

# Fingerprint Authentication in Digital Watermarking Using YCbCr Colour Space & 2D Walsh Code

**B P Mishra<sup>1</sup> & P Das<sup>3</sup>**

<sup>1&3</sup> Indira Gandhi Institute of Technology, Sarang, India  
Email: bishnu.mishra@driems.ac.in, daspranati@yahoo.co.in

**H N Pratihari<sup>2</sup>**

<sup>2</sup> Calcutta Institute of Technology, Westbengal, India  
Email: drhnpratihari@gmail.com

**Abstract**—During the recent development in image manipulating software and vast use of Internet, it is now becomes very difficult to protect the images that are precious and need to be secured so that they will survive against several image modification attacks. This paper represents a new technique to produce robust and efficient Twin blind digital Watermarking with the use of 2-D Walsh code and Discrete Cosine transform. Authentication matching process is introduced during the extraction process to provide extra security to the Host image. Both the Watermarks are embedded into host image through Walsh Code conversion. In this technique, the Embedding and extraction of Watermark is simpler than the other transform previously used. The proposed algorithm uses the YCbCr colour elements of the colour images in DCT province with low frequency components. During the first step the Principal Watermark i.e Hand written signature is embedded through 2-D Walsh coding and then the resultant watermark i.e Biometric fingerprint is embedded to the first Watermarked image through 2-D Walsh coding. The De-watermarking is dawn by checking the Authentication through Biometric fingerprint matching method. The technique is accessed by analyzing various performance parameters like SSIM, PSNR and NC. Further, the evaluation is made through various attacks by using StirMark tool. It was observed from the result that, by utilizing 2-D Walsh coding technique, better robustness is maintained and the proposed technique survived against various attacks such as JPEG compression, median, noise etc.

**Index Terms**—Discrete Cosine Transform, Digital Watermarking, 2-D Walsh code, YCbCr colour space, Authentication matching etc.

## I. INTRODUCTION

Digital information carried out during the vast scale of communication through various sources is accessible for large number of people and produces illegal duplication and manipulation. Then it becomes necessary to provide

security arrangement for copy protection or copyright protection of the Multimedia data used during this process. To avoid the illegal assessment of multimedia data, Digital Watermarking is introduced [2]. It provides the growing need of theft and tampering through the use of Modern Signal Processing methods to embed Authentication and Ownership information within the media data contents.

Digital Watermarking techniques [2] [3] provides the merging of signal permanently into a digital image which can be extracted or detected according to the need by providing necessary Authentication. The Hidden watermark must provide robust enough to survive against any type of manipulation by preserving the quality of the image. Thus permanently marking of Intellectual Property Right remain accessible.

In past many Watermarking algorithms were proposed [1] [2] [3]. Some of them are processed DCT through frequency domain [4] [5] [6]. In this work, new Watermarking technique through DCT using low frequency elements is presented where DCT of (8 X 8) blocks are used for hiding of Watermark information.

In this proposed technique, YCbCr colour components are used instead of RGB components. Generally Y component in the colour space indentifies the Luminance and Cb, Cr components are used as colour information. The equivalent Y channel of the RGB host image is used during the processing of the proposed algorithm [10].

In this work, Walsh code functions are utilized to increase the robustness of the proposed watermarking method [7]. The use of 2-D Walsh function provides information encoding for both Major Watermark i.e Hand written signature and the Resultant Watermark for Authentication i.e Biometric fingerprint before merging them into Y channel of the host colour image [13]. During the processing, Walsh code of length-8 is considered.

Biometric fingerprint recognition or authentication is an automated method of matching and verifying two fingerprints. Fingerprint is mainly used for biometric purpose to recognize individual identity [17]. In the proposed technique, Biometric fingerprint is specifically

used during the detection to extract major Watermark as an Authentication source.

The work has been tested against multiple parameters made for performance like SSIM, NC and PSNR [12]. The verification is also carried out through several intentional and non-intentional attacks by using StirMark toolbox [15].

