International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 08 | Aug 2020 www.irjet.net p-ISSN: 2395-0072

Robust Video Watermarking using Invariant Quaternion Legendre-Fourier Moments & optimization with Bees Algorithm

Mrs. Vrushali Vishnu Jadhav[1], Prof. A.U. Wagdarikar[2]

[1]*Student, Dept. of Electronics &Telecommunication, V.V.P., Solapur, Maharashtra, India*
[2]*Professor, Dept. of Electronics &Telecommunication, V.V.P., Solapur, Maharashtra, India*

Abstract - *Today's fast growing world makes us more insecure in many ways like digital security, financial security and most important our digital media contents like photographs, videos. To increase our security everyone has to perform some manual operation on that or use some digital lockers. In the Digital world data security, protecting the ownership of data and copyright issues are vastly growing. So dealing with these Real world problems in the recent years have become more complex, hence more powerful optimization techniques are needed to solve these complex and unsolvable problems. Digital watermarking is an effective approach, which handles watermarking problem by encoding use or other copyright information directly in the data without providing any access restrictions to such data. In this paper a new scheme is developed for an efficient robust watermarking technique using ABC algorithm & area of best fit equation. The watermarks are embedded into the HL and LH frequency coefficient in wavelet transform domain. Science, the embedding technique is blind which does not require the original image is the watermark extraction. As well the scheme also searches the optimal location in order to improve both quality of watermarked image & robustness of the watermark. The performance of the proposed watermarking technique is watermarking technique is analyzed in terms of Peak signal-to-noise ratio (PSNR) and Normalized Correlation(NC).The experimental and the comparative results show that the proposed technique is achieved a good robustness against most of the attacks and shows appropriate optimization.*

Key Words*: *QLFM, DWT, PSNR, video watermarking, and SVD, DCT.

1. INTRODUCTION

According to today's technological environment making our digital data secure is the most challenge part in the life. For making our digital property authenticated watermarking is the only way. Watermarking is one such problem which needs to be performed well so that the authentication, security and copyright of the data which is distributed over the internet are intact.

Digital watermarking includes a pair of matching procedures one for embedding a watermark into a still or moving image and the other for detecting or extracting the watermark Readability, security, imperceptibility and robustness were the most important characteristics exhibited by watermarking technique. Watermarking is a process of securing the data from illegal actions, by adding an extra signal, called watermark signal to the original data.

The data could be an image, video or audio. This watermark signal is embedded to the original data in such a way that it doesn't change the original data in respect of its appearance and overall structure. Also this new watermarked data should be susceptible to any change performed on that data afterwards. The watermark signal should be robust enough to withstand majority of attacks such as compression, Gaussian filtering, scaling, etc.

The Digital image watermarking process should performed be in such a way that the watermark can be extracted later without doing any damage to the original image. This watermark process should deliver robustness, transparency, security of the watermark image. Watermarking can be classified into many subcategories based on their visibility, domain, and durability. In terms of domain, watermarking can be divided into two parts: spatial domain and frequency domain. The watermark is embedded by directly altering the pixel value of the original image in case of spatial domain technique.

This is rather a less complex and easy to implement. But the disadvantage of fragility of the resulted watermarked image to the various attacks, overshadow this advantageous property of spatial domain watermarking scheme. On the other hand, frequency domain technique is more robust in terms of the watermark image and less fragile to the attacks. Frequency domain scheme, also known as transform domain, modulates certain frequencies in a particular domain, such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD) and Discrete Fourier Transform The watermarking embedding procedure involves the scaling factors which are used to determine the strength of the watermark. These scaling factors should be chosen in such a way that it delineate the deformities in the watermarked image. To do so, we need multiple scaling factors rather than single scaling factor.

The selection of multiple scaling factors (MSF) is very critical as it determines the overall structure, imperceptibility and robustness of the watermarked image. This selection of MSF‟s is an optimization problem which can be solved by

many optimization algorithms such as Firefly Algorithm, Cuttlefish Algorithm, and Bat Algorithm etc.

