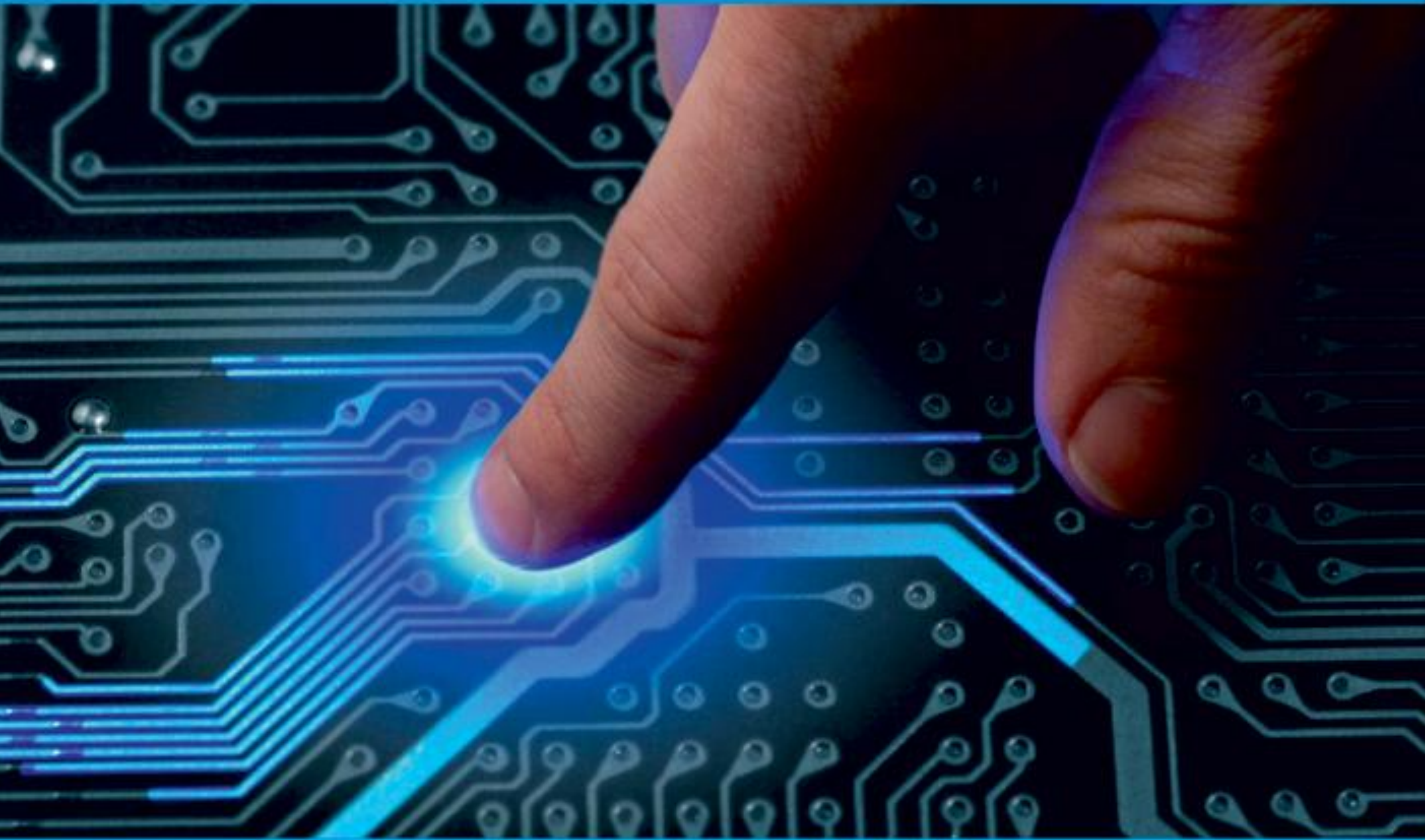
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 7, July 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907185 |

