DOI: 10.21917/ijivp.2018.0255

A ROBUST NON-BLIND HYBRID COLOR IMAGE WATERMARKING WITH ARNOLD TRANSFORM

Mahendra Kumar Pandey, Girish Parmar and Rajeev Gupta
Department of Electronics Engineering, Rajasthan Technical University, India

Abstract

Due to development of the internet technologies and other services, requirement of rightful ownership and copyright is highly required. Hence to protect the copyrighted data from unauthorized user, a robust non-blind hybrid color image watermarking scheme is presented. In this proposed scheme, we use color watermark instead of gray watermark which is generally used in most of the existing digital image watermarking techniques. YC_bC_r color space used to separate the R, G and B channel of images. Y channel of color watermark is embedded into corresponding Y channel of cover image using proposed scheme. Arnold transform are used to scramble the watermark image before embedding process in order to provide more security. The singular value of bands is going to embed with singular values of watermark by making use of variable scaling factor (α). As original image is required at the time of extraction of watermark hence propose scheme belong to non-blind technique group. The two-fidelity parameter namely Peak signal to noise ratio (PSNR) and structural similarity (SSIM) index are used to measure the imperceptibility whereas similarity between original and extracted watermark is measured by using normalized correlation coefficient (NCC). We also compared the results of proposed scheme with other existing watermarking schemes. The experimental results prove effectiveness of the proposed image watermarking scheme in term of robustness and imperceptibility.

Keywords:

Watermarking, Copyright Protection, Stationary Wavelet Transform, Singular Value Decomposition (SVD), Arnold Transform, PSNR, SSIM, NCC

1. INTRODUCTION

With the digitalization and distribution of multimedia data over the internet, it is very important to protect multimedia data by unauthorized user. In past decade, researchers worked very hard on this issue and proposed many different methods for the protection of multimedia data. From last decades digital watermarking has been seen as an effective method for copyright protection and an unauthorized manipulation of the multimedia [1] over existing methods of protection such as cryptography, encryption, steganography etc.

Digital Watermarking is an authentication technique which permanently embeds a digital signal (watermark) in text, image, audio, video files (any Data) by slightly modifying the data without creating any harmful effects on the original data. The embedded watermark may contain information such as identification of the product's owner, user's license information etc. Normally, the image watermarking can be done in spatial domain or in transform domain [2]-[5].

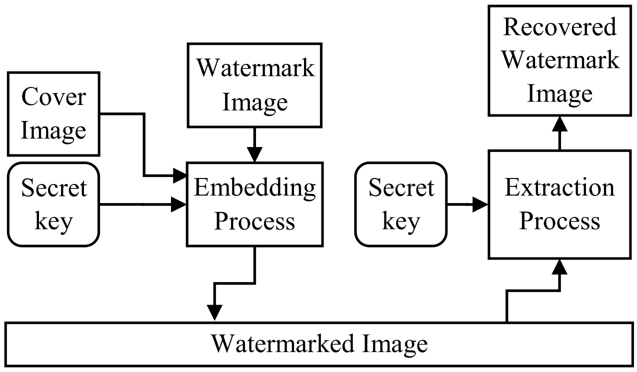


Fig.1. A generic diagram of digital watermarking

In comparison to spatial domain technique, the transform domain-based image watermarking techniques indicate the better performance in term of imperceptibility and robustness criteria [6-8]. In the literature, there are various transform-domain based image watermarking technique like Discrete Wavelet Transform (DWT), the Discrete Cosine Transform (DCT) and Discrete Fourier Transform (DFT) and stationary wavelet transform (SWT) etc. are available. As we know due to excellent spatial localization and multi-resolution characteristics of DWT which are very close to the theoretical models of the human visual system [13], it has been used popularly and more frequently used in watermarking field. Opposite to this, DWT have some drawbacks like down-sampling of its bands etc. As a result of this down sampling, potentially valuable information of image may be removed which are not important to reproduce the image. Due to these rejected coefficients, there observed a little bit shift in the image. The shift variance of DWT causes inaccurate extraction of the cover and watermark image. To solve this problem associated with DWT method, in this paper we propose a method using stationary wavelet transform in association with SVD which is more robust against attacks then traditional methods.

