ISSN No:-2456-2165

Robust Non-Blind Colour Image Watermarking Using Non-Negative Matrix Factorization Technique in DWT Domain

Muhirwa Gratien[1],
[1]Department of Electrical Engineering,
Pan African University. Nairobi, Kenya.

Elijah Mwangi[2],
[2]School of Engineering,
University of Nairobi. Kenya.

Edward Ndungu[3]
[3]Department of Telecommunication and Information Engineering,
Jomo Kenyatta University of Agriculture and Technology.
Nairobi, Kenya.

Abstract:- A robust colour image watermarking scheme for copyright protection using a Non-negative Matrix Factorization (NMF) in Discrete Wavelet Transform (DWT) domain is suggested. The main goal of the proposed scheme is to decompose the RGB host image into four sub-bands using DWT and then apply the NMF to the vertical detail of the host image. This is followed by scrambling and decomposition of the watermark image using Arnold transform and DWT respectively before embedding it in the host image. To test the robustness of the proposed scheme, the watermarked image is subjected to various signal processing attacks and geometrical rotation attack. The results are assessed in terms of Normalized Correlation (NC), Peak Signal to Noise Ratio (PSNR), Structural Similarity Index Measurement (SSIM). Their average numerical values without attacks for the proposed scheme are 0.8411 for NC, 0.98 for SSIM and 35.5dB for PSNR. The proposed scheme is compared to other existing schemes and the results confirm the superior robustness of the proposed scheme to the existing scheme with the same capacity.

Keywords:- *Arnold Transform, Colour Image Watermarking, Discrete Wavelet Transform, Non-negative Matrix Factorization.*

I. INTRODUCTION

Due to the speedy development and growth of information technology on the internet, digital products can be produced, copied, accessed and disseminated more easily, which causes many problems such as piracy and unauthorized tempering and infringement.

For this reason, digital information can be manipulated and duplicated illegally. One possible solution for enforcing the digital products' rights is through watermarking [1]. Digital watermarking is an important approach and essential copyright protection scheme in multimedia industry. Different watermarking techniques have been utilized for copyright protection of digital images. Watermarking can be classified based on domain type: in spatial domain or in frequency domain [2].

In spatial domain, watermarks are embedded directly in the image pixels. This has the advantages of easy implementation and low complexity when compare to frequency domain. However, the major issue in the spatial domain is robustness of the watermark. It is easy to recognize the watermark embedded in the spatial domain, hence spatial domain watermarking algorithms are fragile to various attacks [3]. In frequency domain techniques, the watermark is embedded in the frequency coefficients acquired by frequency transformation of the image. There are many different techniques in frequency domain [3] used to transform image for example DWT, Discrete Cosine Transform (DCT), Singular Value Decomposition (SVD). Generally, frequency transform watermarking algorithms are more robust and more widely practical than spatial transform based algorithms [2].

Recently, a novel signal decomposition technique has been suggested in which a non-negative matrix can be decomposed into two non-negative matrices. This non-negative matrix factorization technique has been applied in many signal analysis areas, such as blind signal source separation as reported in literature [4],[5], frontal face verification [6], image classification [7]. In recent years, NMF has been applied to digital watermarking.

Various authors have proposed watermarking techniques based on NMF. The work of Silja and Soman as reported in [8] proposed a watermarking scheme based on NMF and SVD in contourlet transform. In [9] Yunfeng et *al*. proposed an improved image watermarking scheme based on NMF and DWT. Dhar and Shimamura in [10] introduced an image watermarking in lifting wavelet transform (LWT) domain based on NMF and SVD. Recently, in 2018 Chen et *al*. as reported in [11] proposed a digital watermarking based on general NMF scheme. All the watermarking based on NMF schemes in existence have been applied on grayscale images only.

A novel robust colour image watermarking scheme is proposed. It is based on frequency domain and it is resilient to various attacks. The proposed scheme is based on RGB colour image watermarking using the NMF in DWT domain. To provide the additional security, the watermark

is scrambled using the Arnold transform where the watermark is available only to a legitimate user. The watermarking algorithm involves two stages; these are embedding and recovery of watermark.

The rest of this paper is arranged as follows: The brief introduction on NMF, DWT and Arnold transform are introduced in section II. A discussion of the PSNR, SSIM and NC is given in section III. The proposed watermarking scheme is described in section IV. Then, the experimental results and analysis are given in section V. Lastly, the conclusion is drawn in section VI.

II. DESCRIPTION OF THE PROPOSED SCHEME

A. Non-negative Matrix Factorization

The Non-negative matrix factorization technique breaks down a non-negative matrix into two matrices containing non-negative components [21]. Given a non-negative matrix $A \in \mathbb{R}_{+}^{S\times Z}$ with a positive integer $K < min\ (S,Z)$, the NMF breaks down into a product of two matrices $B \in \mathbb{R}_{+}^{S\times K}$ and $C \in \mathbb{R}_{+}^{K\times Z}$ such that A ≈ BC.

It is necessary first to describe a cost function that quantifies the quality of the approximation in order to obtain an approximate factorization of (A ≈ BC). An iterative NMF algorithm that minimizes the objective function as given in equation (1) has been suggested in [12].

$$\|\mathrm{A}-\mathrm{BC}\|_{\mathrm{F}}^{2}=\sum_{ij}(A_{ij}-BC_{ij})^{2} \quad (1)$$

Where $\|.\|_{\mathrm{F}}^{2}$ denotes the Frobenius norm, also known as the squared Euclidean distance between *A* and *BC* as shown in equation (2). It has been demonstrated in [12], that at each iteration decreases the objective function. In addition to the Frobenius norm, other NMF cost functions have been suggested and a number of distinct algorithms were proposed [13]. In this paper, the Projected Gradient Descent (PGD) method [14] based on NMF has been used to minimize the cost function in equation (2).