Machine Learning for Enhanced and Improved Algorithms Selection Basis on Performance in the Application of Image Watermarking

Shailesh Sakpal , Prof. B. G. Hogade

Research Scholar, Terna Engineering College, Navi Mumbai. Mumbai University, India

Professor, Terna Engineering College, Navi Mumbai. Mumbai University, India

ABSTRACT: Symbols are watermarked into various images, marketing documents, videos and multimedia files before circulating on social media for authenticity and ownership. Digital image watermarking techniques is found suitable for invisible symbol watermarking that is imperceptible and robust to common attacks. In this paper, an image watermarking technique using adaptive wavelet texture features domain through encryption and Bhattacharya distance. The fundamental concept explored is to fragment the carrier image in time domain into four partial non overlapping regions whereas symbol image is encrypted. Symbol image is encrypted based on Rubik's Cube principle through random key generated. Subsequently statistical parameters such as mean (degree 1), standard deviation (degree 2), skew (degree 3), kurtosis (degree 4) and variance are calculated. These parameters are calculated through wavelet coefficients obtained from the regions of carrier image and encrypted symbol, which are further applied to obtain Bhattacharya distance. Minimum Bhattacharya distance is applied criteria between the subbands of regions of carrier image and symbol for embedding in wavelet domain. Also the embedding coefficient is calculated through Bhattacharya distance for invisible watermarking. Robustness, imperceptibility and signal to noise ratio were measured on multiple carrier and symbol images under common attacks, which yield better results.

KEYWORDS: Adaptive watermarking technique, Encryption, Texture feature, Wavelet Transform, Skew, Kurtosis, Variance, Bhattacharya distance, Image processing attacks.

I. INTRODUCTION

Tremendous growth in the internet technology, mobile devices and android applications, large number of images, documents, videos and multimedia files are shared on android applications such as Tik Tok, Helo, etc and social media websites such as Facebook, Instagram, etc. Handling, repetition and tempering of files is now very easy task since access to data / information through numerous signal and image processing algorithms. Moreover an original copy of all digital files is not different from the original file. Henceforth copyright protection and owner authentication is extremely important and become one of the most challenging tasks [1 – 3]. Watermarking has been proved to be an efficient tool for the protection of copyright of multimedia contents. Encryption / decryption algorithms can be applied to restrict access to the symbol or watermark. Encryption algorithm is suitable for the symbol or watermark that can be manipulated and freely shared over the network. Therefore it is necessary to develop a watermarking algorithm that would enforce copyright protection and ownership of the multimedia files used in the social media websites. However continued efforts are required to improve its performance due to new requirements and challenges such as multiple attacks and information sharing on social media websites [4] – [6]. These symbol images are subject to multiple genuine and malicious image processing attacks. It may result in partial damage to underlined symbol watermark. However malicious attacks like duplication by partial or complete removal of symbol watermark from the media files and plagiarising through copying and cropping data. Encryption through Rubik's Cube principle [7] – [9] has certain advantages over other encryption algorithms especially in watermarking. Firstly iterations in this encryption algorithm generate various patterns that can be used to obtain minimum Bhattacharya distance enhancing the watermark embedding efficacy. Secondly it is based on row and column rotations and simple mathematical operations require less processing time. Finally it provides necessary security to the symbol or watermark through private key.

