into perceptually more significant image components. Current image-based digital watermarks may be grouped under two general classifications: those that fall into the image domain and those that fall into the transform domain.

2. EXISTING SYSTEM

The original image is splitted into blocks using DCT domain. Then apply Singular Value Decomposition (SVD) on the blocks. After that watermark is embedded by modifying singular values .The DE algorithm is used to find out the best scaling value in order to achieve the best performance in terms of robustness. To enhance the security, Arnold transform is performed before embedding. Experimental results show that this scheme maintains a satisfactory image quality and hence the PSNR value is comparatively low for various attacks such as rotation, histogram equalization, cropping and gamma correction.

3. PROPOSED SYSTEM

In our proposed system we use Discrete Wavelet Transform (DWT). The original RGB cover image is splitted into 8 ×8 square wavelets by using DWT technique. Then the wavelets

transform. The SVD is applied to the LL region of the watermark image which contains Red, Green and Blue plane. Now the watermark image is embedded into the cover image by modifying scaling factors with the singular values of the watermark. The DE algorithm is used to select the best scaling factor to achieve the best performance in terms of robustness without compromising with the quality of the image. Finally the peak-signal-to-noise-ratio (PSNR) is calculated for the original cover image.

The extraction process is the exact reverse of the embedding process. The DWT transform is applied to the corrupted watermarked image that split the image into 8 ×8 square wavelets. Then SVD technique is applied to the wavelets generated. The singular values of the matrix is found. Then the Arnold transform is used to extract the watermark which is being embedded in the original cover image.

Finally the peak-signal-to-noise-ratio (PSNR) for the distorted watermark image is calculated to compare the distortion occurred in extracted image to that of original image while performing image processing attacks. This technique results in higher PSNR value for the possible image processing attacks and hence it provides high level authentication and security

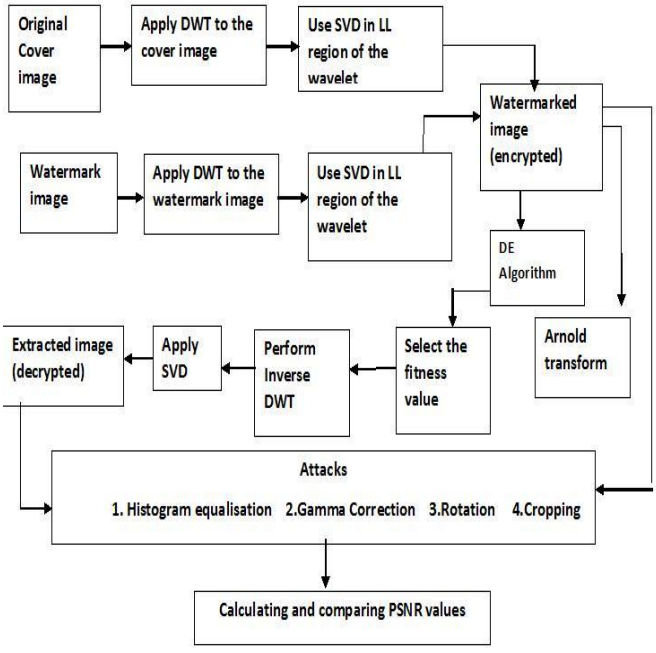

Fig -1: System implementation

In DWT process, first the RGB host image is taken; the original host image is splitted into 8 ×8 square wavelets by using DWT technique. The host image will have LL, Hl, LH, HH image resolutions where the LL part is considered. Each wavelets contains all the features that exist in original image.

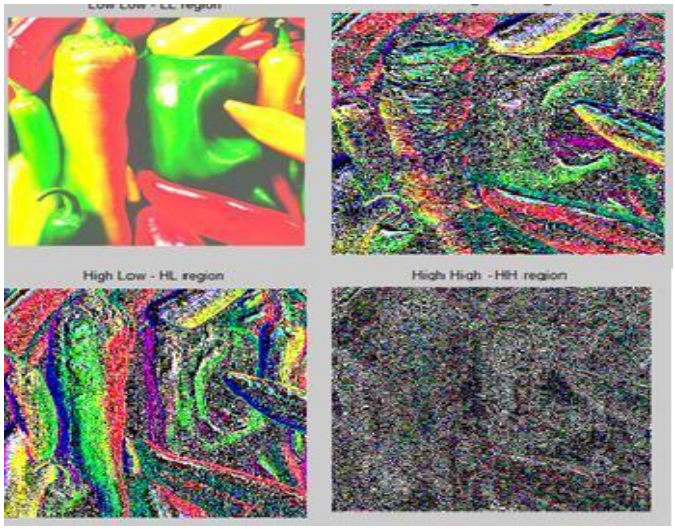

Fig -2: Splitting RGB image into wavelets

For whole process, single wavelet in the LL region is considered because it consists of all features and it can only be viewed by the user.