## II. PROPOSED EMBEDDING ALGORITHM

The proposed algorithm consists of three different sections to produce the Watermarked image. During the first section, two dimensional Walsh coding is applied to the Major Watermark i.e Binary signature image and converted it into its equivalent binary number. During the second section, both Horizontal and Vertical Walsh coding is applied to the Biometric fingerprint image to produce its equivalent binary number. During the third section the Embedding process of major watermark and then Authentication Watermark is carried out in the low frequency elements of DCT blocks.

### A. 2-d Walsh Coding of Major Watermark

In the proposed technique 2-D Walsh function is used to increase the robustness. 2-D Walsh function is applied to encode the handwritten signature before embedding it into the main host image. During the process of converting the signature image into its equivalent Walsh function, every individual vector of the signature's equivalent vector is changed by its corresponding Walsh code sequence. The process is applied horizontally and then vertically to all signature pixels.

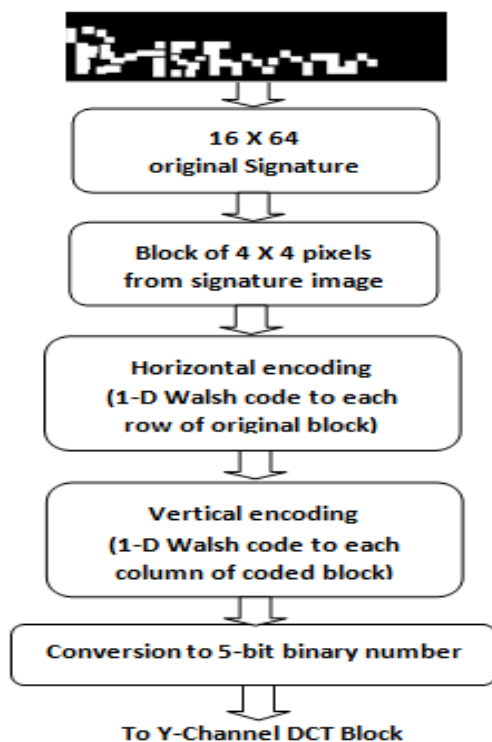


Fig. 1. Applying 2D Walsh coding on the Signature image

Equivalent binary signature as major Watermark is utilized here as watermarking information. The 16 X 64 size original signature is divided into 4x4 blocks. In the first section, Walsh code is multiplied with each row's elements of the block to produce 1-D Walsh code. In the same way the consequential codes are used to generate a 4x4 block. The produced elements will be decimal numbers in the range -2 to 4. The section's resulting 1-D Walsh coded block is then applied to the second stage. During the second stage, again Walsh code is multiplied with each column's element of the input Walsh coded block and then multiplexed to produce 2-D Walsh coded block. Every element of the produced Walsh coded block is in the range -8 to 16 in decimal number. Finally by converting them into five bit binary number it is ready for insertion into DCT blocks.

Original Handwritten signature is converted into its equivalent binary signature and then processed as per the requirement of the algorithm. By the method of 2-D Walsh coding, binary signature image is converted to its equivalent 5-bit binary number for further insertion in the DCT blocks.

### B. 2-D Walsh Coding of Authentication Watermark

As an Authentication watermark, Biometric fingerprint is used to embed in the Watermarked Y channel image after generating its equivalent Walsh code. In the proposed technique, 2-D Walsh function is used with length 8 to encode the fingerprint after scanning the same by proper Biometric Scanner to generate its equivalent binary code.

To avail 2-D Walsh code, fingerprint is applied for both vertically then horizontally and can be generated by multiplying vector of fingerprint's each row by Walsh code and then adding them for getting horizontal part. After that vector of fingerprint's each column is multiplied with the result of first part and adding them to get Two Dimensional Walsh code of fingerprint.

