

# Encryption Based Hybrid DWT-SVD Watermarking Technique for Data Hiding

M.P. Anitha and S.S. Lijina

**Abstract---** This paper widely deals with how data hiding can be more effectively done by encryption based hybrid image watermarking viz., DWT and SWD. Then an image encryption concept is used to protect the image contents. The basic idea of the proposed technique consist of three phases. First phase includes fusing of multiple watermark images with wavelet fusion to produce fused watermark and in the second phase hybrid DWT-SVD based algorithm is used to embed fused watermark on the original image. Finally, it encrypts the watermarked image into Visually Meaningful Encrypted Image (VMEI). The method not only enhances the capacity of the embedded information but also its robustness without affecting the perceptual quality of original image and security.

**Keywords---** Data Hiding, Wavelet Fusion, Discrete Wavelet Transform(DWT), Singular Value Decomposition (SVD), Visually Meaningful Encrypted Image(VMEI), Discrete Wavelet Transform based Content Transform (DWTCT)

## I. INTRODUCTION

TODAY, the internet is the most important media for data communication. So Important challenge is to protect the data which is transmitted over internet. Data hiding is used for this purpose. Reversible data hiding incorporates a special technique which validates the images followed by restoring these images to their original form by removing the digital watermark and superseding the image data that has been overwritten. A digital watermarking is typically used to identify the ownership of the copyright of such image. Watermarking is the process of hiding digital information in a host image. Digital image watermarks can be used to validate the authenticity and adherence of the host image or to reveal the identity of its owners.

Watermarking can be undergone using many algorithms. Different techniques are implemented using a variety of algorithms. The way watermark is embedded in the images and the host data scores chosen for hiding the information determines the productivity of the technique being used.

In [4], [5] various watermarking technique are studied and a comparative study is done on DCT, DWT, CT and SVD techniques. Based on the watermark application, fragility or robustness, unambiguity, imperceptibility, low complexity and

invisibility properties should be reliable, so that the watermarking method incorporated is fruitful.

Data protection [12] now a day goes behind data encryption techniques. The original data is encrypted by converting it to an unreadable format in data encryption. The information cannot be accessed without reversing the process i.e., decryption. Plain data is used to represent the original data and the encrypted data is called cipher data. Encryption is a digital process in which plain data to be transferred is coded which can be decrypted only by a special receiver which is loaded with the instructions to decode the ciphered data. Encryption can be applied to text, image, video for data protection.

In the proposed technique, encryption is employed to enhance the image security. Here it directly encrypts the original image into visually meaningful encrypted image(VMEI)[2]. Because a VMEI has a visual feature similar to a normal image, attackers have extreme difficulty distinguishing VMEIs from large number of normal images. Hence this method is able to protect original images with a much higher security level.

This paper portrays a hybrid and sophisticated technique of encryption and data hiding with a more enhanced security and capacity without even merely affecting the original and integral quality of the image. Here initially, wavelet fusion technique is used for fusing multiple watermarks. Then a watermarked image is induced using the hybrid DWT-SVD watermarking algorithm by embedding the combined watermark in the host (original) image. Finally encrypts the watermarked image into visually meaningful encrypted image.

## II. DESIGNING PRINCIPLES OF IMAGE WATERMARKING ALGORITHM

Image watermarking algorithm should have the following characteristics [7]

- Security: Only authorised persons should be accessible to the watermark.
- Robustness: Curb modifications or updations due to attacks by removing or eliminating the watermarked images by unauthorised persons.
- Imperceptibility: The host image quality should not be affected by the watermarked image.
- Capacity: represents the count of bits that can embedded with the host signal.

All these characteristics are must to produce a robust watermarking algorithm.

M.P. Anitha, Computer Science and Engineering Department, Kannur University. E-mail:anithamp@gmail.com

S.S. Lijina, Computer Science and Engineering Department, Malabar Institute of Technology, Anjarakandy, India. E-mail:lijina.nambiar@gmail.com

DOI: 10.9756/BIJDM.7205

### III. DIGITAL WATERMARKING LIFE CYCLE

The watermarking technique consist of three steps [4]

- **Embedding:** The host and the data to be embedded are inputted to the algorithm to produce a watermarked signal. The resultant signal is transmitted to the destination or stored.
- **Attack:** Unauthorised access or modification of the embedded signal.
- **Extraction:** A special algorithm is used on the signal obtained at the destination for the watermark from the signal. The watermark can be extracted if the signal remains unchanged throughout the transmission.

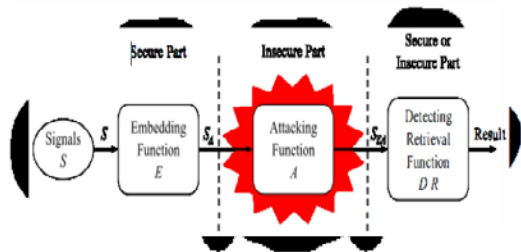


Fig. 1: Watermarking Life Cycle [4]

### IV. PROPOSED TECHNIQUE

The technique comprises 3 phases. The initial phase deals with fusing of multiple watermark images by wavelet fusion to generate fused watermark. In the following phase, the obtained fused watermark is embedded on the host image using hybrid DWT-SVD watermarking. And in the last phase the watermarked image is ciphered or coded to VMEI or Visually Meaningful Encrypted Image (VMEI).