This paper mainly focuses on the protection of color images from its unauthorized utilization using a novel digital color image watermarking method. Previously, Agreste and Andaloro [6] developed a DWT-based method for any size of image which implants watermark data into high-frequency sub-bands of DWT coefficient. This watermarked data is imperceptible as per human visual system (HVS) directions. Later, Agreste and Andaloro [7] modified the previous method by changing the filer bank by Daubechies-2 and observed that it is more robust to geometric, filtering, and Stir Mark attacks with a low rate of false alarm. Vahedi et al. [8] exploited the advantage of symlet-4 filter bank to increase the quality and robustness of watermarking method as compared to existing methods. Vahedi et al. [8] showed that three level decomposition with all the four subspaces namely; approximation, horizontal, vertical, and diagonal along with symlet-4 filter bank provide better results for image watermarking.

Golea et al. [9] proposed the SVD-based RGB color image watermarking for embedding the color RGB watermark into the RGB host image. Manish et al. [11] proposed a DWT-based image watermarking method using uncorrelated color space (UCS) with GA. In this paper, Manish et al. used three level DWT to embed the watermark. However due to down sampling of its bands and shift variance causes the less precise extraction of the cover and watermark image which is generally observed in DWT. To solve the problems, hybridization of Stationary Wavelet Transform (SWT) in association with singular value decomposition (SVD) has been presented in the proposed work [12] - [13].

Rest of the paper is organized as follows. Section 2 describes methodology overview and security key in this paper. The proposed method has been described in section 3. Section 4 describes the fidelity parameters, experimental results and discussions whereas the comparative analysis with existing schemes have been given in sections 5. Finally, conclusions of paper followed by future work presented in section 6.

2. METHODOLOGY OVERVIEW

In this section, methodology overview of SWT, SVD, and security key used in the proposed approach has been described.

2.1 OVERVIEW OF STATIONARY WAVELET TRANSFORM (SWT)

Discrete Wavelet transform (DWT) is a mathematical tool for hierarchically decomposing an image. DWT analyze a digital image at different frequency bands with different resolutions by decomposing the image into its coefficients which is generated by the different filters. But due to some drawbacks of DWT like down-sampling of its bands and shift invariance, it causes inaccurate extraction of the cover and watermark image. To overcome the drawbacks of DWT, we use stationary wavelet transform (SWT). Due to translation-invariance property of SWT, it is more efficient than other wavelet-based transforms technique. In SWT, the output of each level contains the number of samples equal to the input due to redundancy. Hence when an image decomposed at N levels, there is a redundancy of N in the wavelet coefficients. By using SWT, any image can be decomposed into four sub-band with null placing procedure. The Fig.2 show the LL (Approximation), HL (Vertical), LH (Horizontal), HH (Diagonal) sub-band of an image [5].

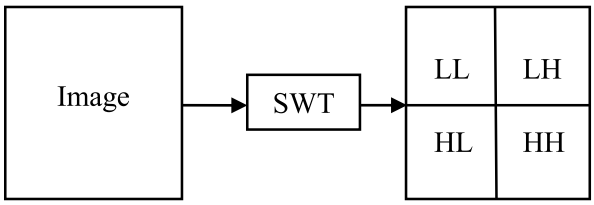


Fig.2. SWT decomposition of image at level-1

2.2 OVERVIEW OF SINGULAR VALUE DECOMPOSITION (SVD)

SVD is linear algebra technique which efficiently represents intrinsic algebraic properties of an image. SVD decomposed an image represented by $m\times n$ matrix (M) into two orthogonal matrices (U and V) and one diagonal matrix S whose entries are known as a singular value of the matrix C. This type of decomposition is called Singular Value Decomposition of M and can be expressed as

$$M = U\Sigma V^T \tag{1}$$

where U is a $m\times n$ matrix with orthogonal columns known left singular vector, Σ =diag(σ_1, σ_2,..., σ_n) is an $n\times n$ diagonal matrix having nonnegative singular values as a diagonal element arranged in descending order and V is an $m\times n$ matrix with orthogonal columns known as right singular vectors.