$$f(B,C)=\|\mathrm{A}-\mathrm{BC}\|_{F}^{2} \quad (2)$$

It has two components *B* and *C*, hence it is not convex and it is a constrained optimization problem i.e.: *(B, C)* are non-negative matrices. The projected gradient descent algorithms has update rules of the form specified in the following pseudocodes:

Initialize B≥0, as *S*x*K* random matrix
Initialize C≥0, as *K*x*Z* random matrix
Choose step size parameters ϵ_B and ϵ_C

While stopping condition is not met
Update
On variable B:
Step size: $t_B^k = \frac{1}{\|C^k(C^k)^T\|_{\mathrm{F}}}$;
Update: $B^{k+1} = max[B^k - t_B^k \nabla_B f(B^k; C^k)\epsilon_B]$;
On variable C:
Step size: $t_C^k = \frac{1}{\|(B^{k+1})^T B^{k+1}\|_{\mathrm{F}}}$;
Update: $C^{k+1} = max\ [C^k - t_C^k \nabla_C f(C^k; B^k)\epsilon_C]$;
Until converged or the maximum number of iterations is reached
end

B. Discrete Wavelet transform

The DWT offers a number of powerful decomposition in image processing algorithms such as edge detection, noise reduction and compression. The DWT is computed by consecutive of low-pass and high-pass filtering of the discrete time-domain signal. Detailed information is provided at each stage by the high pass filter, whereas the low pass filter linked to the scaling function generates coarse approximations. The two-dimensional DWT is used in the image processing. If an image has *n* rows and *n* columns, then the first level of decomposition will achieve four sub-band images. The band are: *HH*, *HL*, *LH* and *LL* [25], each with columns of *n/2* rows and *n/2* as shown in Figure 1.

The notation for the image components corresponds to the filter operation and direction. The first letter *L* or *H* relates to the rows for low pass frequency operation or high frequency operation, and the second letter relates to the filter applied to the column. The DWT can be used to decompose the input image using orthonormal filters like Haar filters, so that the image is split into four non-overlapping multiresolution sub-bands. The lowest resolution level (*LL*) contains the approximation part of the host image. The rest consists of the detail part and provide horizontal details (*LH*), vertical details (*HL*) and diagonal details (*HH*) [25]. The second level of DWT decomposition is executed on the first level *LL* sub-bands of the image and ends into another level of decomposition.

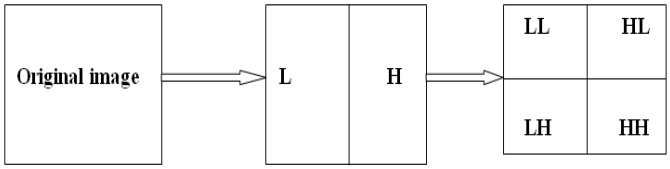

Fig 1:- Image Decomposition using DWT

C. The Arnold Transform

The Arnold Transform is chaotic method which randomizes the pixels of an original image and makes the image indistinguishable or chaotic. The Arnold Transform changes the position of the pixels in image, thus obtaining a scrambled image. However, it is only suitable for square images. The Arnold transform [29] is defined as given in equation (3).

ISSN No:-2456-2165

$$\begin{pmatrix} X_1 \\ Y_1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} X_0 \\ Y_0 \end{pmatrix} mod\ N \quad (3)$$

Where (X_0, Y_0) is the location of the pixels in the host image, (X_1, Y_1) is the location of the pixels after the Arnold transformation and *NxN* is the size of an image. It is a periodical mapping with a period *T*. If the transformation is repeated several times in Arnold transform, it returns to its initial states. The period varies in accordance with the dimension of image i.e.: a colour image of 64x64 size has a period of 192, i.e. after 192 times the scrambled image is reduced back to its original image [30].In addition, an iteration number is utilized as the encryption key. In other words, the iteration number is used as a secret key to extract the secret image when the Arnold transform is applied to an image [31]. After the scrambling, the watermark image becomes chaotic. If the scrambling algorithm and the security key are unknown, the attacker cannot extract the watermark. Therefore, the Arnold transform provides security for digital multimedia content and robustness of the algorithm because the spatial relationships of an image's pixels have become totally disordered [29].

III. PERFORMANCE MEASUREMENT OF A WATERMARKING ALGORITHM

Three objective measures used to test the performance of the developed algorithm are: Normalized Correlation (*NC*), Peak Signal-to Noise Ratio (*PSNR*) and Structural Similarity Index Measurement (*SSIM*). The *PSNR, NC* and *SSIM* are defined in equation (4), (5) and (6) respectively.

The PSNR is a mathematical tool used for evaluation of the image quality after the watermarking process. This means that the invisibility of a watermarking scheme can be described by the *PSNR* [19]. It is expressed in dB. The *PSNR* is given [20] in equation (4).

$$PSNR\ (dB) = 10log_{10} \frac{3MN[Max\ I_{1(x,y,k)}]^2}{\sum_{x=1}^{N}\sum_{Y=1}^{M}\sum_{K=1}^{3}[I_{1(x,y,k)} - I_{2(x,y,k)}]^2} \quad (4)$$

Where $Max\ I_{1(x,y,k)}$ is the maximum possible pixel value of the image and is 255 for an 8-bits. $I_{1(x,y,k)}$ and $I_{2(x,y,k)}$ are the pixel value at position (*x*,*y*) in three colour channel (*k*) of the original host image and the watermarked image respectively. *M* and *N* represent size of original host image.

The NC is a technique used for comparison between the original watermark and the recovered watermark. The NC [19] is given as shown in equation (5).

$$NC = \frac{\sum_{i=1}^{m} W_i \times W_i'}{\sqrt{\sum_{i=1}^{m} W_i^2} \times \sqrt{\sum_{i=1}^{m} W_i'^2}} \quad (5)$$

Where W_i is Original watermark; and W_i' is extracted watermark.

Structural similarity index measurement (*SSIM*) is a technique used to assess the quality and the similarity between two images. The *SSIM* has between 0 and 1.