The size of 16 X 64 fingerprint image is repeated four times and then Shuffling to achieve 64 X 64 size. The 64 X 64 binary bits are multiplied and added together to get horizontal Walsh to form a new matrix  $64 \times 64$  with decimal numbers in the range 2 to 4. Then these numbers are multiplied vertically and added together to get 2-D Walsh code. The resulting product is in the range 8 to 16. Finally the numbers are converted in the range 0 to 24 where these decimal numbers are converted into five bit binary numbers for insertion into Watermarked Y channel DCT block.

Using fingerprint scanner, applied fingerprint is converted to its equivalent binary code. By the process of 2-D Walsh coding, fingerprint image is converted to its equivalent 5-bit binary number for further insertion in the DCT blocks.

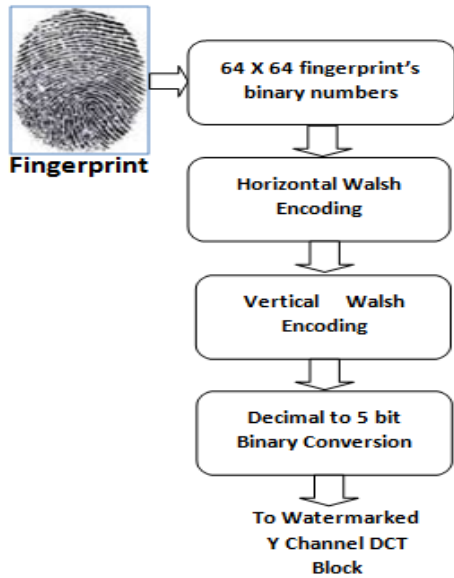


Fig. 2. Applying 2-D Walsh coding on Fingerprint image

C. DCT Embedding Algorithm

In the proposed method, DC components are excluded while very low frequency band is modified in the process of Embedding Watermarks into DCT blocks. The process involved twice Embedding one after another. First major Watermark i.e Hand written signature is embedded to get first Watermark image and then Authentication Watermark i.e Biometric fingerprint is embedded to get final Watermarked image. Both the watermarks are converted to its equivalent 2-D Walsh code before embedding them into DCT blocks. This is done by modifying the DCT coefficient value. First it is divided by a scaling factor and then rounded to an integer:

$$P2(i, j) = Round \left[ \frac{P1(i, j)}{S} \right] \tag{1}$$

Where  $P1$  is the image original coefficient and  $P2$  is the modified coefficient.  $S$  is the scaling factor.

Before embedding the Watermarks, the host RGB image is converted to its equivalent Y channel where YCbCr colour components are utilized. Then DCT is applied to the image where it is divided into (8x8) blocks. The process of inserting or embedding is carried by placing the encoded bits (either -1 or +1) into the stated (even or odd) element value of the block and then applying the IDCT for constructing the final Watermarked Y channel image. Lastly the Y channel Watermarked image is converted to its equivalent RGB Watermarked image. It is proposed to embed two different Watermarks in the same host image while maintaining image quality. The embedding process of two Watermarks i.e Hand written signature which has to be extracted during recovering process and Biometric fingerprint which can be utilized for Authentication resource for extraction of Major Watermark. Fig.3 shows the whole Embedding Process of 2-D Walsh coded Watermarks to the Host image.