If rank (M) = r, then Σ satisfies $\sigma_1 \geq \sigma_2 \geq \ldots \geq \sigma_r \geq \sigma_r+1 = \sigma_r+2 = \ldots\ \sigma_n = 0$.

The SVD efficiently represents intrinsic algebraic properties of an image, where singular values correspond to brightness of the image. Since singular matrix has many small singular values which reflect geometrical features of the image. Hence slight variations in singular values of an image may not affect the visual perception of original image. To take the advantage of this features, watermark embedding through slight variations of singular values in the segmented image has been introduced as a choice for robust watermarking [14-16].

2.3 SECURITY KEY FOR WATERMARK IMAGE

As our aim to provide the extra level of security to the proposed method, here we use Arnold transform with number of iteration as a security key to add one more level of security for extraction of the watermark image from watermarked image.

2.3.1 Arnold Transform:

The Arnold transform, also commonly known as cat-face transformation, or cat-face mapping, was introduced by Arnold. For an image C with N*N size, the Arnold transform operation on the position (x,y) pixel is given by

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod N \tag{2}$$

The Arnold transform, which changes the positions of the pixels, can be repeated many times in order to obtain a scrambled image. However, due to the periodicity of the Arnold transformation, the original image can be restored after a certain number of iterations [10].

2.3.2 Anti-Arnold Transform:

Use of the Arnold transform periodicity on a scrambled image to recover the original image could be achieved at the expense of possibly a large computational complexity depending on how many iterations have already been used to obtain the scrambled image. The anti-Arnold transform is given by

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} \bmod N \tag{3}$$

If a scrambled image is obtained by using n iterations of the operation of the Arnold transform, it needs the same number of iterations to recover the original image using the anti-Arnold transform. Hence to recover the original image, anti-Arnold transform can provide significant savings in computation, if $n << T_n$ [10].

3. PROPOSED WATERMARKING METHOD

Here, we propose an Arnold integrated hybrid image Watermarking Technique based on SWT-SVD in LL band. The proposed algorithm is divided into two parts, watermark embedding and watermark extraction.

3.1 WATERMARK EMBEDDING PROCESS

The watermark embedding process is described below as following:

Step 1: Load and convert the cover image and watermark image into YC_bC_r color space from RGB color space and choose Y channel for embedding.

Step 2: Decomposed cover the image into four sub-bands using SWT-SVD.

Step 3: Apply the Arnold transform on the watermark image to obtain scrambled watermark image using n iteration.

Step 4: Decomposed scrambled watermark image into four sub-bands using SWT-SVD.

Step 5: Compute new sigma matrix using fusion of both sigma matrix with scaling factor alpha as key.

$$S_m = S_i + \alpha S_j \quad (4)$$

where S_i, S_j and S_m represents the singular value of cover, watermark and watermarked image respectively

Step 6: Using new computed sigma matrix, obtain the modified channel by combining altered LL sub-band and other three unaltered wavelets sub-band.

Step 7: Finally, watermarked image is obtained by combining the watermarked channel with the other non-modified channels.