For the value of *SSIM* closer to unity, the watermarked image is similar to the host image [21].The *SSIM* is defined in [21] as given in equation (6).

$$SSIM(H_0, H_1) = l(H_0, H_1) \times c(H_0, H_1) \times s(H_0, H_1) \quad (6)$$

Where H_0 is the original host image and H_1 refers to the watermarked image.

$$\begin{cases} l(H_0, H_1) = \frac{2(\mu_{H_0} \times \mu_{H_1}) + C_1}{\mu_{H_0}^2 + \mu_{H_1}^2 + C_1} \\ c(H_0, H_1) = \frac{2(\sigma_{H_0} \times \sigma_{H_1}) + C_2}{\sigma_{H_0}^2 + \sigma_{H_1}^2 + C_2} \\ s(H_0, H_1) = \frac{\sigma_{H_0 H_1} + C_3}{\sigma_{H_0} \times \sigma_{H_1} + C_3} \end{cases} \quad \mathbf{(7)}$$

The figure 2 shows differents standard test images used in the experiment for the proposed scheme.

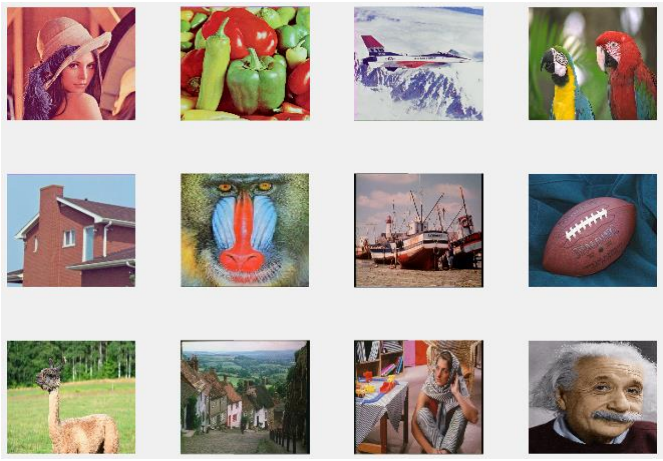

Fig 2:- Different Test Images Set: Lena, Peppers, F16, Parrot, House, Baboon, Boats, Football, Llama, Goldhill, Barbara, Einstein

IV. PROPOSED WATERMARKING SCHEME

The proposed scheme has two stages: The watermark embedding process as the first stage and watermark recovery process as the second stage.

A. The Watermark Embedding Process

The steps of embedding a watermark image in colour images are performed as summarized from step (i) to step (viii).

Step (i): The host colour image is first divided into red (*R*), green (*G*) and blue (*B*) channels.

Step (ii): Then, the first level Discrete Haar wavelet transform is applied on each of the three colour components of host image to get four sub-bands frequency of the respective components namely approximation part (*LL*),

ISSN No:-2456-2165

Horizontal details (*LH*), Vertical details (*HL*), and diagonal details (*HH*). This is followed by the decomposition of those sub-bands into sub-channels. Each sub-band contains red, green, blue channels information i.e: vertical detail for red component (*HLr*), vertical detail for green component *(HLg*) and vertical detail for blue component (*HLb*).

Step (iii): The sub-band *HL* is selected such that *HLr=Vr*, *HLg=Vg* and *HLb=Vb*, an approach coefficient matrices *Vr*, *Vg* and *Vb* are obtained.

It is known that *LL* comprises the approximation part of the host image, hence embed a watermark in *LL* degrade the quality of image. The *LH*, *HL* and *HH* are relatively high frequency sub-bands, if watermark message is embedded in the high sub-band frequency area, the robustness of the watermark will be strengthened and the watermark embedded in that sub-band does not affect the quality of host image. In *HH* sub-band most of the pixels in that area are zeros and embedding factor will not have much effect on embedding process. Hence, the *HL* sub-band of host image is selected to embed the watermark elements among the highest sub-band frequency.

Step (iv): Apply the NMF on the selected sub-band *HL*. The NMF is used to decompose *HL* into the matrices, $HL_x = WxHx$ subject to the constraints $W_x, H_x \geq 0$, where *x* is Red or Green or Blue. The three matrices (HL_r, HL_g and HL_b have the same size, i.e.: W_x and H_x have dimensions (*M*x*K*) and (*K*x*N*) respectively.

The projected gradient descent technique was used among the existing bound-constrained optimization techniques, because it is simple to implement, it exhibits strong optimization properties and it has convergence property [14],[22]. As the number of iterations increase the relative error reduces until the convergence is obtained.

Step (v): The watermark image is first decomposed into red, green and blue components, thereafter scrambled by the Arnold transformation with a security key to enhance the watermark security before embedded it in the host image.

Step (vi): The scrambled watermark is decomposed into four sub-bands namely approximation part of watermark (*LLw*), Horizontal details of watermark (*LHw*), Vertical details of watermark *(HLw*), and diagonal details of watermark (*HHw*) using the Discrete Haar wavelet transform. This is followed by the decomposition of those sub-bands into sub-channels. Then, each sub-band contains red, green, blue channels information i.e: vertical detail for red component of watermark (*HLwr*), vertical detail for green component of watermark (*HLwg*), vertical detail for blue component of watermark (*HLwb*).

Step vii: Thereafter, embed the watermark element into the selected vertical detail (*HL*) of host image. The watermark element is embedded into the matrix *H* randomly using embedding factor ($\alpha = 5$). Suppose the elements of vertical detail of watermark (*HLw*) is embedded in the coefficients of matrix *H* as shown in equation (8). As soon as all the elements of watermark embedded, the new update value of *HL* is obtained as shown in equation (9).

$$H'_{\mathcal{X}} \leftarrow H_{\mathcal{X}} + \alpha(\mathrm{HLw}x) \quad (8)$$

$$HL'_{\mathcal{X}} = W_{\mathcal{X}} H'_{\mathcal{X}} \quad (9)$$

Where α denotes the watermark embedding factor and $\mathcal{X}$ represents Red or Green or Blue .