In SVD process, the RGB host image is taken and svd technique is applied to the image having R, G, and B plane region. Then U, S, V matrix of the corresponding Red, Blue and Green regions is generated SVD result.

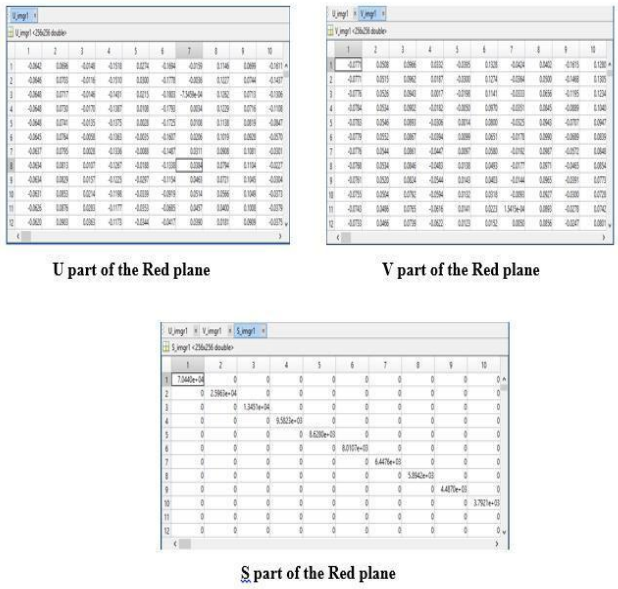

Fig -3: Applying SVD to RGB plane

In embedding process, first the RGB host image is taken and DWT technique is applied to the host image. Then the SVD technique is applied to the U, V, and S part of the image having R, G, and B region of the wavelets is added with the constant value “a” which is the scaling factor. This process is called watermarking.

Fig -4: Watermark embedding

3. RESULTS AND DISCUSSIONS

Various attacks have been imposed on the embedded watermark such as histogram equalization, cropping, rotation and gamma correction.

Rotation attack breaks the synchronisation between original image and encrypted image and here the rotation is performed at 30 degree. Histogram equalisation attack is to contrast the adjustment of the image using image histogram.

Fig -5: Applying Histogram equalization to encrypted and decrypted image

Fig -6: Applying cropping to encrypted and decrypted image

Fig -7: Applying rotation- 30 degree to encrypted and decrypted image

Nonlinearity encountered during image capturing, printing and displaying can be corrected using gamma correction. Few part of the image is cropped in order to fit into the particular application which is the cropping attack.

PSNR is the ratio between the maximum possible power of the encrypted image and the power of decrypted watermark that affects the fidelity of its representation. It generally indicates the reconstruction is of higher quality, in some cases it may not.

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{(X_{MAX})^2}{1/(n\times n)\sum_i\sum_j(X(i,j)-\hat{X}(i,j))^2}\right)$$

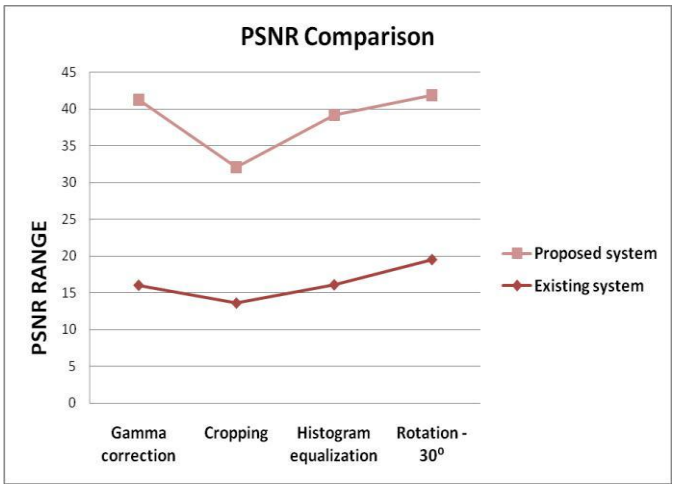

Chart -1: PSNR Value Comparison

By using the PSNR formula the PSNR value of the encrypted and extracted watermark is found. Then the PSNR ratio is found for the various attacks such as gamma correction (25.1796), cropping (18.4203), histogram equalization (23.0245) and rotation through 30 degree (22.3078). Then the PSNR values have been compared with that of the existing system values.