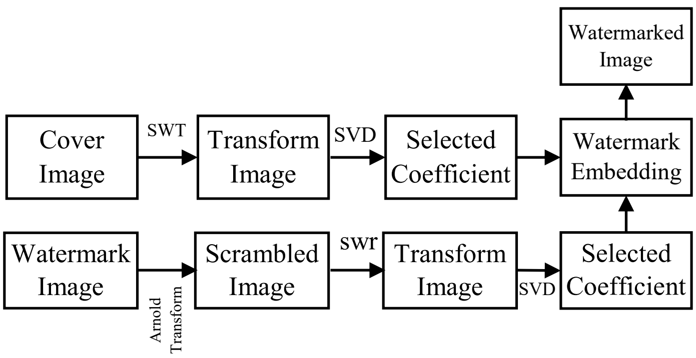


Fig.3. Embedding Process

3.2 WATERMARK EXTRACTION PROCESS

Watermark extraction process is also very important process. It recovers the hidden information from watermarked image which are embedded into cover image. The watermark extraction process is described below as following:

Step 1: Load watermarked image and converted it into YC_bC_r color space from RGB and pick the watermarked channel.

Step 2: Decomposed the images into sub-bands using SWT-SVD respectively.

Step 3: Compute extracted sigma matrix from combination of both sigma matrix using scaling factor which work as key at time of watermark embedding process.

$$S_{j\_n} = \frac{S_m - S_i}{\alpha} \quad (5)$$

where S_{j_n} represents extracted singular values of matrices.

Step 4: Using new computed extracted sigma matrices and orthogonal matrices, we reconstruct the image by using formula:

$$W = U_m * S_{j\_m} * V_m^{'} \quad (6)$$

Step 5: Finally, desired extracted watermark image obtained by applying inverse Arnold and SWT.

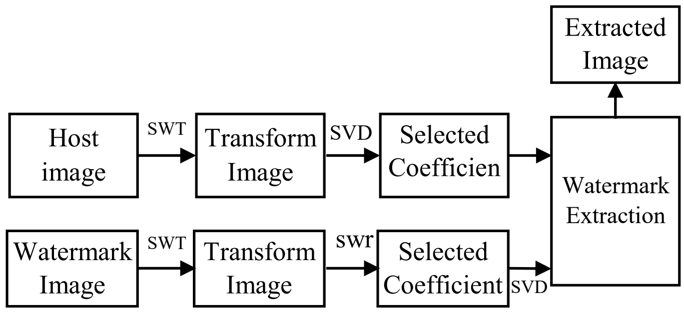


Fig.4. Extraction Process

4. RESULTS AND DISCUSSION

In this section, experimental results are demonstrated to show the effectiveness of the proposed color image watermarking scheme. To compare the performance of proposed method with other considered color image watermarking methods, we use 24-bit RGB color images namely; Lena, Mandrill as host images and for watermark purpose, we use RGB color RTU logo and RGB color image namely Aeroplane which are shown in Fig.3. Size of cover image and watermark image are 512×512 which are obtained from USC-SIPI image database as a standard evaluation database for watermarking algorithms [17].

4.1 EVALUATION FIDELITY PARAMETERS

Numerous experiments have performed to investigate the effects of embedding and extraction of color watermark into the color images. The visual performance of watermarked images is determined by using peak signal-to-noise ratio (PSNR), structural similarity (SSIM) index and Normalized Correlation coefficient (NCC) which are historically adopted in image processing in order to evaluate the performance of the output results.

Perceptual imperceptibility which shows the quality of watermarked image is measured using PSNR [2], [3], [5].

$$MSE = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\left(f\,(i,j) - g(i,j)\right) \quad (7)$$

$$PSNR = 10\log_{10}\frac{L^2}{MSE} \quad (8)$$

where L show the values of pixel range and $f(i,j)$ and $g(i,j)$ represents the host and watermarked image respectively . As MSE is inversely proportional to PSNR, hence the small mean square error tends to high signal to noise ratio. Quality of image depend upon the value of PSNR. Hence for better image quality the PSNR must be high.

To evaluate the imperceptible capability, we use a new parameter known as structural similarity (SSIM) index which measure the similarity between the original image and the watermarked image.

The robustness which show the similarity of original watermark with extracted watermark [3] [5] is measured via NCC.