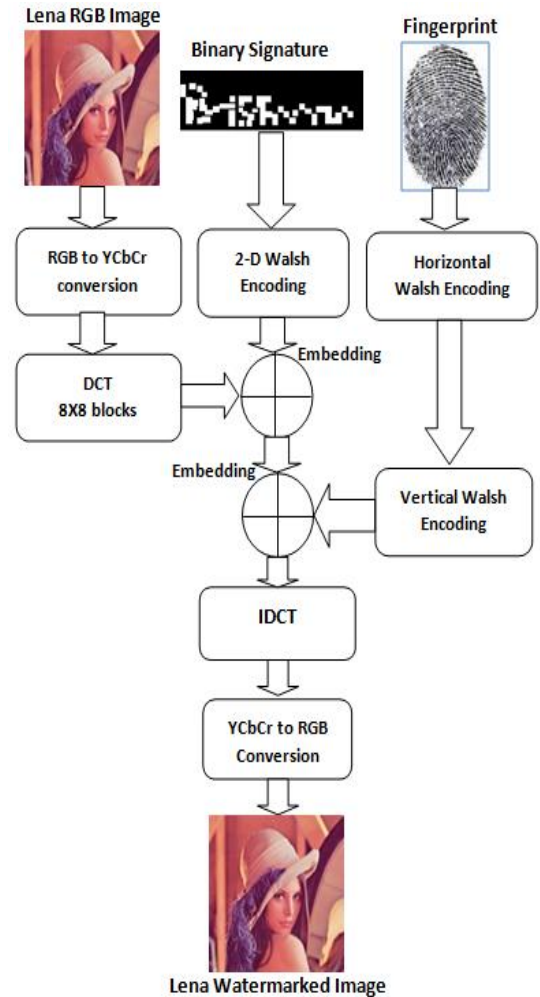


Fig. 3. Embedding of both Watermarks through 2D Walsh coding

During the work multiple 512 X 512 RGB images [16] were used to verify the algorithm. Fig.4(a) Lena image, 4(b) Adya image, 4(c) Mena image and 4(d) Cartoon image are the examples of sample RGB images that were used during the work.



Fig. 4(a)



Fig. 4(b)



Fig. 4(c)

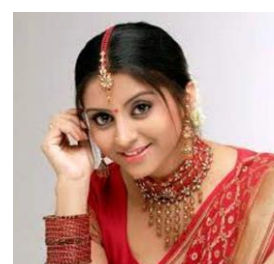


Fig. 4(d)

### III. ALGORITHM FOR WITHDRAWAL OF WATERMARKING

The proposed algorithm used for withdrawal of Major Watermark i.e Binary handwritten signature includes colour space conversion followed by horizontal and then vertical decoding, Authentication matching and finally Watermark extraction. The following actions have been taken to extract Binary handwritten Signature from the Watermarked image:

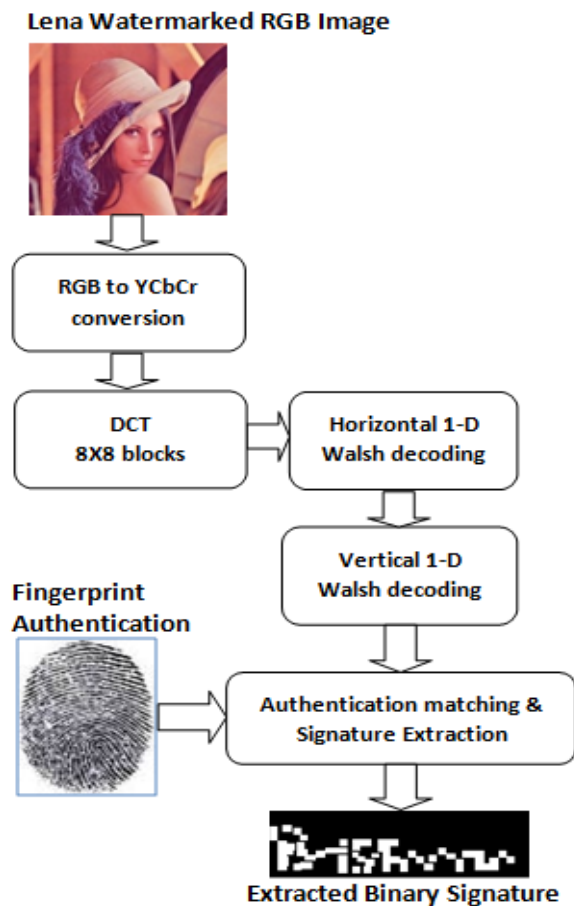


Fig. 5. Extraction of Binary signature

- First step is to convert Watermarked RGB image to its equivalent Y channel image.
- Y-channel Watermarked image is divided into 8 X 8 blocks and DCT is applied to each block.
- Watermarked coefficients are checked for even and odd value.
- Binary bits are extracted and 2-D 4X4 blocks are constructed by decimal numbers.
- Horizontal 1-D decoding followed by vertical 1-D Decoding is performed.
- Fingerprint is applied and matched for Authentication.
- Binary signature is extracted.