The Artificial Bee Colony algorithm has emerged as a strong solution to these optimization problems in the field of digital image/ video watermarking. This paper presents the Artificial Bee Colony algorithm which is proved to solve many complex optimization problems of digital video watermarking.

The proposed technique is different from existing watermarking-based quaternion techniques, fast; highly accurate and numerically stable QLFM moments provided us a better visual imperceptibility and higher robustness against the geometric distortions and common signal Processing attacks.

2. LITERATURE REVIWE:

Digital watermarks are used in copyright protection and securing data during their transmission through networked environment [7, 20]. Technically, digital watermarking aims to hide a small piece of digital data called a "digital watermark" into the actual digital media such as digital images, digital videos and digital audios without significance change of its normal usage [17].

During the last two decades, researchers paid their attention to watermarking technology based on invariants moments. Alghoniemy and Tewfik [1] first applied image moments to image watermarking technology which is robust against RST attacks by using the Hu'smoment invariants. Unfortunately, their method encountered major problems such as instability and poor visual imperceptibility. Since then, a several moment-based watermarking algorithms have been proposed.

Liu et al. [16] proposed a wavelet-based watermarking scheme for color images through visual masking. A color visual model is designed to modify a perceptual model used in the image coding of gray scale images.

Color image watermarking scheme based on non-blind luminance was presented by Hussein et al. [13].

Peng et al. [21] presented a support vector machines (SVMs) based image watermarking method for color images in multi-wavelet domain, in which the special frequency band and property of image in multi-wavelet domain are employed.

Alper Koz et al. [19] designed a technique, named spread sptrum technique for the Human Visua System (HVS) based on video watermarking. This technique makes use of a temporal dimension through the temporal sensitivity of HVS. The temporal contrast and the threshold value are described for enhancing the water-mark. The spread spectrum mechanism attained improved robust-ness with respect to noisy pixels, temporal shifts, and frame rate conversions, but the method faces certain complications while employing the HVS systems.

Komwit Surachat et al. [20] developed a pixel-wise digital video watermarking technique utilizing a Weiner filter. Here, the embed-ding is done in chrominance channel for the video frame. During extraction, the filter uses a 3 × 3 window size for improving the quality of watermarking. The result generated by the pixel-wise digital video watermarking technique offered better performance and thus, improves the robustness from security attacks, but the extraction influences the accuracy.

Samira Mabtoul et al. [21] developed a Singular Value Decom-position (SVD) using a watermarking algorithm based on complicated wavelet transforms. The method considers the input data as a color image that comprises YCbCr color components. At first, the color component of every video frame applies 2-level decomposition of Dual Tree-Complex Wavelet Transform (DT-CWT) transform to obtain the sub bands and then, the SVD is finally applied. The obtained embedded image is robust against blur, histogram equalization, scaling, and Gaussian noise. In several cases, the SVD based techniques alleviate the rate of embedding.

Hui-Yu Huang et al. [22] designed a pseudo-Three Dimensional Discrete Cosine Transform (3D DCT) and quantization index modulation to initiate video watermarking. Here, the input frames were chosen on the basis of blocks, in which the message was embedded. The pseudo-3-D DCT used DCT transformations for evaluating the factor and for recovering the hidden messages efficiently. Ac-accordingly, the data is entrenched in the quantization regions of the frame using Quantization Index Modulation (QIM), but the method was susceptible to several attacks, like geometric attacks that include scaling and rotation.

Sake and Tirumala [3] developed a method by employing Bi-orthogonal Wavelet Transform (BWT) and SVD for protecting the copyrights of images. Two main processes, which include watermark extraction and watermark embedding processes, are employed for improving the efficiency of video watermarking. After embedding, the input video sequences are transformed to a total number of frames. Artificial Bee Colony (ABC) approach is adapted in BWT to produce random frames for initiating the embedding process in watermark video sequences. Further, the extraction of the watermarked image, which is considered as the reverse process of the watermark embedding, is performed where the watermark image is extracted from the video sequences.