The quality of the image is measured using normalized co-relation coefficient (NCC) and is obtained given below equation by,

$$NCC = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M} g(i,j) * g'(i,j)}{\sqrt{\sum_{i=1}^{N}\sum_{j=1}^{M} g^2(i,j)}\sqrt{\sum_{i=1}^{N}\sum_{j=1}^{M} g^2(i,j)}} \quad (9)$$

where $g(i,j)$ and $g'(i,j)$ are the original watermark and extracted watermark respectively. If extracted watermark similar to original watermark then the value of NCC equal to one otherwise for no similarities the value of NCC is zero.

4.2 SIMULATED EXPERIMENTAL RESULTS

Lena Mandrill

Fig.5(a). Lena and Mandrill used as a cover image

RTU Logo Aeroplane

Fig.5(b). RTU logo and Airplane used as a watermark image

The Fig.5(a) and Fig.5(b) shows the cover image and watermark image used in proposed work.

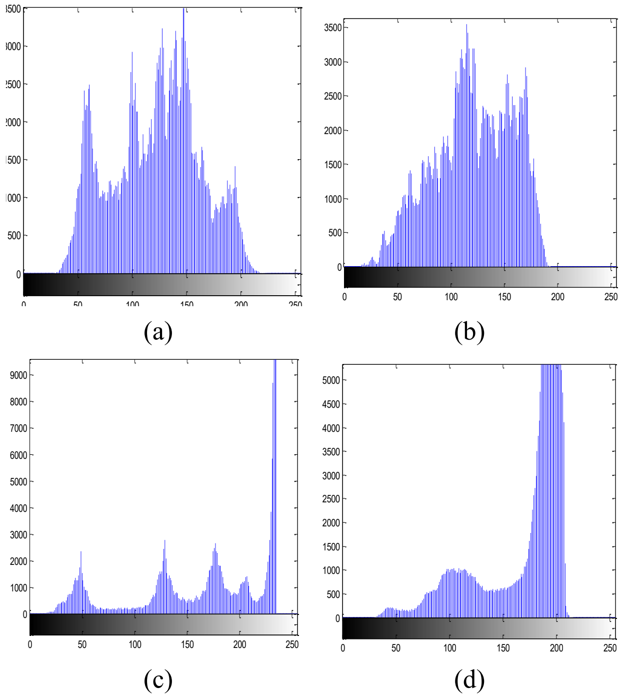
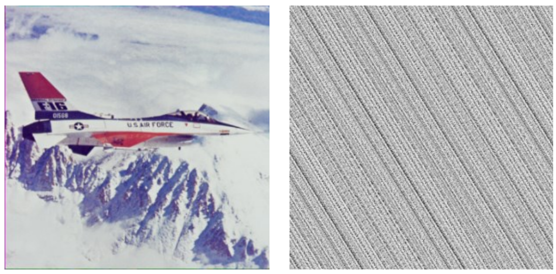


Fig.6. Histogram of original images: (a) Lena (b) Mandrill (c) RTU Logo (d) Aeroplane

(a) RTU Logo (b) Scrambled image using Arnold Transform at n=5



(c) Aeroplane (d) Scrambled image using Arnold Transform at n=5

Fig.7. Scrambled image of RTU Symbol and Aero plane using Arnold Transform at n=5 iteration

The Table.1 shows the PSNR Value and SSIM value for proposed image watermarking techniques at n = 5 iteration of Arnold transform (Lena (as cover) and RTU logo (as watermark).

Table.1. PSNR Value and SSIM value for proposed image watermarking techniques

Scaling factor	Proposed method	
α	**PSNR**	**SSIM**
0.01	41.26	0.9998
0.015	37.87	0.9995
0.02	35.47	0.9991
0.025	33.63	0.9986
0.03	32.10	0.9980
0.05	27.74	0.9945
1	6.60	0.4298

Table.2. NCC value for proposed image watermarking techniques at *n*=5 iteration of Arnold transform (Lena (as cover) and RTU logo (as watermark)

Scaling factor *α*	NCC
0.01	0.9811
0.015	0.9978
0.02	0.9948
0.025	0.9956
0.03	0.9937
0.05	0.9898
1	0.5415