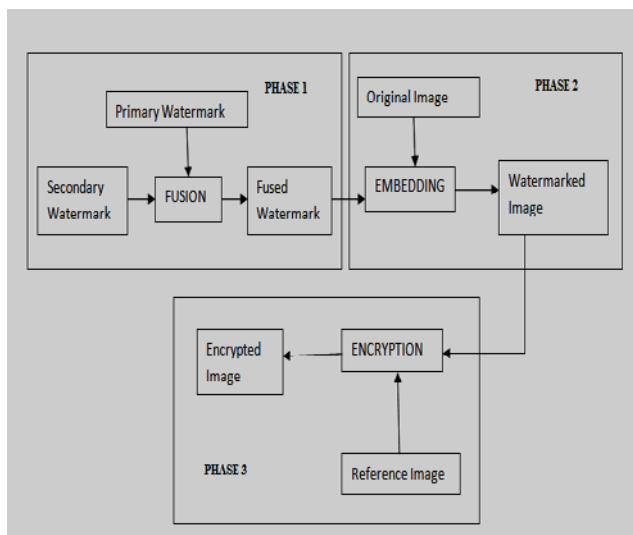


Fig. 2: Proposed Technique

#### A. Phase 1: Wavelet Based Image Fusion

It has been undoubtedly proven that [11] wavelet based fusion techniques excel the standard fusion techniques in spectral as well as spatial qualities particularly in colour distortion minimizing. Image fusion algorithm based on this technique is mainly recommended to enhance the geometric

resolution of the images. Here the 2 images to be processed are initially disintegrated into sub images of the same resolution in same level and also of different resolutions in different levels. Then following the gradient criteria, the information fusion is carried out with the sub images with high frequency and finally these sub images are remounted on the resultant image along with abundant information. As the high-frequency information in the image is the key factor to its geometric resolution, good results can be induced from the image fusing algorithm.

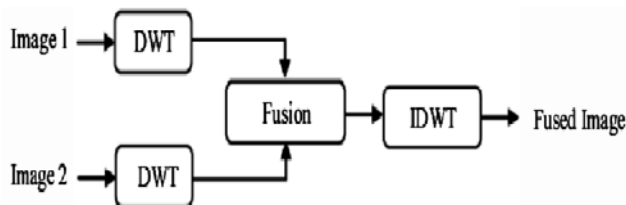


Fig. 3: Wavelet Fusion of Two Images [11]

#### B. Phase 2: Embedding Using Hybrid DWT-SVD Watermarking Algorithm

##### 1. DWT Watermarking Algorithm

A wide variety of signal processing applications such as audio, image and video compression & removal of noise in audio, uses the Discrete Wavelet Transform or DWT [8]. In DWT, one-dimensional DWT separates an image into four bands of data represented as Lower Level (LL) resolution approximation image, Diagonal (HH), Vertical (LH), Horizontal Level (HL) detail components.

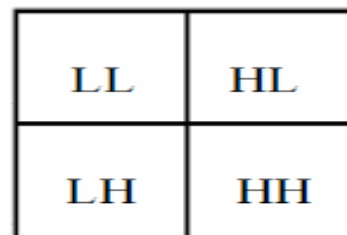


Fig. 4: One-level DWT [7]

##### 2. SVD Watermarking Algorithm

A mathematical technique is followed in SVD [4] i.e., Singular Value Decomposition. From the image processing view point the main pros of SVD are the Singular Values, SV's of images which:

- Exhibits peerless stability when an image is added with small perturbations. Images remain sturdy against different attacks as its SV doesn't show any significant changes.
- Pictures the image's intrinsic algebraic properties. Using these properties and without much variations, the watermark may be embedded to SVD matrix.

One diagonal matrix 'S' and two orthogonal matrices 'U', 'V' is derived by computing the SVD of an image. The approach is then followed by combining the watermark 'W' with matrix 'S'.

### C. Phase 3: Encrypt the Watermarked Image into VMEI.

The encryption system consist of two parts: pre-encryption process and a discrete wavelet transform based content transform(DWTCT). The image pixel values and locations are effectively updated by permutation and substitution in the pre-encryption process. The pre-encrypted image is usually a noise like image. It is then transformed by DWTCT into VMEI that is visually similar to the reference image.