Fig.5 gives the flow diagram used for extracting the Binary signature. During the process of withdrawal of Major Watermark, it is not required to use the host image. So the algorithm used for this purpose is blind in nature.

### IV. RESULT AND ANALYSIS

The capability of the proposed algorithm was examined by taking various colour images of size 512 X 512 pixels and multiple Signatures has been applied of size 16 X 64 for testing the potential of the algorithm. The robustness of the technique is also examined. During the investigation, Scaling factors from 4 to 20 were applied on the Watermarking to test the effect of the Resulting Watermarked images. Table 1 shows the effect of applying 2-D Walsh code on test images with Scale factor 20.

Table 1. Watermarking effect of applying 2-D Walsh code on Test images with Scale factor 20.

Image Name	Test Image	SSIM	PSNR	Watermarked Image
lena.jpg		0.9625	40.9421	
adya.jpg		0.9732	40.3011	
mena.jpg		0.9688	40.5498	
cartoon.jpg		0.9748	41.3311	

Table 1 shows the idea about the effects of producing Watermarked image where both Walsh coded Watermarks is embedded in the Host image through their respective 2-D Walsh code against SSIM and PSNR with Scale factor 20.

The projected algorithm using Walsh code length of 8 was tested for justification. The observation regarding the variations of values by changing the Scaling factors on the Perceptual invisibility was verified and noted using the PSNR and SSIM. The strength of algorithm beside JPEG compression was also observed. The capability of the algorithm in terms of robustness was also tested using the StirMark tool. The processing of algorithm by taking different Scaling factors shows the Perceptual invisibility of the Watermarked images and their individual SSIM and PSNR index value.

#### A. Evaluation Using Proposed Algorithm

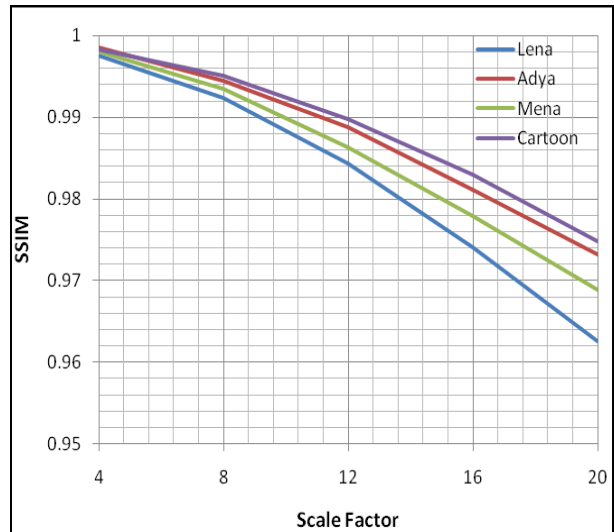
Based on the 2-D Walsh coding of length 8, the proposed technique was processed and evaluated. By taking different Scaling factors from 4 to 20 during the validation of the algorithm, the Perceptual invisibility of the Watermarked images and their individual SSIM and PSNR index values were observed. During the evaluation, verities of standard and non- standard colour images of size 512 X 512 were tested. From the obtained SSIM and PSNR values, distortion caused at the Watermarked images is evaluated and it is concluded that there is an invisible distortion created by the Watermark method and the effect takes place for the same was studied.