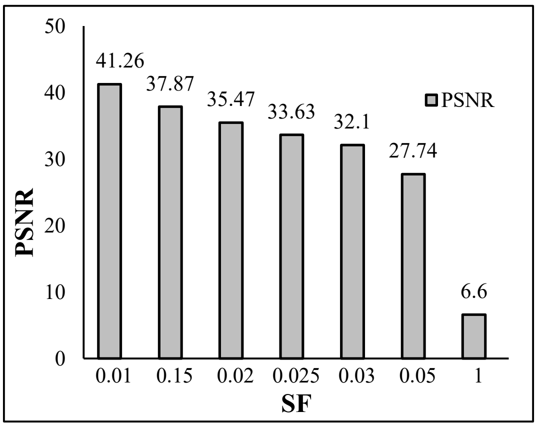


Fig.8. Barchart for PSNR at different value of Scaling factor (S.F)

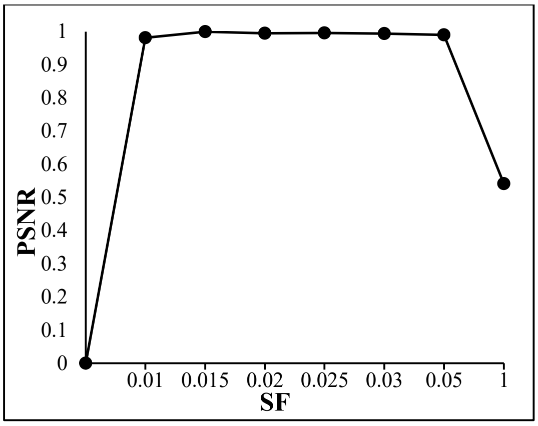


Fig.9. PSNR at different value of scaling factor for proposed method

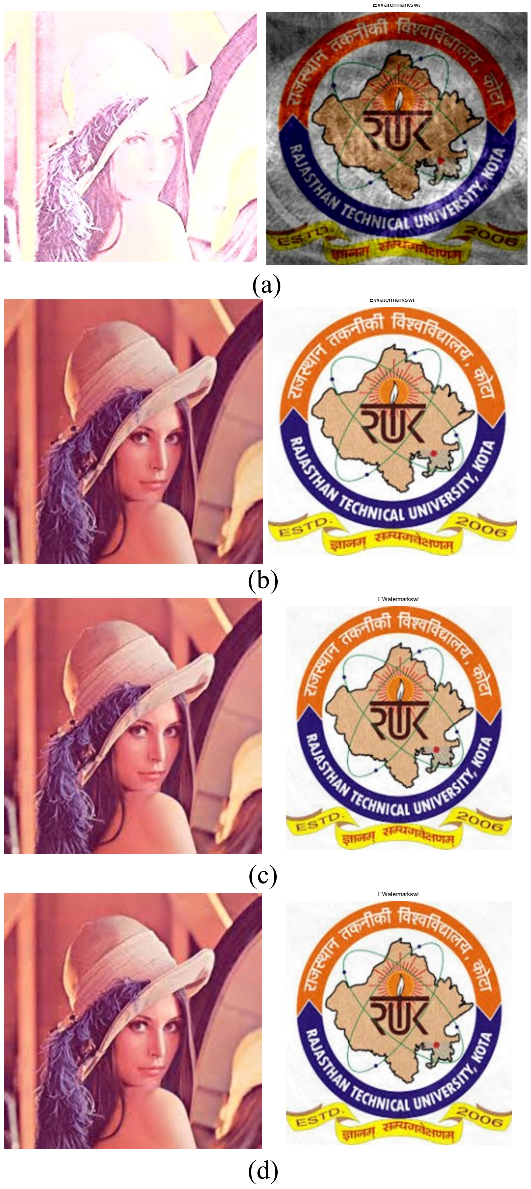
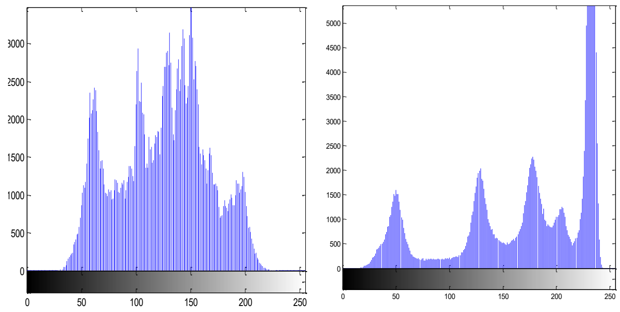