Step (viii): The watermarked image is obtained by the inverse of discrete wavelet transform (IDWT).

The Figure 3 shows *Lena* as host image, first level decomposition of host image using DWT, the watermark, the scrambled watermark and the watermarked image.

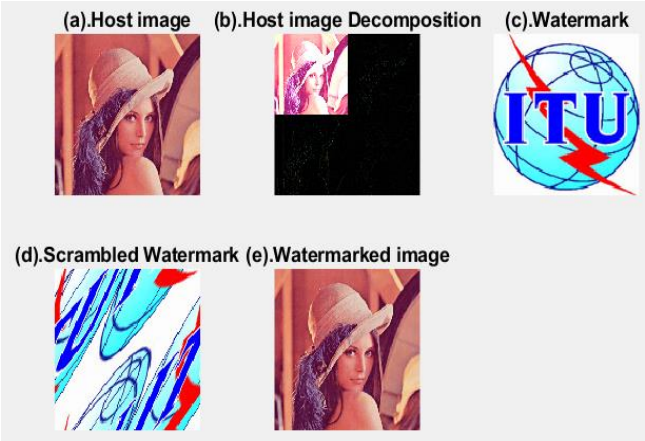

Fig 3:- The Embedding Process of Watermark

B. The Watermark Recovery Process

The watermark recovery is the reverse process of embedding process. It requires the host image, the embedded location and secret key to recover the watermark. The steps of the watermark recovery are performed as summarized from step (i) to step (xiii).

Step (i): The watermarked image is first decomposed into red (R), green (G) and blue (B) colour components.

Step (ii): The watermarked image is decomposed into four sub-bands namely approximation part of watermarked image (*LLwa*), Horizontal details (*LHwa*), Vertical details of (*HLwa*), and diagonal details (*HHwa*) using the first level Discrete Haar wavelet transform. This is followed by the decomposition of those sub-bands into sub-channels. Then, each sub-band contains red, green, blue channels information, i.e: vertical detail for red component of watermarked image (*HLwar*), vertical detail for green component of watermarked image (*HLwag*), vertical detail for blue component of watermarked image (*HLwab*).

Step (iii): Set all the coefficients of *LLwa*, *LHwa*, *HHwa* to zero. Extract the watermark according to the embedded location.

ISSN No:-2456-2165

Step (iv): The sub-channel *HLwa* contains the watermark information is selected such that $HLwar=V_3$, $HLwag=V_4$ and $HLwab=V_5$ the coefficient matrices V_3, V_4, V_5 are obtained.

Step (v): The NMF is used to decompose the matrix V_3, V_4, V_5 such that $V_3=W_3H_3$, $V_4=W_4H_4$, $V_5=W_5H_5$ subject to the constraints $W_3,H_3 \geq 0$, $W_4,H_4 \geq 0$, $W_5,H_5 \geq 0$. Then, the coefficient matrices H_3, H_4 and H_5 contain the watermark information are obtained.

Step (vi): Then, on other hand, the host image is first divided into red, green and blue channels.

Step (vii): The Discrete Haar wavelet transform is applied on each of the three colour components of host image to obtain four sub-bands frequency of the respective components namely approximation part (*LL*), Horizontal details (*LH*), Vertical details (*HL*), and diagonal details (*HH*). This is followed by the decomposition of those sub-bands into sub-channels. Then, each sub-band contains red, green, blue channels information as *LL=[LLr, LLg, LLb]*, *LH=[LHr, LHg, LHb]*, *HL =[HLr, HLg, HLb] and HH=[HHr, HHg, HHb]* channels respectively.

Step (viii): The sub-band HL is selected such that $HLr=V$, $HLg=V_1$ and $HLb=V_2$, an approach coefficient matrices V, V_1 and V_2 are obtained.

Step (ix): Apply the NMF on the selected sub-band HL. The NMF is employed to decompose HL into the matrices i.e. $V=W_rH_r$, $V_1=W_gH_g$ and $V_2=W_bH_b$ subject to the constraints $W_r,H_r \geq 0$, $W_g,H_g \geq 0$ and $W_b,H_b \geq 0$. The coefficient matrices H_r, H_g and H_b are obtained.

Step (x): Then, scrambled coefficients of vertical detail of watermark are gathered together using embedding coefficient ($\alpha = 5$). So that the extracted vertical detail component is obtained as shown from equation (10) to equation (12).

$$HLwr = \frac{H_3 - H_r}{\alpha} \quad (10)$$

$$HLwg = \frac{H_4 - H_g}{\alpha} \quad (11)$$

$$HLwb = \frac{H_5 - H_b}{\alpha} \quad (12)$$

Step (xi): Hence, the new extracted vertical detail of watermark is obtained.

Step (xii): Then, through the inverse of DWT, the extracted watermark is constructed by combining the new extracted vertical detail with approximation part, horizontal and diagonal components of original watermark.

Step (xiii): Finally, the inverse of Arnold Transform with the same number of iterations and the security key as used in embedding process is applied to re-order the pixels into its original position, hence the recovered watermark is obtained.

The Figure 4 shows *Lena* as host image, the watermark, watermarked image, the extracted watermark image and the recovered watermark image.

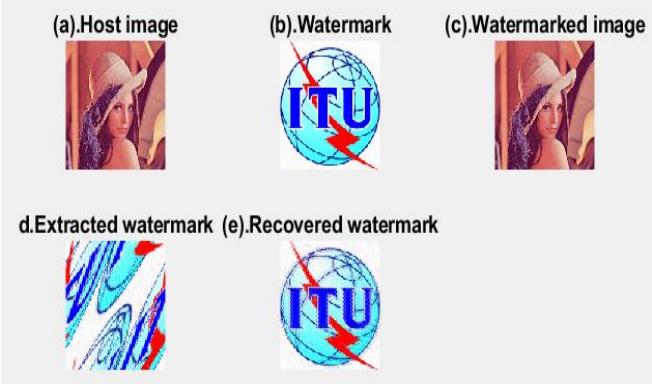

Fig 4:- The Watermarking Process

V. EXPERIMENTAL RESULTS AND ANALYSIS

A. The Quality Evaluation between Watermarked and Host Images

The quality assessment of watermarked image is computed by the *PSNR* and the *SSIM*. The variation of *PSNR* and *SSIM* values for each category of 12 sample images are shown in Figures 5 and 6 respectively.