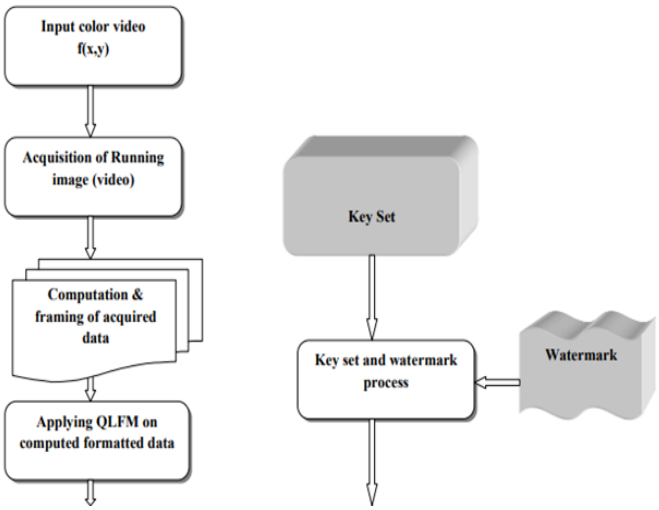
Shukla and Sharma [16] designed a scene based video watermarking technique by adapting discrete wavelet transform for protecting the video copyrights. The technique integrates vide watermarking with Successive Estimation of Statistical Measure (SESAME) technique. For reducing the

computation complexity, the watermark is embedded in the scene change frames. This technique focused on correlation-based scene change detection method. However, the method failed to consider a secure method to provide copyright protection for the embedded video.

Naseem.et al. [17] developed a block-based transform domain technique based on Fuzzy Rule Based System (FRBS), which chooses an image from a test image to embed and hold the desired capacity using high robustness. FRBS contains two phases, in which the initial process selects candidate image blocks, and the second process selects the coefficients from the chosen candidate blocks to embed the desired capacity. At last, the image is chosen as a candidate image, which contains improved Peak Signal to Noise Ratio (PSNR) and correlation values with equal desired capacity. The technique failed to increase the capacity of data embed while retaining high imperceptibility and robustness and suffers from high computational complexity.

3. METHADOLOGY:

Accurate and stable computation of the QLFMs moments is an essential step which results in accurate and robust watermarking algorithms. Since the QLFMs are defined in a circular domain, computational processes in polar coordinates are preferable. In this subsection, a summary of this accurate method will be presented. In this method we are using QLFM technique for input color video. Moreover, the LFM coefficients are more suitable for robust watermarking. The proposed technique is different from existing watermarking-based quaternion techniques, fast, highly accurate and numerically stable QLFM moments provided us a better visual imperceptibility and higher robustness against the geometric distortions and common signal processing attacks the detail explanation are explain as follows:



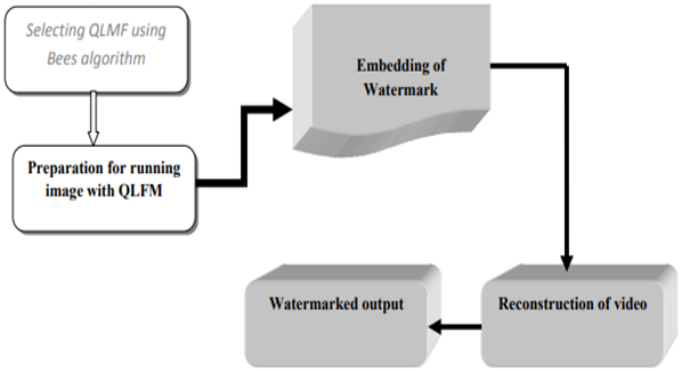


Fig -1: Methodology of our project

3.1 RUNNING IMAGE ACQUISITION:

In the process of video watermarking firstly we have to input some running images or video using quaternion Fourier transform of color images. These color images can be selected as frame of image for the watermark purpose. Color image pixels have three components, and they can be represented in quaternion form using pure quaternions.
For example, a pixel at image coordinates (m, n) in an RGB image can be represented as