1.1 Related Work

The primary objective of the symbol watermarking is to establish the authenticity of the documents, multimedia files, brochures and marketing materials [10] – [12]. Therefore indeed it requires handling of image imperceptibility, better

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

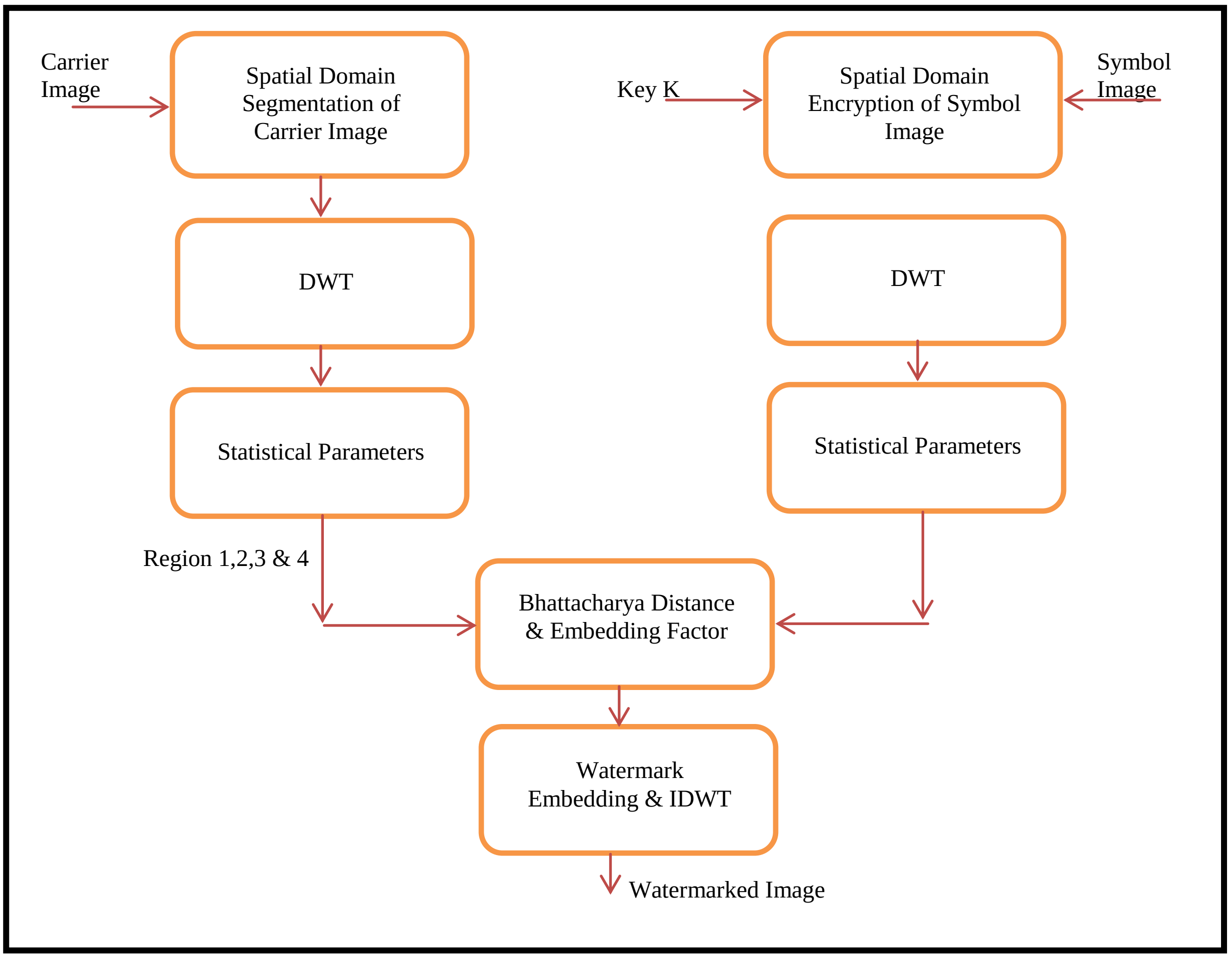
| DOI: 10.15680/IJIRCCE.2021.0907185 |

resistant to several attacks, robustness, accommodate large number of symbols and carrier images. Previous work on invisible watermarking was concentrated on symbols that represent the signature. Discrete wavelet transform (DWT), Discrete Cosine Transform (DCT) and FFT are efficient techniques in transformed domain that decomposes carrier and symbol image into several frequencies. These transform domain techniques are computationally efficient and can be implemented using convolution operation [13] – [16]. In [17] entropy of the wavelet subbands of the carrier and symbol image was calculated for watermarking and maximum entropy subband was selected, also subbands of the symbols were shuffled to achieve robustness. In [6] Fuzzy inference models was employed to generate the weighing factor for embedding the watermark and input to the Fuzzy Inference System was taken from the Human Visual System model. It was demonstrated that the proposed system using fuzzy inference system that exploits fuzzy logic was indeed effective. Watermarking algorithm using DWT and edge insertion of the symbol was demonstrated in [18], it uses HH subband of the carrier image for watermark embedding. In [19] – [20] logo or symbol was encrypted through random key and watermarked into carrier image using wavelet transform. Encryption or scrambling using Arnold transform was used to enhance the robustness of the algorithm thereafter the symbol was embedded into LL subband of the carrier image. However it is desired to build an invisible symbol watermarking technique that employs previously known techniques but adopting adaptive techniques without sacrificing on the security of the symbol through encryption. Most importantly it is desired develop watermarking robust to common image processing attacks such as noise, compression, geometrical and cropping.

1.2 Organization of the paper

The paper is organized as follows section I introduces to watermarking, section II describes embedding and extraction algorithm in details. Results are discussed in section III and finally concluded in section IV.

Figure 1 Proposed adaptive watermarking embedding technique through encryption and wavelet texture feature



| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |
|| Volume 9, Issue 7, July 2021 ||
| DOI: 10.15680/IJIRCCE.2021.0907185 |

II. PROPOSED ADAPTIVE WATERMARKING TECHNIQUE THROUGH ENCRYPTION AND WAVELET TEXTURE FEATURE

In this paper, symbol watermarking technique through adaptive water marking in wavelet domain, encryption, statistical parameters and Bhattacharya distance depicted in figure 1 is presented. The carrier image is segmented into four different non overlapping regions as depicted in figure 2. Symbol image is encrypted based on Rubik's Cube principle through random key k generated. Next statistical parameters such as mean, standard deviation, skew, kurtosis and variance are calculated from the wavelet coefficients of each regions of carrier image and symbol [1] given in equation (1) – (5). These statistical parameters of regions of carrier image and symbol are used to obtain Bhattacharya distance [1]. Finally the one out of four bands of symbol is embedded into each the region of carrier image with minimum Bhattacharya distance equation (6) in wavelet domain. Also the embedding coefficient is calculated through Bhattacharya distance for invisible watermarking. Thus it exploits the mixed spatial and frequency domain segmentation of the carrier image of and symbol for better texture matching. The watermarked embedded image is obtained and thus it completes the process of watermark embedding. The resultant image contents watermark whose visibility can be controlled using parameter alpha through k [1]. The texture features are invariant with respect to translation and rotation of the image. Thus both provide the much needed robustness to algorithm. Watermarking parameters original carrier and symbol embedded carrier image was determined to evaluate the performance of the proposed algorithm. Watermark extraction algorithm also includes stages such as segmentation, DWT, parameter extraction, computing Bhattacharya distance and symbol extraction in wavelet domain. Watermark extraction is almost reverse process of watermark embedding depicted in figure 3.

$$\text{Mean } \mu_{mn} = \frac{E_{mn}}{P\ x\ q} \quad (1)$$

$$\text{Standard deviation } \sigma_{mn} = \frac{\sqrt{\sum_x \sum_y (|G_{mn}(x,y)| - \mu_{mn})^{\ 2}}}{(P\ x\ q) - 1} \quad (2)$$

$$\text{Variance } v_{mn} = \frac{\sum_x \sum_y (|G_{mn}(x,y)| - \mu_{mn})^{\ 2}}{(P\ x\ q) - 1} \quad (3)$$

$$\text{Skew } \alpha_{mn} = \frac{\sum_x \sum_y (|G_{mn}(x,y)| - \mu_{mn})^{\ 3}}{\sigma^3} \quad (4)$$

$$\text{Kurtosis } \gamma_{mn} = \frac{\sum_x \sum_y (|G_{mn}(x,y)| - \mu_{mn})^{\ 4}}{\sigma^4} \quad (5)$$