In the watermarking technique, the high *PSNR* value denotes high imperceptibility of the watermarked image and its high similarity to the host image. The value of watermarking embedding factor (α) is selected based on compromise between *NC* and *PSNR* values [19]. For choosing the value of α, different samples images for different α values are examined. The Table 1 shows the proposed scheme's *PSNR* and *NC* values without attacks for the sample of three colour images of size 512x512 taken as host image.

ISSN No:-2456-2165

Embedding Factor (α)	Peppers		Lena		Barbara	
	PSNR (dB)	NC	PSNR (dB)	NC	PSNR (dB)	NC
$\alpha = 1/2$	34.37	0.8194	35.62	0.8201	29.22	0.8068
$\alpha = 1$	34.35	0.8353	35.60	0.8351	29.20	0.8292
$\alpha = 3/2$	34.33	0.8397	35.56	0.8395	29.18	0.8357
$\alpha = 2$	34.30	0.8406	35.55	0.8400	29.17	0.8389
$\alpha = 2.5$	34.28	0.8407	35.51	0.8402	29.16	0.8399
$\alpha = 3$	34.25	0.8409	35.49	0.8403	29.14	0.8401
$\alpha = 3.5$	34.23	0.8410	35.44	0.8405	29.12	0.8404
$\alpha = 4$	34.20	0.8411	35.40	0.8407	29.11	0.8405
$\alpha = 4.5$	34.17	0.8411	35.37	0.8408	29.10	0.8407
$\alpha = 5$	34.10	0.8412	35.20	0.8409	29.02	0.8410
$\alpha = 5.5$	34.07	0.8413	35.16	0.8410	29.00	0.8411
$\alpha = 6$	34.00	0.8413	35.10	0.8411	28.60	0.8411

Table 1:- The Sample of the Proposed Scheme's PSNR and NC Values Without Attack

In general, a PSNR between 29dB to 48dB represents acceptable image quality [2],[23]. In watermarking assessment, a value of $NC > 0.75$ is considered as an acceptable value [24]. For selecting the optimum value of embedding factor (α), different sample of images for different value of α values are examined. In the experiment, *Peppers*, *Lena* and *Barbara* for different values of α are employed. By varying value of α from 0.5 to 6 with interval of 0.5. Thereafter, computed the PSNR of the watermarked image and NC of the watermark recovery. The Table 1 denotes the summary of PSNR and NC for different values of α. As it can be remarked in Table 1, for embedding factor of $\alpha > 5.5$, the obtained PSNR value for *Barbara* image become less than acceptable lower limit based on the condition presented in [2],[23]. For $\alpha < 4.5$ it is difficult to recover the watermark, the resulting image is completely blurred. However, for the value of α from 4.5 to 5.5 is good for both PSNR and *NC* values. Therefore, based on these results, the watermarking embedding factor is determined as $\alpha = 5$ for the experiment.

The Figure 5 shows the graph of PSNR values and Figure 6 shows its SSIM values between host and watermarked images for different colour images when $\alpha = 5$.

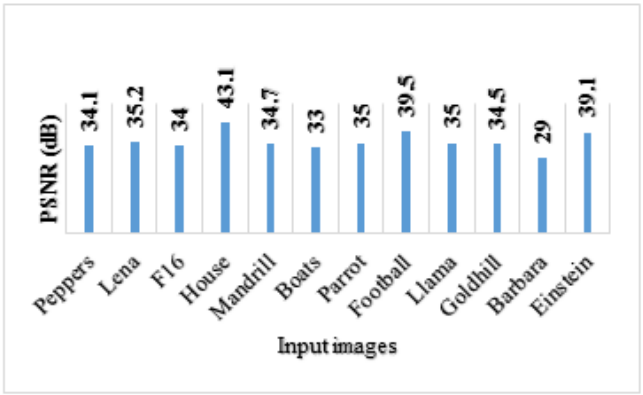

Fig 5:- *PSNR* Values between Host and Watermarked Image for Different Colour Images

Based on the results obtained in Figure 5, the average PSNR value for this proposed scheme is 35.50dB. Therefore, the average *PSNR* value is in the range of 29dB to 48dB represents acceptable watermarked image quality according to condition presented in [2], [23]. Hence the watermarked image is similar to the host image.

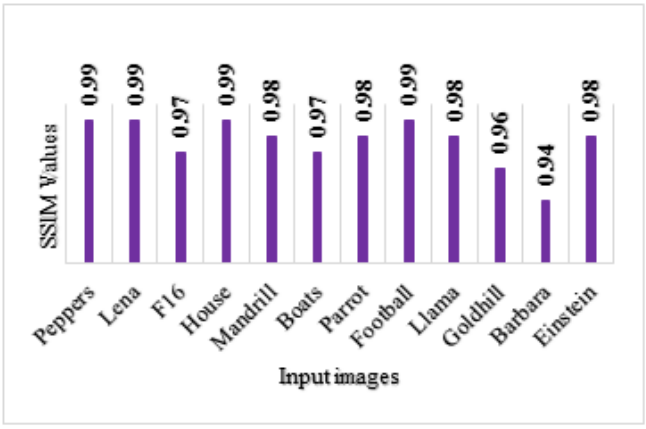

Fig 6:- SSIM Values between Host and Watermarked Image for Different Colour Images

Based on the results of SSIM values obtained in Figure 6, the maximum SSIM value is achieved for *House*, *Peppers*, *Lena and Football* images with a value of 0.99 and minimum value is achieved for *Barbara* image with 0.94; they are closer to one. Hence the watermarked image is similar to the host image.