$$f(m, n) = R(m, n)\mathbf{i} + G(m, n)\mathbf{j} + B(m, n)\mathbf{k}.$$

Where R(m, n) is the red component, and G(m, n) and B(m, n) are the green and blue components of the pixel, respectively. The same approach may be used with a luminance-chrominance color space, such as YCbCr. The choice of the imaginary part to represent pixel values is determined by interpretation of color pixels as vectors.
These running images acquisition process uses the quaternion Fourier transforms for the acquisition of image.

$$I = \{R(x, y), G(x, y), B(x, y)\}\ (0 \le x < M, 0 \le y < N)$$

3.2 FRAMING OF ACQUIRED IMAGE DATA:

For the process of watermarking we have select certain frame of image for placing the watermark over that frames in this process in order to dispel the pixel space relationship of the binary image, and improve the robustness of the whole digital watermark system, image scrambling algorithm is used at first.

In this scheme, the acquired image is scrambled from W to W1 by using transformation.
it is given by

$$(x, y) = (1,1,1,2)(x,y)(\text{mod } N)$$

where (x, y) is the pixel of the image, (x, y) is the pixel of the image after scrambling, N is order of image matrix. Since the transformation is periodic, the number of scrambling can be considered as the key to enhance the security. After that, the

scrambled binary image W1 is divided into watermark blocks
Wk of 2 ×2 bits Wk = {wk(i, j), 0 ≤ i ≤ 1, 0 ≤ j ≤ 1} (k = 1, 2, . . . , p/2 ∗ Q/2)

3.3 APPLYING QLFM ON DATA AND SELECTING USING BEES ALGORITHM:

The robustness of the proposed watermarking algorithm is enhanced by selecting the most suitable QLFMs moments based on two factors.

The first one, QLFMs moments with
q = 4m, m ∈ Z(i.e. q = 0, q = 4, q = 8, q = 12, ...) are dropped from the selection process where are not suitable for encoding watermark bits.

The second factor, only the independent QLFMs moments with positive repetition q > 0 are used. The QLFMs moments with negative repetition q < 0 are dependent, and then are dropped to avoid information redundancy.

Therefore, according to geometric invariance and the reconstruction accuracy of QLFMs coefficients, the independent and accurate final moment set used for watermark embedding in the proposed scheme based on selection process could be described as follows:

S ={ Mpq, q≠4m ,m∈Z}

For a watermark bit sequence of length equal to l = P × Q, the performance of the watermarking algorithm could be increased by selecting form the feature vector:
M(1) = {Mp1q1, Mp1q2, ...,Mp1q1

In order to optimize both the quality of watermarked image and robustness of the watermarked image, proposed scheme uses of the artificial bees colony algorithm to search for the optimal steps. ABC algorithm is applied in the watermarked embedding and the watermark extraction processes for the optimization process. The evaluation function of this process is computed by using factors such as PSNR and NC that relate to both imperceptibility and robustness of a watermark. A high quality extracted watermark image and robust watermark can then be achieved.

3.4 WATERMARK EMBEDDING:

In the watermark embedding process key sets are used these unique set of keys help to achieve the secure watermarking process. In our digital watermark embedding scheme, the block watermark embedding strategy is adopted. The watermark block Wk with 2 × 2 watermark bits is embedded into the color image blocks Bk with 8 × 8 pixels by modifying the real quaternion Fourier transform coefficients as shown in following figure:

$$a'_k(1,1)=\begin{cases}2\Delta*round(a_k(1,1)/2\Delta)+\Delta/2 \text{ if } & w_k(0,0)=1\\ 2\Delta*round(a_k(1,1)/2\Delta)-\Delta/2 \text{ if } & w_k(0,0)=0\end{cases}$$