Fig.10. Visual representation of watermarked and recovered watermark image at different value of (a) *SF* = 1 (b) *SF* = 0.015 (c) *SF* = 0.03 (d) *SF* = 0.05 using proposed method



Lena Mandrill

Fig.11. Histogram of watermarked image and recover RTU logo respectively at α=0.15

From the simulated results as shown in Table.1, it is observed that proposed method has good value of PSNR and SSIM between watermarked and cover image. For different value of scaling factor, proposed method shows the better results in term of imperceptibility. Quality of watermarked image in term of imperceptibility depend upon the value of scaling factor if scaling factor increases/decrease quality of watermarked image decreases/increase respectively. From the Table.2, it is also observed that the calculated NCC value between recovered watermark image and watermark image is above 0.98 which indicate the good robustness of the proposed method. Hence it is concluded that that the proposed technique is able to hide and protect the data and able to extract the embedded information back from watermarked image.

5. COMPARISON OF IMPERCEPTIBILITY OF PROPOSED METHOD AND OTHER EXISTING METHODS

Here in this section, we want to validate our results. For this purpose, we compare the results of proposed methods with some other existing techniques. For relatively fair comparison, same images adopted for the experimental purpose which was used in existing methods of watermarking.

Table.3. Comparison of imperceptibility of proposed method and other existing methods

Watermarked image	**Watermark**	**Proposed Method**	**Manish et al. [11]**	**Vahedi et al. [8]**
Lena	RTU logo	37.87	35.92	36.74
Mandrill	RTU logo	37.96	35.67	35.85
Lena	Aero plane	38.36	35.61	36.32
Mandrill	Aero plane	38.40	35.59	35.42

The Table.4 indicate the results of average subjective quality test applied on different people to check the quality of proposed work. Hence the results obtained from various simulated experiments are verified qualitatively by visual representation of watermarked and extracted watermark image. From results, it is clearly seen that the proposed method has the robust efficiency of watermarking with data hiding ability. Hence it is concluded that the proposed algorithm is robust and efficient with data hiding properties as per HVS requirements.

Table.4. Average subjective quality comparison of original and watermarked images by 10 human beings in the scale of 0 to 5

Watermarked image	**Watermark**	**Proposed Method**	**Manish et al. [11]**	**Vahedi et al. [8]**
Lena	RTU logo	5	5	5
Mandrill	RTU logo	5	5	5
Lena	Aeroplane	5	5	5
Mandrill	Aeroplane	5	5	5

6. CONCLUSIONS

In this paper, a robust non-blind hybrid color image watermarking technique is presented. Here, the performance of proposed work is evaluated using color watermark at different scaling factor to fulfill the requirement of high robustness and simultaneously increase the value of transparency. The simulated results validate that proposed watermarking technique show the better results in comparison to other existing techniques for all the considered fidelity parameters. Besides this it is also observed that proposed scheme is not fast enough as per need of some real-time applications for online security of data in real time application. Hence it needs to be improved in the future works by upgrading the watermark embedding strategy and multimedia contents. Hence finally considering the all merits and demerits, it is concluded that the proposed method is efficient with adaptive in nature and produces high quality images with robustness and can further be used for protection of the copyrighted images. The proposed work can be further extended for other multimedia contents such as audio signal, video signals and 3D images.