Where G_{mn} are the wavelet coefficients

$$d_{xy} = 0.125 * \left(\frac{(\mu_x - \mu_y)}{v_{xy}}\right) * \left(\frac{(\mu_x - \mu_y)}{v_{xy}}\right)^T + 0.5 * \log\left(\frac{v_{xy}}{\sqrt{v_x + v_y}}\right) \quad (6)$$

$$\text{Where} \quad v_{xy} = \frac{(v_x + v_y)}{2} \quad (7)$$

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907185 |

Figure 2 Spatial domain regions of carrier image

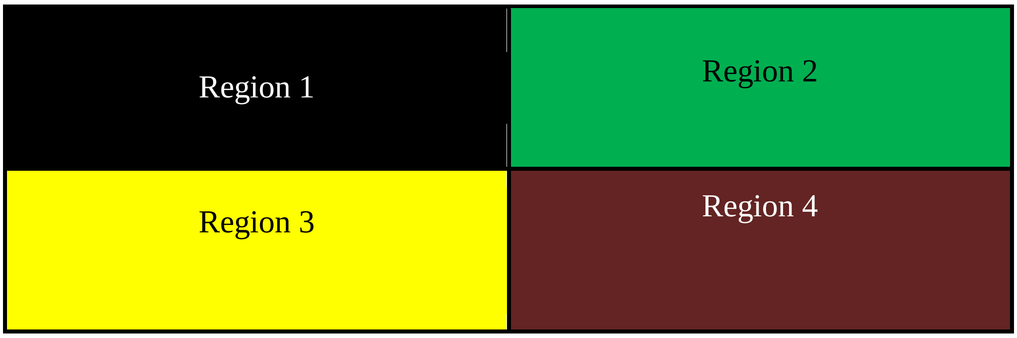
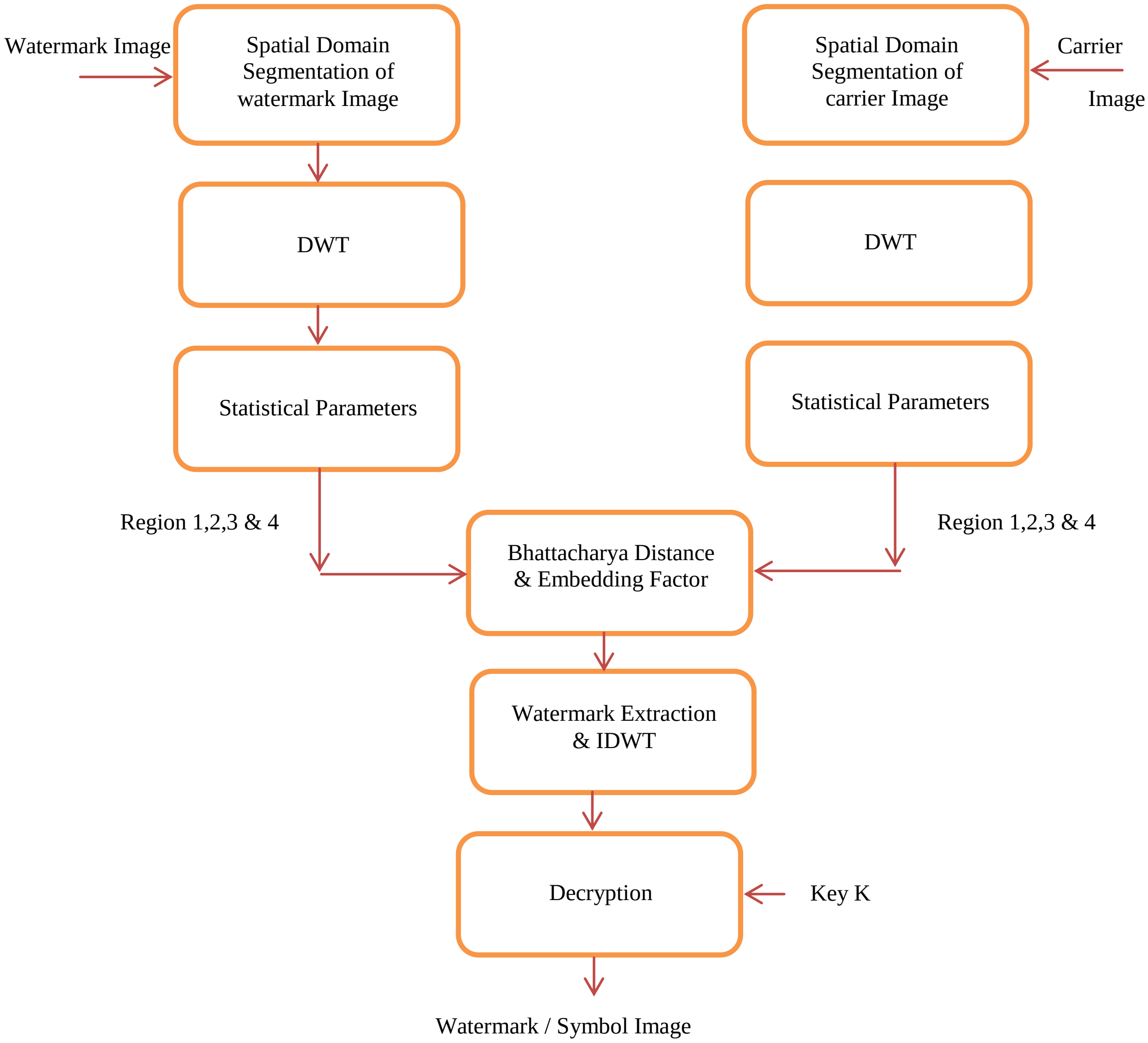