$$a'_k(1,2)=\begin{cases}2\Delta*round(a_k(1,2)/2\Delta)+\Delta/2 \text{ if } & w_k(0,1)=1\\ 2\Delta*round(a_k(1,2)/2\Delta)-\Delta/2 \text{ if } & w_k(0,1)=0\end{cases}$$

$$a'_k(2,1)=\begin{cases}2\Delta*round(a_k(2,1)/2\Delta) \text{ if } & w_k(1,0)=1\\ 2\Delta*round(a_k(2,1)/2\Delta) \text{ if } & w_k(1,0)=0\end{cases}$$

$$a'_k(2,2)=\begin{cases}2\Delta*round(a_k(2,2)/2\Delta) \text{ if } & w_k(1,1)=1\\ 2\Delta*round(a_k(2,2)/2\Delta) \text{ if } & w_k(1,1)=0\end{cases}$$

Fig -2: Real Quaternion Fourier Transforms Coefficients

(k = 1, 2, . . . , P/2 ∗ Q/2)

Where,
Wk = {wk(i, j), 0 ≤ i ≤ 1, 0 ≤ j ≤ 1} is the digital watermark block,
Ak = {ak(i, j), 0 ≤ i ≤ 7, 0 ≤ j ≤ 7} is the old real quaternion Fourier transform coefficients block of color image blocks

Bk, Ak = {ak(i, j), 0 ≤ i ≤ 7, 0 ≤ j ≤ 7} is the new real quaternion Fourier transform coefficients block, round(·) denotes round operator, is the watermark embedding strength.

4. ATTACKS:

There are four categories based on the classification: Removal attack, Geometric attack, Cryptographic attack and Protocol attack.

4.1Removal attack:

Removal attack aims at the complete removal of the watermark information from the watermarked data without breaking the security of the watermarking algorithm. Most of image processing methods, such as image smoothing and Gaussian noise, belong to removal attack category.

4.2Geometric attack:

Geometric attack is different from removal attack. Instead of removing the watermark signals out from the watermarked data, geometric attack intends to distort the watermark detector synchronization with the embedding information. Rotation, scaling and translation attacks are the most famous algorithm in geometric attack.

4.3 Cryptographic attack:

The aim of **cryptographic attacks** is to break the security of watermarking schemes and thus find a way to procedurally

remove the embedded watermark information or to embed misleading watermarks. One of the techniques in this category is the brute-force search method. This technique extensively attempts to identify the used watermark algorithm by using a large number of known possible measures and extract the watermark.

4.4 Protocol attack:

Protocol attack is a different type of watermark attack in a sense that it targets the entire concept of using watermarking techniques as a solution to copyright protection rather than the watermark itself. Whereas the other types of attacks aim at destroying, distorting or extracting the watermark signal, protocol attacks aim at producing ambiguities on the true ownership of the data in question. An example of a protocol attack is the copy attack; instead of destroying the watermark, the copy attack estimates a watermark from watermarked data and copies it to some other data with the purpose of attacking the credibility of such watermark in claiming ownership.

4.5 Interference Attack:

Interference attacks are those which add additional noise to the watermarked object. Loss compression, quantization, collusion, de noising, demodulation, averaging, and noise storm are some examples of this category of attacks.

4.6 Low Pass Filtering Attack:

A low pass filtering is done over the watermarked image and it results in a difference map composed of noise.

5. RESULT:

Following screens show the process of embedding, extracting of watermark into video and framing of the video.