REFERENCES

[1] W. Bender, D. Gruhl, N. Morimoto and A. Lu, "Techniques for Data Hiding", *IBM System Journal*, Vol. 35, No. 3, pp. 313-336, 1996.

[2] E.T. Lin and E.J. Delp, "A Review of Data Hiding in Digital Images", *Proceedings of International Conference on Image Processing, Image Quality, Image Capture Systems*, pp. 274-278, 1999.

[3] P.H.W. Wong, O.C. Au and G.Y.M. Yeung, "A Novel Blind Multiple Watermarking Technique for Images", *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 13, No. 8, pp. 813-830, 2003.

[4] A.P. Singh and A. Mishra, "Wavelet Based Watermarking on Digital Image", *Indian Journal of computer Science and Engineering*, Vol. 1, No. 2, pp. 86-91, 2011.

[5] G. Dayalin Leena and S. Selva Dhayanithy, "Robust Image Watermarking in Frequency Domain", *International Journal of Innovation and Applied Studies*, Vol. 2, No. 4, pp. 582-587, 2013.

[6] S. Agreste, G. Andaloro, D. Prestipino and L. Puccio, "An Image Adaptive, Wavelet-Based Watermarking of Digital Images", *Journal of Computational and Applied Mathematics*, Vol. 210, pp. 13-21, 2007.

[7] S. Agreste and G. Andaloro, "A New Approach to Preprocessing Digital Image for Wavelet-based Watermark", *Journal of Computational and Applied Mathematics*, Vol. 221, pp. 274-283, 2008.

[8] E. Vahedi, R.A. Zoroofi and M. Shiva, "Toward A New Wavelet- based Watermarking Approach for Color Images using Bio-Inspired Optimization Principles", *Digital Signal Processing*, Vol. 22, pp. 153-162, 2012.

[9] N.H. Golea, R. Seghir and R. Benzid, "A Blind RGB Color Image watermarking based on Singular Value Decomposition", *Proceedings of IEEE International Conference on Computer Systems and Applications*, pp. 771-776, 2010.

[10] L. Wu, J. Zhang, W. Deng and D. He, "Arnold Transformation Algorithm and Anti-Arnold Transformation Algorithm", *Proceedings of IEEE International Conference on Information Science and Engineering*, pp. 12-23, 2009.

[11] M. Gupta, G. Parmar, R. Gupta and M. Saraswat, "Digital Image Watermarking using Uncorrelated Color Space", *Proceedings of IEEE Symposium on Computer Applications and Industrial Electronics*, pp. 1-7, 2014.

[12] Samira Lagzian, Mohsen Soryani and Mahmood Fathy, "A New Robust Watermarking Scheme Based on RDWT-SVD", *International Journal of Intelligent Information Processing*, Vol. 2, No. 1, pp. 1-8, 2011.

[13] G. Tripathi, M. K. Pandey and S. Agrawal "Performance Analysis of Non-Blind Arnold Integrated Hybrid Image Watermarking Technique with DWT-SVD", *Journal of Emerging Technologies and Innovative Research*, Vol. 4, No. 3, pp. 207-211, 2017.

[14] Nilanjan Dey, Anamitra Bardhan Roy and Sayantan Dey, "A Novel Approach of Color Image Hiding using RGB Color Planes and DWT", *International Journal of Computer Applications*, Vol. 36, No. 5, pp. 16-24, 2011.

[15] P.V. Nagarjuna and K. Ranjeet, "Robust Blind Digital Image Watermarking Scheme Based on Stationary Wavelet Transform", *Proceedings of 6th International Conference on Contemporary Computing*, pp. 8-10, 2013.

[16] Fangjun Huang and Z.H. Guan, "A Hybrid SVD-DCT Watermarking Method based on LPSNR", *Pattern Recognition Letters*, Vol. 25, No. 15, pp. 1769-1775, 2014.

[17] USC-SIPI Image Database, Available at: http://sipi.usc.edu /database/ database. php.