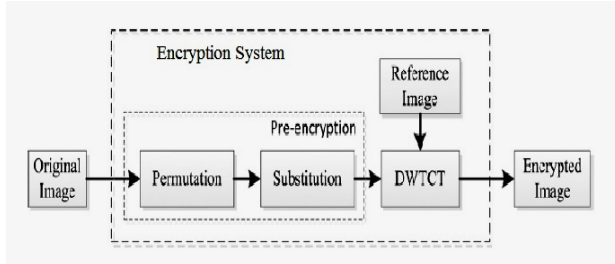


Fig. 5: Encryption System

## V. ALGORITHM DESCRIPTION

### A. Watermarking Embedding Algorithm

The watermark embedding algorithm works as follows:

1. The original image is transformed in to four sub-bands using one-level DWT.
2. The block-based SVD is performed on the original image (F matrix).

$$F=USV^T$$

3. The primary and secondary watermarks are fused using wavelet fusion algorithm.
4. The watermark (W matrix) is added to the SVs of the original image (S matrix).

$$D=S+kW$$

5. The SVD is performed on the D matrix.

$$D=U_w S_w (V_w)^T$$

6. The watermarked image (F<sub>w</sub> matrix) is obtained using the modified SVs (S<sub>w</sub> matrix).

$$F_w=US_w V^T$$

7. The watermarked image is inversed using the one-level IDWT.

### B. Watermarking Extracting Algorithm

The watermark extracting algorithm works as follows:

1. The Watermarked image is transformed using one-level DWT.
2. The block-based SVD is performed on the possibly distorted watermarked image (F<sub>w</sub><sup>\*</sup> matrix).

$$F_w^* = U^* S_w^* (V^*)^T$$

3. The matrix includes the fused image is calculated.

$$D^* = U_w S_w^* (V_w)^T$$

4. The possibly fused watermark is obtained.

$$W^* = (D^* - S)/k$$

5. Anti-fusion of the fused watermark using wavelet fusion to extract primary and secondary watermarks.

### C. Algorithm for Encryption

1. The pre-encrypted image P can be defined by

$$P = F(O, K_p)$$

2. Apply DWT defined by parameter  $K_i$  to the reference image R, obtain  $C_A$ ,  $C_H$ ,  $C_V$  and  $C_D$ .
3. for m=1 to M do
4. for n=1 to N do
5.  $C_V(m,n) = \text{floor}(P(m,n)/10)$
6.  $C_D(m,n) = P(m,n) \bmod 10$ .
7. end for
8. end for
9. Apply the inverse DWT to  $C_A$ ,  $C_H$ ,  $C_V$  and  $C_D$ .

## VI. CONCLUSION

In the said method multiple watermark images are initially fused productively using wavelet fusion to enhance the capacity of embedding information. Then the obtained fused watermark is embedded in the original image using hybrid DWT-SVD watermarking which enhances the robustness without affecting the original quality of image. At last the watermarked image is encrypted to VMEI by accelerating the security which is of low computational cost. The encryption system utilizes a pre-encryption process with excellent diffusion and confusion properties to protect the image contents and an effective DWT based content transform to generate VMEIs with many different visual appearances. The proposed methods have potential applications for privacy and copyright protection in networks and cloud computing.

## ACKNOWLEDGMENT

The authors are grateful to the anonymous referees for their valuable comments and suggestions to improve the presentation of this paper. Also we wish to thank the Department of Computer Science and Engineering for providing all resources and their valuable support.

## REFERENCES

- [1] Gamal Attiya, Fathi Abd El-Samii Ezz El-Din Hemdan and Nawal El-Fishaw, "Hybrid digital image watermarking technique for data hiding," 2013.
- [2] Long Bao and Yicong Zhou, "Image Encryption: Generating visually meaningful encrypted images," 2015.
- [3] R. liu and T. tan, "An SVD-Based Watermarking Scheme for protecting rightful ownership," IEEE Trans. on multimedia, Vol. 4, No. 1, March 2002.
- [4] M. Nizamuddin Afrin Zahra Husaini, "Challenges and approach for a robust image watermarking algorithm," International Journal of Electronics Engineering, 2, Pp.229–233, 2010.
- [5] M.I. Dessouky, N.A. El-Fishawy, F.E. Abd El-Samie, R.A. Ghazy and M.M. Hadhoud, "Performance evaluation of block based svd image watermarking," 2008.
- [6] T. Tan and R. liu, "An SVD-based watermarking scheme for protecting rightful ownership," Vol. 4, 2002.
- [7] Vipula Singh, "Digital watermarking: A tutorial," 2011.
- [8] Suneeta Agarwal, Sushila Kamble, Vikas Maheshkar and Vinay Kumar Srivastava, "Dwt-based multiple watermarking for privacy and security of digital images in e-commerce," International Conference on Multimedia, Signal Processing and Communication Technologies, 2011.

- [9] Song Han, Vidyasagar M. Potdar and Elizabeth Chang, "A survey of digital image watermarking techniques," 3rd IEEE International Conference on Industrial Informatics (INDIN), 2005.
- [10] R.A. Ghazy, M.M. Hadhoud, M.I. Dessouky, N.A. El-Fishawy and F.E. Abd El-Samie, "Performance Evaluation of Block Based Image Watermarking," Progress in Electromagnetics Research, Vol. 8, Pp.147-159, 2008.
- [11] Shih-Gu Huang, Wavelet for image fusion.
- [12] V V Divya, S K Sudha, V R Resmy, "Simple and secure Image Encryption," IJCSI International journal of Computer Science Issues, Vol. 9, No. 3, November 2012.
- [13] K J Giri, M.A.Peer and P Nagabhushan, "A Robust color image watermarking scheme using Discrete Wavelet Transform," 2015.