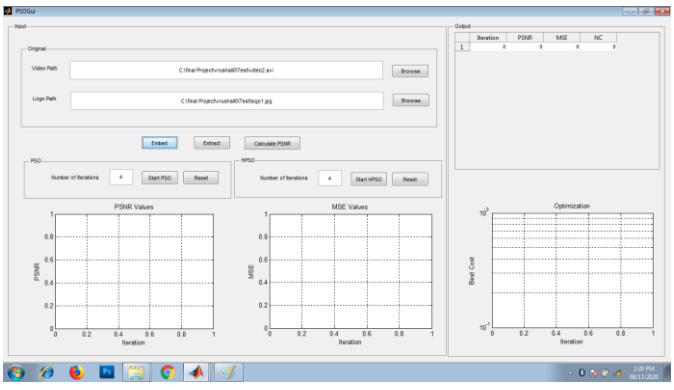


Fig -3: Main dashboard of video watermarking

In this screen the PSNR value, MSE value and optimizations displayed in the form of graphical representation.

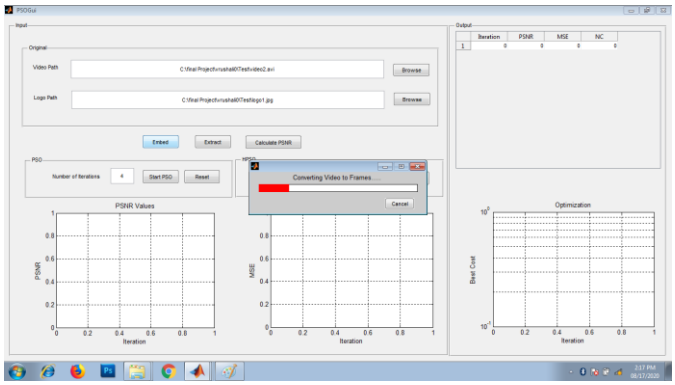


Fig -4: Converting Videos into Frames

In this screen after selection of the sample video file it converts the video part into number of frames for the further process.

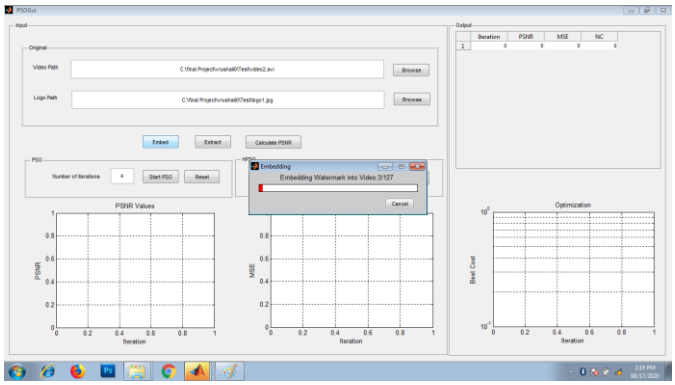


Fig -5: Embedding the watermark into video

After converting video into the frames embedding of watermark to video gets started and embed the selected watermark on frames of video.

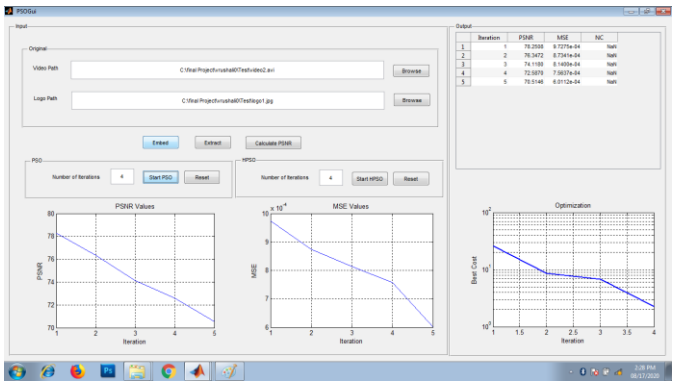


Fig -5: Final embedded watermarked output window

This window shows the final output of watermarked video shows PSNR vales MSE values in the form of graphs.

6. CONCLUSION

The existing color running image watermarking schemes were always designed to mark the image luminance component only, which are sensitive to color attacks and geometric distortion. In this project, we have proposed a blind color watermarking method in quaternion Fourier transform domain. The method embeds the watermark information into original color video by adaptively modulating the real coefficients of quaternion Fourier transform.