Figure 3 Proposed adaptive watermarking extraction technique



III. EXPERIMENTAL RESULTS & DISCUSSION

Primary objective of this session is to evaluate the qualitative and quantitative performance of the proposed adaptive wavelet texture features domain through encryption and Bhattacharya distance. Experiments through software

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907185 |

simulation using MATLAB were carried to determine the watermarking parameters on three sets of carrier images. These carrier images were classified based on entropy, the 8-bit image with entropy close to eight (8) contents rich texture whereas the entropy close to six(6) contents significantly lesser details. Figure 4 depicts an image from these three categories of carrier images with varied entropy and symbol image. Peak signal to noise ratio (PSNR) and normalized cross correlation coefficients (NCC) are employed to evaluate the performance in terms of imperceptibility and robustness of the proposed algorithm. Furthermore it was desired to encrypt symbol image that enables to generate various patterns in encrypted domain. These patterns facilitates algorithm to embed the texture features to achieve robustness to attacks such as noise, geometric and compression. Robustness of the algorithm was measured through geometrical attack such as rotation, salt and pepper noise and JPEG compression attack mostly applied in image processing systems. Embedding factor controls the visibility of the watermark and is calculated using Bhattacharya distance.

Figure 4 Carrier and symbol image with their respective entropy

(a) Greeting card

(b) Brochure

(c) Letter

(d) Symbol or logo

Figure 5 Encryption of symbol images using Rubik's Cube Principle

(a) Color (b) Grey scale (c) Encrypted (d) Decrypted

Experimental results are demonstrated in figure 5 & 6 which clearly shows the images at various stages of algorithm. The encrypted and decrypted symbol images are depicted in figure 5, the visual appearance clearly shows the difference between original and encrypted image. Figure 6 shows the images obtained during watermark embedding and extraction process. Table 1 & 2 list the measured parameters PSNR and NCC for the retrieved watermark image

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

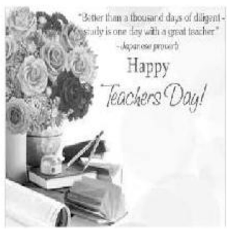
| DOI: 10.15680/IJIRCCE.2021.0907185 |

without and with attack respectively which depicts the robustness of the algorithm. Comparison of watermarking parameters with other methods is listed in table 3 which illustrates better method for watermarking.

Figure 6 Symbol images embedded and extracted without / with attack

Carrier image

Symbol image



Watermarked image

Extracted symbol with no attack

Extracted symbol with noise attack

Carrier image

Symbol image

Watermarked image

Extracted symbol with no attack

Extracted symbol with geometric attack

Table 1 Parameters without attack

Parameters	Greeting Card	Letter	Brochure
PSNR (dB)	60.24	61.77	62.1
NCC	0.84	0.88	0.91

Table 2 Parameters with attack

Attacks	Parameters	Greeting Card	Letter	Brochure
Noise	**PSNR (dB)**	40.12	39.7	39.17
	NCC	0.54	0.51	0.52
Geometric	**PSNR (dB)**	36.5	36.55	35.99
	NCC	0.67	0.69	0.66
Compression	**PSNR (dB)**	33.64	35.66	36.73
	NCC	0.61	0.62	0.61

Table 3 Comparison of results under geometric attack

Parameters	[21]	Our Work
PSNR (dB)	22.49	35.99
Bit error rate	0.3086	0.28

IV CONCLUSION

An image watermarking technique using adaptive wavelet texture features domain through encryption and Bhattacharya distance is attempted successfully. The fundamental concept explored is to fragment the carrier image in time domain into four partial non overlapping regions whereas symbol image is encrypted. Symbol image is encrypted based on Rubik's Cube principle through random key generated. Subsequently statistical parameters such as mean (degree 1), standard deviation (degree 2), skew (degree 3), kurtosis (degree 4) and variance are calculated. These parameters are calculated through wavelet coefficients obtained from the regions of carrier image and encrypted

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907185 |

symbol, which are further applied to obtain Bhattacharya distance. Minimum Bhattacharya distance is applied criteria between the subbands of regions of carrier image and symbol for embedding in wavelet domain. Encryption through Rubik's Cube principle enables better texture matching between symbol and carrier image along with benefits of security. Adaptive texture matching enhances robustness and imperceptibility which is effectively applicable using Bhattacharyya distance. The proposed adaptive algorithm is resistant to geometric, noise and compression attack, further investigation is required to ascertain completeness of the algorithm.

REFERENCES

[1] Prashant Vaidya, et al, "Digital Watermarking for Copyright Protection of Digital Images in Wavelet Domain," in 2nd International Symposium on Computer Vision & Internet Published by Elsevier Procedia Computer Science 58, pp 233 – 240, 2015.

[2] Allaf Hassani and M. Ait Kbir, "A Review of Digital Watermarking Applications for Medical Image Exchange Security", Springer Nature Switzerland AG 2019, pp. 472–480, 2019.

[3] Lei Chen and Jiying Zhao, "Adaptive Digital Watermarking Using RDWT and SVD," in IEEE International Symposium on Haptic, Audio and Visual Environments and Games (HAVE), 2015.

[4] Deepti Shukla, Nirupama Tiwari and Deepika Dubey, "Survey on Digital Watermarking Techniques," in International Journal of Signal Processing, Image Processing and Pattern Recognition Vol.9, No.1, pp.239-244, (2016).

[5] Peng F, et al, "Adaptive reversible data hiding scheme based on integer transform," in Signal Processing, vol. 92, issue 1, pp 54 – 62, 2016.