Table 2. SSIM & PSNR with 2-D Walsh coded extraction of Binary signature

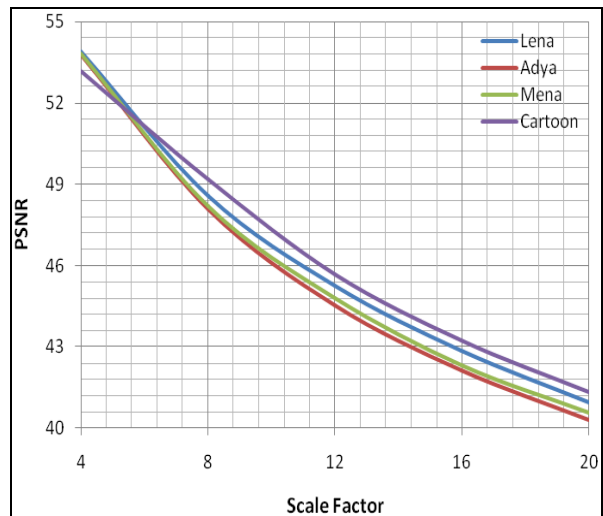
Test Image Name	Scale Factor	SSIM	PSNR
lena.jpg	4	0.9975	53.9048
	8	0.9923	48.5792
	12	0.9843	45.2463
	16	0.9741	42.8489
	20	0.9625	40.9421
adya.jpg	4	0.9985	53.7807
	8	0.9944	48.0892
	12	0.9887	44.5386
	16	0.9811	42.1304
	20	0.9732	40.3011
mena.jpg	4	0.9980	53.8349
	8	0.9935	48.1768
	12	0.9863	44.8029
	16	0.9779	42.3093
	20	0.9688	40.5498
cartoon.jpg	4	0.9983	53.1693
	8	0.9951	49.1774
	12	0.9898	45.6878
	16	0.9829	43.2159
	20	0.9748	41.3311

In the Table 2, the display of the Perceptual invisibility of the Watermarked images by taking Scale factors from 4 to 20 in terms of evaluated values of the respective SSIM and PSNR index is shown. The method accessed through SSIM, the minimum value obtained is 0.9625 and the maximum value is 0.9985. When the method is accessed through PSNR, the minimum value obtained is 40.3011 where the maximum value is 53.9048. It was observed from the table that, when the value of the Scaling factor is increased, the feature of the watermarked image is exaggerated. Plot 1 shows the graphical representation on SSIM verses Scaling factor for all test images where Plot 2 gives the representation on PSNR obtained against Scaling factors.

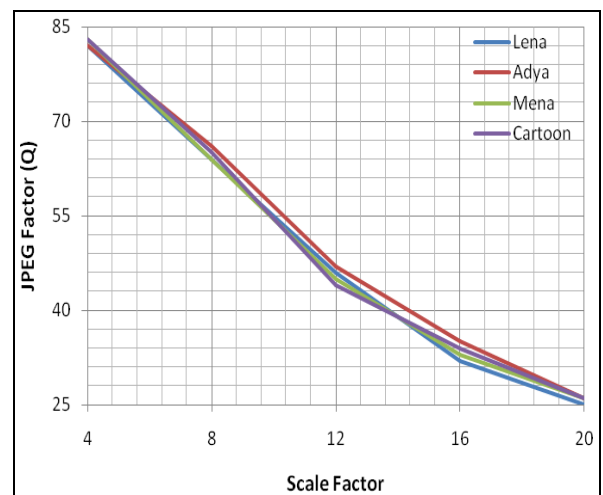
Plot 1: SSIM with Walsh code 8 against Scale factor



Plot 2: PSNR with Walsh code 8 against Scale factor







Plot 3: JPEG factor (Q) with 2-D Walsh code 8 against Scale factor for Binary signature recovery.



During the evaluation, the detail lowest JPEG Quality factor obtained for Scaling factors 4 to 20 is shown in

Table 3. It gives the report on the lowest Q with Walsh code 8 below which the Binary signature cannot be recovered. From the table it is observed that the value of the JPEG Quality factors varies from 83 to 25. Plot 3 gives the representation on the effect of JPEG Quality factor against the Scale factor.

Table 3. Lowest JPEG factor Q for 2-D Walsh coded extracted Binary signature under JPEG attack.