B. Robustness Evaluation of the Proposed Scheme

To evaluate the robustness, a variety of signal processing and geometric rotation attacks were simulated on the watermarked images. The robustness is measured by the normalized correlation (*NC*) factor between the recovery watermark and original watermark. The high *NC* values indicate that the effect of attack on the watermarked image is less [25]. If the value of *NC* is closer to unity under a special attack, it implies that the scheme has high

ISSN No:-2456-2165

robustness against that attack. Robustness indicates survival or resistance of the embedded watermark in the watermarked image against attacks. The tables 2, 3 and 4 represent the *NC* values of recovered watermark of the proposed scheme when watermarked image is subjected to various attacks types. Signal processing attacks such as sharpening, histogram equalization, contrast adjustment, median filtering, noise addition like salt and pepper and Gaussian noise were applied.

Salt and pepper, and Gaussian noises are considered as noise addition attacks and they are added to the watermarked image. In this investigation, salt and pepper noise with diverse noise densities (0.01, 0.05 and 0.1) are presented on the set of twelve watermarked images as illustrated in Table 2. Noise density indicates the probability of the image area containing noise values. Gaussian noise with different variances (0.01, 0.05 and 0.1) are introduced on the set of twelve watermarked images as illustrated in Table 2.

Attacks / Input images	**Salt and pepper (0.01)**	**Salt and pepper (0.05)**	**Salt and pepper (0.1)**	**Gaussian noise (0.01)**	**Gaussian noise (0.05)**	**Gaussian noise (0.1)**
Peppers	0.8404	0.8403	0.8401	0.8404	0.8403	0.8400
Lena	0.8403	0.8402	0.8400	0.8404	0.8403	0.8400
F16	0.8403	0.8402	0.8400	0.8405	0.8404	0.8402
Parrot	0.8402	0.8401	0.8399	0.8402	0.8401	0.8399
House	0.8402	0.8401	0.8399	0.8405	0.8404	0.8402
Mandrill	0.8400	0.8399	0.8398	0.8403	0.8402	0.8401
Boats	0.8403	0.8402	0.8400	0.8406	0.8405	0.8403
Football	0.8403	0.8402	0.8400	0.8402	0.8401	0.8399
Llama	0.8404	0.8403	0.8401	0.8404	0.8403	0.8400
Goldhill	0.8403	0.8402	0.8400	0.8404	0.8403	0.8400
Barbara	0.8403	0.8402	0.8400	0.8405	0.8404	0.8402
Einstein	0.8402	0.8401	0.8399	0.8404	0.8403	0.8401

Table 2:- The *NC* Values for Noise Addition Attacks for Different Colour Images

The *NC* results in Table 2 are greater than 0.75. Hence, the proposed scheme presents high resistance against Salt and pepper, and Gaussian noises according to the condition presented by Najafi in [24]. It can be noticed that the performance of robustness against these attacks decreases with the increase of the noise density and variance for each image presented.

Histogram equalization adjusts image intensities to enhance contrast. Contrast adjustment remaps image intensity values to the full display range of the data type. The main objective of sharpening is to highlight edges and fine details which may exist in an image. Table 3 illustrates the results of *NC* values of a recovery watermark on the set of twelve different images when median filter, sharpening, contrast adjustment and histogram equalization attacks are applied to watermarked images. Median filtering attack is utilized in this investigation with a block size of 3x3 pixels.

Attacks / Input images	**Sharpening**	**Histogram equalization**	**Median filter(3x3)**	**Contrast adjustments of 50%**
Peppers	0.8403	0.8402	0.8400	0.8401
Lena	0.8401	0.8400	0.8400	0.8401
F16	0.8402	0.8401	0.8401	0.8399
Parrot	0.8398	0.8398	0.8399	0.8398
House	0.8400	0.8400	0.8398	0.8397
Mandrill	0.8401	0.8401	0.8399	0.8398
Boats	0.8403	0.8402	0.8402	0.8402
Football	0.8397	0.8399	0.8396	0.8396
Llama	0.8402	0.8401	0.8400	0.8402
Goldhill	0.8402	0.8400	0.8400	0.8400
Barbara	0.8401	0.8403	0.8402	0.8399
Einstein	0.8402	0.8402	0.8401	0.8400

Table 3:- The *NC* Values for Non-Geometrical Attacks for Different Colour Images

This group of attacks in Table 3 includes sharpening, histogram equalization, median filtering and contrast adjustment attacks. Their *NC* values are greater than 0.75, means that the proposed scheme is robust against these four types of attacks based on the condition presented by Najafi in [24].

The geometrical rotation attack performs geometric transform which maps position (a_1, b_1) of a watermarked image to a new position (a_2, b_2) by rotating it through a certain angle. Rotation does not destroy visual content of the watermarked image but due to rotation, pixels move to new positions and embedded watermark can be altered. The Table 4 illustrates the *NC* results when the watermarked image is subjected to different rotation angles (5^o,10^o ,30^o , 60^o ,90^o ,180^o).