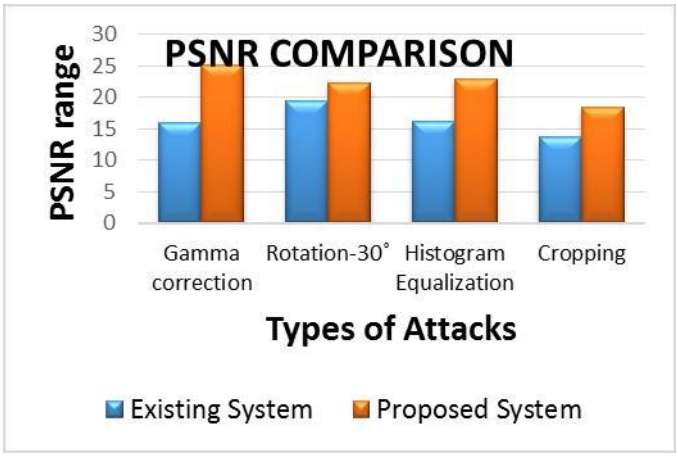

Chart -2: PSNR Value Comparison

3. CONCLUSIONS

A robust Image watermarking technique using SVD and DE algorithm in DWT domain has been implemented. The cover RGB image has been splitted into wavelets in the DWT domain and the SVD technique is applied to the splitted wavelets which generates the R, G and B regions of the cover image. The DE algorithm have been used in order to find the best fitness value. Then the Arnold transform is used to retain the original quality of the image. Then the watermarked image is also splitted into wavelets and then SVD technique is applied to the watermark .Then the watermark is embedded into the cover image by generating the constant scaling factor. The watermark has been extracted from the original encrypted image by performing the inverse process of embedding. Finally the PSNR value is calculated for the encrypted watermark and the extracted watermark to compare the distortion of the extracted image to that of the original image. The PSNR has also been calculated while performing the attacks and hence it yields greater value leading to higher level security and robustness. However, the proposed system is not suitable for any other stronger attacks. Because this may lead to distortion of images and have the possibility of easy retrieval of the hidden information.

REFERENCES

[1] Yang, H., Kot, A.C., Rahardja, S., "Orthogonal data embedding for binary images in Morphological transform domain – a high-capacity approach", IEEE Transactions on Multimedia 10 (3), 339–351, 2008.

[2] Ou, B., Li, X., Zhao, Y., Ni, R.,"Reversible data hiding based on PDE predictor",Journal of Systems and Software 86 (10), 2700–2709, 2013.

[3] Wu, M., Liu, B.,"Data hiding in binary image for authentication and annotation", IEEE Transactions on Multimedia 6 (4), 528–538, 2004.

[4] Willems, F.M.J., van Dijk, M., "Capacity and codes for embedding information in gray scale signals",IEEE Transactions on Information Theory 51 (3),1209–1241, 2005.

[5] Wu, M.Y., Lee, J.H., "A novel data embedding method for two-color facsimile images", In: Proceedings of International Symposium on Multimedia Information Processing, Taiwan, 1998.

[6] Wu, M., Fridrich, J., Goljan, M., Gou, H., "Handling uneven embedding capacity in binary images: a revisit", In: Proceedings of SPIE Conference on Security, Steganography, and Watermarking of Multimedia Contents VII, San Jose, CA,USA, pp. 194–205, vol. 5681.2005.

[7] Yang, H., Kot, A.C., "Pattern-based data hiding for binary image authentication by connectivity-preserving", IEEE Transactions on Multimedia 9 (3), 475–486, 2007.25

[8] Yang, H., Kot, A.C., Rahardja, S., "Orthogonal data embedding for binary images in morphological transform domain – a high-capacity approach", IEEE Transactions on Multimedia 10 (3), 339–351, 2008