Test Image	Scale Factor	JPEG factor (Q)	Recovery of binary signature at Scale factor 20
lena.jpg	4	82	
	8	64	
	12	46	
	16	32	
	20	25	
adya.jpg	4	82	
	8	66	
	12	47	
	16	35	
	20	26	
mena.jpg	4	83	
	8	64	
	12	45	
	16	33	
	20	26	
cartoon.jpg	4	83	
	8	65	
	12	44	
	16	34	
	20	26	

From the observation it was found that by applying 2-D Walsh coding to the Watermarks before embedding into the DCT blocks provides elevated robustness against JPEG attacks. It is also experimented that the proposed technique of Watermarking can continue to exist against high JPEG compression ratios. It is also ensured that increase in the range of Scaling factors will provide the increase in robustness of the algorithm at the disbursement of enhancing the distortion happened to the Watermarked images.

Finally the proposed technique was validated against different standard and nonstandard attacks by using the StirMark tool which is a standard benchmark. The validation was performed on the image lena.jpg under scaling factor 20. The detail observation on the StirMark attacks and their respective NC values are shown in Table 4. It is observed that the Binary signature successfully recovered under different attacks.

Table 4. NC values for Lena image with Scale factor 20 at StirMark attacks.

Attack	NC with Walsh 4 Walsh-4
Additive Noise- 0.2	1
Additive Noise- 0.5	1
Additive Noise- 0.7	1
Additive Noise- 0.9	1
JPEG-20	0.9813
JPEG-30	0.9958
JPEG-75	1
Median 3X3	0.9457
Median 5X5	0.9882
PSNR-50	1
PSNR-70	1
PSNR-90	1
Rotation-0.5°	0.9883
Rotation-1.0°	0.9892

V. CONCLUSION

In this work, a blind technique for Watermarking algorithm was proposed by applying two-dimensional Walsh coding of length eight to embed the Watermarks in the DCT blocks after converting the Host image into its equivalent YCbCr colour space. The embedding is carried out in five low frequency coefficient of DCT. The proposed scheme produced minimum distortion on the Watermarking images. The algorithm prepared to embed Binary signature as Major Watermark and Biometric fingerprint is also embedded secondly to be utilized as Authentication matching during the process of extraction. The algorithm is found to be more sensitive against robustness and against JPEG compression and the common Watermarking attacks of image processing by the use of 2-D Walsh code. The technique is proving to be blind as the Major Watermark can be extracted without the use of original image. It is concluded that, increase in the range of Scaling factors will provide the increase in robustness of the algorithm at the disbursement of enhancing the distortion happened to the Watermarked images. The distortion created by the proposed Watermarking algorithm was validated using their respective PSNR and SSIM index values.

ACKNOWLEDGMENT

This paper is fully supported by the department of Electronics & Telecommunication Engineering under Indira Gandhi Institute of Technology, Sarang, Odisha, India for Utkal University, Odisha, India.