Attacks Input images	**Rotation (5^o)**	**Rotation (10^o)**	**Rotation (30^o)**	**Rotation (60^o)**	**Rotation (90^o)**	**Rotation (180^o)**
Peppers	0.8403	0.8403	0.8401	0.8402	0.8400	0.8401
Lena	0.8401	0.8401	0.8400	0.8401	0.8401	0.8400
F16	0.8400	0.8402	0.8401	0.8401	0.8400	0.8399
Parrot	0.8398	0.8399	0.8397	0.8398	0.8397	0.8396
House	0.8401	0.8401	0.8400	0.8399	0.8400	0.8399
Mandrill	0.8404	0.8403	0.8402	0.8402	0.8400	0.8401
Boats	0.8403	0.8403	0.8401	0.8402	0.8400	0.8401
Football	0.8398	0.8399	0.8398	0.8398	0.8398	0.8397
Llama	0.8401	0.8401	0.8400	0.8398	0.8397	0.8396
Goldhill	0.8401	0.8401	0.8400	0.8401	0.8400	0.8399
Barbara	0.8402	0.8402	0.8400	0.8401	0.8401	0.8400
Einstein	0.8402	0.8402	0.8401	0.8402	0.8401	0.8400

Table 4:- The NC Values of Rotation Attack for Different Colour Images

Based on the simulation results obtained in Table 4, the results show that all *NC* values are greater than 0.75. Therefore, the scheme is robust to rotation attack through the presented angle according to the condition presented by Najafi in [24].

C. *Performance of the Proposed Scheme in Comparison with Other Existing Schemes*

In this section, the proposed scheme based on NMF in DWT domain is compared with other existing scheme in transform domain applied to colour image. The comparison of the proposed scheme with the scheme in [19] and in [26] are considered under approximately the same conditions as shown in Table 5.

Method	Colour model	PSNR (dB)	Host image (size)	Watermark size
Proposed scheme	**RGB colour space**	**35.50**	**512x512**	**64x64**
H. S. Abolfazl and S. Arash [19]	YCbCr colour space	40.48	512x512	64x64
D. O. Muñoz-Ramirez et *al* [26]	YCbCr colour space	42.00	512x512	64x64

Table 5:- Basic Conditions between the Proposed Scheme and its Counterparts

The scheme of *Abolfazl* and *Arash* in [19] represents a digital watermarking algorithm based on combination of the Discrete Cosine Transform (DCT) and Principal Component Analysis (PCA). The watermark is positioned within a range of DCT coefficients of the host image. The watermarking system is accomplished by inserting a watermark of size 64x64 in the first component of the PCA. The robustness evaluation of the scheme in [19] is done under few attacks (only Sharpening, Salt and pepper noise, Gaussian noise, and Median filtering) and other attacks were not considered. In addition, the number of test images employed in [19] were fewer with results only reported for *Lena*, *Peppers* and *Mandrill*. Then, the comparison is limited to the common considered host images and attacks. This comparison is presented in Table 6.

The scheme of *Muñoz-Ramirez* et *al* in [26] represents a digital watermarking scheme based on a Discrete Cosine Transform (DCT) and Quantization Index Modulation (QIM). The watermark is inserted into the mid-frequency of DCT coefficients of the host image. The watermarking process is performed by embedding a watermark of size

64x64. The host image was transformed from *RGB* to *YCbCr* colour space, then only the luminance channel *Y* is selected; meanwhile, the RGB channels of the watermark are divided and encoded to guarantee the robustness and imperceptibility of the watermark. The robustness evaluation of the scheme in [26] is done under few attacks only Salt and pepper noise, Gaussian noise, Contrast adjustment (50%) attacks and other attacks were not considered. In addition, the number of test images employed by *Muñoz-Ramirez* et *al* in [26] were fewer with results only reported for *Lena, Peppers, Mandrill, F16, House and boats* and other host images employed in this research investigation were not considered. Then, the comparison is limited to the common considered host images and attacks. The robustness comparison of the techniques in [19] and in [26] with the proposed scheme is summarized in the Table 6 and the best *NC* value is highlighted in each attack.

Attacks	Proposed scheme	H. S. Abolfazl and S. Arash [19]	D. O. Muñoz-Ramirez et *al* [26]
	NC	NC	NC
Salt and pepper (0.01)	**0.8403**	0.81	Non Applicable
Gaussian noise (0.01)	**0.8404**	0.61	0.83
Sharpening	**0.8401**	0.71	Non Applicable
Median filter (3x3)	0.8400	**0.94**	Non Applicable
Salt and pepper (0.05)	**0.8402**	Non Applicable	0.84
Contrast adjustment (50%)	0.8401	Non Applicable	**0.93**

Table 6:- *NC* Comparison of the Proposed Scheme with the Scheme in [19] and in [26] for *Lena* Image

It is evident from the Table 6 that the proposed scheme performed better than *Abolfazl* and *Arash*'s technique, and *Muñoz-Ramirez*'s technique when various attacks such as Sharpening, Salt and pepper noise, and Gaussian noise were simulated on the *Lena* watermarked image. In addition, the proposed scheme is more secure than the scheme in [19] and in [26] as the watermark is first scrambled by using Arnold transform with a secret key before embedding it in host image. Hence, the attacker cannot extract the watermark unless the secret key and algorithm are known.

VI. CONCLUSION

In this paper, a non-blind colour image watermarking method using NMF and DWT has been presented. This scheme uses DWT to decompose image into sub-bands and NMF to factorize the vertical detail of the *RGB* host colour image in order to achieve the watermarking requirements. The experimental results show that the proposed scheme is effective. The proposed technique has high robustness against various attacks such as sharpening, histogram equalization, contrast adjustment, rotation, salt and pepper noise, and Gaussian noise. The proposed technique is comparable to other existing techniques in terms of NC and PSNR values. The work can be extended to include other colour spaces like *YCbCr, YIQ*.

ACKNOWLEDGEMENT

The authors are grateful to the African Union (AU) for providing financial support of this work.

REFERENCES

[1]. G. Mane and G. Chiddarwar, "An Imperceptible Video Watermarking Algorithm using Fusion of Wavelet Based," in *2013 IEEE International Conference on Computational Intelligence and Computing Research, Enathi, India, December*, 2013, pp. 1–7.

[2]. M. Moosazadeh and G. Ekbatanifard, "An improved robust image watermarking method using DCT and YCoCg-R colour space," *Optik - International Journal for Light and Electron Optics*, vol. 140, pp. 975–988, 2017.

[3]. F. Sarkardeh and M. Khalili, "Effective SVD-YCbCr Colour Image Watermarking," *International Journal of Computer Network and Communication Security*, vol. 3, no. 3, pp. 110–116, 2015.