[6] B. Jagadeesh, et al, "Fuzzy Inference System Based Robust Digital Image Watermarking Technique using Discrete Cosine Transform," in International Conference on Information and Communication Technologies, published by Elsevier Procedia Computer Science 45, pp 1618 – 1625, 2015.

[7] Khaled Loukhaoukha, Jean-Yves Chouinard, and Abdellah Berdai, "A Secure Image Encryption Algorithm Based on Rubik's Cube Principle," in Hindawi Journal of Electrical and Computer Engineering, Volume 2012, pp 1 – 14, 2012.

[8] G. Bhatnagar, Q. J. Wu, and B. Raman, "A new fractional random wavelet transform for fingerprint security," in IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans, 42, (1), pp. 262–275, (2012).

[9] B. Norouzi, S. M. Seyedzadeh, S. Mirzakuchaki, and M. R. Mosavi, "A novel image encryption based on row-column, masking and main diffusion processes with hyper chaos," in Springer Multimedia Tools and Applications, pp. 1–31, 2013.

[10] M. Natarajan and G. Makhdumi, "Safeguarding the digital contents: Digital watermarking," DESIDOC J. Library Inf. Technol., vol. 29, no. 3, pp. 29–35, 2009.

[11] C. I. Podilchuk and E. J. Delp, "Digital watermarking: Algorithms and applications," IEEE Signal Process. Mag., vol. 18, no. 4, pp. 33–46, Jul. 2001.

[12] X. Zhao and A. T. S. Ho, "An introduction to robust transform based image watermarking techniques," in Intelligent Multimedia Analysis for Security Applications, vol. 282. Berlin, Germany: Springer-Verlag, 2010, pp. 337–364.

[13] L. R. Roldan, M. C. Hernández, J. Chao, M. N. Miyatake and H. P. Meana, "Watermarking-based Color Image Authentication With Detection And Recovery Capability," in IEEE Latin America Transactions, Vol. 14, No. 2, pp 1050 - 1057, 2016.

[14] Aniket Roy, Arpan Kumar Maiti, Kuntal Ghosh, "A perception based color image adaptive watermarking scheme in YCbCr space," in 2nd IEEE International Conference on Signal Processing and Integrated Networks (SPIN), 2015.

[15] Navneet Yadav, Kulbir Singh, "Transform Domain Robust Image-Adaptive Watermarking: Prevalent Techniques and Their Evaluation," in IEEE International Conference on Computing, Communication and Automation, 2015.

[16] Deepti Shukla, Nirupama Tiwari and Deepika Dubey, "Survey on Digital Watermarking Techniques," in International Journal of Signal Processing, Image Processing and Pattern Recognition Vol.9, No.1, pp.239-244, 2016.

[17] Hai Tao, et al, "Robust Image Watermarking Theories and Techniques: A Review," in Journal of Applied Research and Technology, Vol. 12, pp 122 – 138, (2014).

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907185 |

[18] Henri Bruno Razafindradina, Attoumani Mohamed Karim, “Blind and robust images watermarking based on wavelet and edge insertion”, International Journal on Cryptography and Information Security (IJCIS), Vol.3, No. 3, 2013.

[19] Pushpa Mala S., et al, “Digital Image Watermarking Techniques: A Review,” in International Journal of Computer Science & Security, vol. 9, issue 3, pp 140 – 156, 2015.

[20] Emanuele Maiorana, et al, “High-capacity watermarking of high dynamic range images,” in Springer EURASIP Journal on Image and Video Processing, 2016.

[21] Lin Sun, Jiucheng Xu, Xingxing Zhang,1 and Yun Tian, “An Image Watermarking Scheme Using Arnold Transform and Fuzzy Smooth Support Vector Machine,” in Hindawi Publishing Corporation Mathematical Problems in Engineering, Volume 2015, pp 1 – 14, 2015.