REFERENCES

- [1] Er-Hsien Fu, "Literature Survey on Digital Image Watermarking" *EE381K Multidimensional Signal Processing*.
- [2] I. Cox, M. Miller, and J. Bloom, *Digital Watermarking, Morgan Kaufmann Publishers*, San Francisco, 2001.
- [3] F. Hartung and M. Kutter, "Multimedia Watermarking Techniques", *Proc. IEEE*, Vol.87, no.7, pp 1079-1107, 1999.
- [4] Wai Chu, "DCT-Based Image Watermarking Using Sub sampling." *IEEE Transactions on Multimedia*, Mar. 2003. pp. 34-38.
- [5] Min-Jen Tsai, Hsiao-Ying Hung, "DCT and DWT-Based Image Watermarking by Using Sub sampling" *Proceedings of the 24<sup>th</sup> International Conference on Distributed Computing Systems Workshops, MNSA (ICDCSW'04)*, March 23 - 24, 2004, Hachioji, Tokyo, Japan, pp. 184-189.
- [6] M. Barni, F. Bartolini, V. Cappellini, and A. Piva, "A DCT-Domain System for Robust Image Watermarking," *Signal Processing*, vol. 66, 1998, pp. 357-372.
- [7] Beauchamp K G "Walsh functions and their applications", *London: Acad Press*, 1975.
- [8] Al-Gindy, A. Tawfik H. Al- Ahmad and R. Qahwaji, "Enhanced DCT Based Technique with Shuffle Scheme For Robust Image Watermarking of Handwritten Signatures", *International Conference for Communication, Computer and Power (ICCCP)*, Oman, February 2007, pp.450-455.
- [9] A. Al-Gindy, A. Tawfik H. Al- Ahmad and R. Qahwaji, "A New Blind Image Watermarking Of Handwritten Signatures using Low-Frequency Band DCT coefficients", *IEEE International Conference on Signal Processing and Communications (ICSPC)*, November 2007, pp.1367-1370.
- [10] A. Al-Gindy, H. Al-Ahmad, R. Qahwaji and A. Tawfik, "Watermarking of Color Images in the DCT Domain Using Y Channel", *IEEE/ACS International Conference on Computer Systems and Applications*, May 2009, pp.1025-1028.
- [11] A. Al-Gindy, A. Tawfik H. Al Ahmad and R. A. Qahwaji, "A New Blind Image Watermarking Technique for Dual Watermarks Using Low-Frequency Band DCT Coefficients", *IEEE International Conference on Electronics, Circuits and Systems (ICECS)*, 2007, pp.538-541.
- [12] Hou Wang, A. C. Bovik, H. R. Sheikh, E. P. Simoncelli "Image Quality Assessment: From Error Visibility to Structural Similarity", *IEEE Transaction on Image Processing*, Vol.13, No.4, April 2004, pp.600-612.
- [13] A. Bin Sewaif, H. Al-Ahmad, and M. E. Al-Mualla, "2-D Walsh Coding for Robust Digital Image Watermarking," *Signal Processing and Information Technology (ISSPIT)*, December 2004.
- [14] B P Mishra, H.N.Pratihari & P.Das "DCT Based Grey Scale Still Image Watermarking Using 1-D Walsh Code and Biometric Protection" *IJETCS*, Vol-4, Issue-2, 2015, pp28-32.
- [15] <http://www.images.google.com>
- [16] [http://en.wikipedia.org/wiki/Fingerprint\\_recognition](http://en.wikipedia.org/wiki/Fingerprint_recognition).
- [17] B.P.Mishra, H.N.Pratihari & P.Das "Twofold watermarking technique for enhancement of security in grey scale still image", *Journal of Emerging trends in computing and Information Science*, Vol-6, Issue-3, 2015, pp174-179.
- [18] B.P.Mishra, H.N.Pratihari & P.Das " Copyright protection in Grey scale image by applying dual Watermarking and

2-D Walsh Coding" , *International Journal of Graphics and Image Processing*, Vol-5, Issue-2, 2015, pp56-61.

### Authors' Profiles



**B P Mishra**, male, is a research scholar at Indira Gandhi Institute of Technology, Sarang an Autonomous Institute of Government of Odisha, India. He is currently working towards the Ph.D degree in the Electronics & Telecommunication Engineering at IGIT Sarang under Utkal University. He has completed his M.Tech degree from Biju Patnaik University of Technology, Odisha, India. His research interests include Digital Image Processing, Image Security and Signal Processing.



**H N Pratihari**, male, is a Professor in the department of Electronics & Telecommunication Engineering at Calcutta Institute of Technology, Westbengal, India. He has completed his M.Tech from National Institute of Technology, Rourkela and PhD from Utkal University, Bhubaneswar, Odisha. He has published number of research Papers and conference papers in both national and international level. His research interests are control System Engineering, Digital Image Processing and Power Electronics.



**P Das**, female, is an Associate Professor in the department of Electrical Engineering at Indira Gandhi Institute of Technology, Sarang an Autonomous Institute of Government of Odisha, India. She has made her M.Tech & PhD from Indian Institute of Technology, Kharagpur, India and Engineering graduation from Sambalpur University, Odisha, India. She has published number of research and conference papers in both national and international forum. Her area of research interests are Image Processing and Signal Processing.