[4]. A. Cichocki, R. Zdunek and S. I. Amari, "New algorithms for non-negative matrix factorization in applications to blind source separation," in *2006 IEEE International Conference on Acoustics Speech and Signal Processing Proceedings, Toulouse, France, May*, 2006, vol. 5, pp. 1–4.

[5]. A. Rolet, V. Seguy, M. Blondel and H. Sawada, "Blind source separation with optimal transport non-negative matrix factorization," *EURASIP Journal on Advances in Signal Processing*, vol. 53, no. 1, pp. 1–16, 2018.

[6]. S. Zafeiriou, A. Tefas, I. Buciu and I. Pitas, "Exploiting discriminant information in nonnegative matrix factorization with application to frontal face verification," *IEEE Transactions on Neural Networks*, vol. 17, no. 3, pp. 683–695, 2006.

[7]. D. Guillamet, J. Vitrià and B. Schiele, "Introducing a weighted non-negative matrix factorization for image classification," *Pattern Recognition Letters*, vol. 24, no. 14, pp. 2447–2454, 2003.

[8]. M. S. Silja and K. P. Soman, "A watermarking algorithm based on contourlet transform and non-negative matrix factorization," in *2009 International Conference on Advances in Recent Technologies in Communication and Computing, Kottayam, Kerala, India, October*, 2009, pp. 279–281.
[9]. G. Yunfeng, C. Delong, Y. Guilan and X. Jianbin, "An Improved Image Watermarking algorithm based on NMF and DWT," in *ICINS 2014 International Conference on Information and Network*, 2014, pp. 2–7.
[10]. P. K. Dhar and T. Shimamura, "Image watermarking in LWT domain based on nonnegative matrix factorization and singular value decomposition," in *2014 9th International Forum on Strategic Technology (IFOST), Cox's Bazar, Bangladesh, October*, 2014, pp. 144–147.
[11]. Z. Chen, L. Li, H. Peng, Y. Liu and Y. Yang, "A Novel Digital Watermarking Based on General Non-Negative Matrix Factorization," *IEEE Transactions on Multimedia*, vol. 20, no. 8, p. 14, 2018.
[12]. D. D. Lee, M. Hill and H. S. Seung, "Algorithms for Non-negative Matrix Factorization," *Advances in neural Information Processing Systems*, vol. 13, no. 1, pp. 556–562, 2001.
[13]. M. W. Berry, M. Browne, A. N. Langville, V. P. Pauca and R. J. Plemmons, "Algorithms and Applications for Approximate Nonnegative Matrix Factorization," *Computational Statistics & Data Analysis*, vol. 52, no. 1, pp. 1–31, 2007.
[14]. D. H. Ngoc, "Non-negative matrix factorization algorithms and applications," PhD Thesis, Universite Catholique de Louvain, Belgium, 2008.
[15]. S. Hongqin and L. Fangliang, "A blind digital watermark technique for colour image based on Integer Wavelet Transform," in *2010 International Conference on Biomedical Engineering and Computer Science, Pune, India, December*, 2010, vol. 2, no. 2, pp. 236–241.
[16]. F. J. Dyson and H. Falk, "Period of a Discrete CAT Mapping," *The American mathematical monthly*, vol. 99, no. 7, pp. 603–614, 1992.
[17]. B. J. Saha, C. Pradhan, K. K. Kabi and A. K. Bisoi, "Robust watermarking technique using Arnold's transformation and RSA in discrete wavelets," in *2014 International Conference on Information Systems and Computer Networks, Mathura, India , March*, 2014, pp. 83–87.
[18]. D. Elmaci and N. B. Catak, "An Efficient Image Encryption Algorithm for the Period of Arnold transform," *International journal of Intelligent Systems and Applications in Engineering*, vol. 2, no. 2, pp. 80–84, 2018.
[19]. H. S. Abolfazl and S. Arash, "A New Method for Color Image Watermarking Based on Combination of DCT and PCA," in *2015 International Conference on Communications, Signal Processing, and their Applications (ICCSPA'15), Sharjah, United Arab Emirates, February*, 2015, pp. 1–5.
[20]. K. D. W. Ngongang, E. Mwangi and E. Ndungu, "Blind Colour Image Watermarking Scheme Based on Quaternion and SVD Techniques," *International Journal of Engineering Research and Technology*, vol. 11, no. 6, pp. 897–908, 2018.
[21]. Z. Wang, A. C. Bovik, H. R. Sheikh, S. Member and E. P. Simoncelli, "Image Quality Assessment : From Error Visibility to Structural Similarity," *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600–612, 2004.
[22]. C. Lin, "Projected Gradient Methods for Non-negative Matrix Factorization," *Neural Computation*, vol. 19, pp. 2756–2779, 2007.
[23]. C. Pradhan, S. Rath and A. Kumar, "Non-Blind Digital Watermarking Technique Using DWT and Cross Chaos," in *2nd International Conference on Communication, Computing & Security, KIIT University, Bhubaneswar,India, November*, 2012, vol. 6, pp. 897–904.
[24]. E. Najafi, "A robust embedding and blind extraction of image watermarking based on discrete wavelet transform," *Mathematical Sciences*, vol. 11, no. 4, pp. 307–318, 2017.
[25]. T. Bandyopadhyay, B. N. Chatterji, and B. Bandyopadhyay, "Attacks on Digital Watermarked Images in the Internet Environment and their counter measures," *International Journal of Advanced Research in Computer Science*, vol. 4, no. 4, pp. 155–159, 2013.
[26]. D. O. Muñoz-Ramirez, V. Ponomaryov, R. Reyes-reyes, V. Kyrychenko, O. Pechenin and A. Totsky, "A Robust Watermarking Scheme to JPEG Compression for Embedding a Color Watermark into Digital Images," in *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kiev, Ukraine, May*, 2018, pp. 619–624.