REFERENCES

[1] Alghoniemy M, Tewfik AH (2004) Geometric invariance in image watermarking. IEEE Trans Image Process 13(2):145–153

[2] Al-Otum HA, Al-Taba AO (2009) Adaptive color image watermarking based on a modified improve pixel-wise masking technique. Comput Electr Eng 35(5):673–695

[3] Bianchi T (2013) Secure watermarking for multimedia content protection: a review of its benefits and open issues. IEEE Signal Process Mag 30(2):87–96

[4] Chauhan DS, Singh AK, Kumar B, Saini JP (2017) Quantization based multiple medical information watermarking for secure e-health. Multimedia Tools and Applications:1–13.

[5] Chou CH, Liu KC (2010)A perceptually tunedwatermarking scheme for color images. IEEE Trans Image Process 19(11):2966–2982

[6] Chu SC, Huang HC, Shi Y,Wu SY, Shieh CS (2008) Genetic watermarking for Zerotree-based applications. Circuits, Syst, Signal Process 27(2):171–182

[7] Cox IJ, Millter ML, Bloom JA, Fridrich J, and Kalker T (2008) Digital watermarking and steganography. Morgan Kaufmann Publishers (Elsevier), Burlington,

[8] Ell TA, Sangwine SJ (2007) Hypercomplex Fourier transforms of color images. IEEE Trans Image Process 16:22–35

[9] Hamilton WR (1866) Elements of quaternions. Longmans Green, London

[10] Hosny KM (2011) Accurate orthogonal circular moment invariants of gray-level images. J Comput Sci 7(5):715–722

[11] Hosny KM, Darwish MM (2016) A Kernel-Based method for Fast and accurate computation of PHT inpolar coordinates, Journal of Real-Time Image Process., J Real-Time Image Proc, doi: https://doi. org/10.1007/s11554-016-0622-y, p. 1–13 (Online first)

[12] Hosny KM, Darwish MM (2017) Invariant image watermarking using accurate polar harmonic transforms.Comput Electr Eng 62:429–447

[13] Hussein JA (2012) Luminance-based embedding approach for color image watermarking. Int J Image Graph Signal Process 4(3):49–56

[14] Huang, H.-C., Pan, J.-S., Chu, C.-M.: 'Optimized copyright protection systems with genetic-based robust watermarking'. IEEE Int. Conf. on Intelligent Information Hiding and Multimedia Signal Processing, 2007

[15] Huang, H.-C., Chen, Y.-H., Abraham, A.: 'Optimized watermarking using swarm-based bacterial foraging', J. Inf. Hiding Multimed. Signal Process., 2010,1, (1), pp. 51–58

[16] Shukla D, Sharma M. A new approach for scene-based digital video watermarking using discrete wavelet transforms. Int J Adv Appl Sci 2018;5(2):148–60.

[17] Naseem MT, Nadeem M, Qureshi IM, Hussain A. Optimal secure informationusing digital watermarking and fuzzy rule base. Multimed Tools Appl 2018;,78 , 6 :1–22.

[18] Thongkor K, Amornraksa T, Delp EJ. Digital watermarking for camera-captured images based on just noticeable distortion and Wiener filtering. J Vis Commun Image Represent 2018;53:146–60.

[19] Koz A, Alatan AA. Oblivious spatio-temporal watermarking of digital video by exploiting the human visual system. Circu Syst Video Technol 2008;18(3):326–37.

[20] Surachat K, Amornraksa T. Pixel-wise based digital watermarking using Weiner filter in chrominance channel. In: Proceedings of International Symposium on Communications and Information Technology; 2009. p. 887–92.

[21] Mabtoul S, IbnElhaj Ehassan, Aboutajdine D. Robust colour image watermarking based on singular value decomposition and dual tree complex wavelet transform. In: Proceedings of International Conference on Electronics, Circuits and Systems; 2007. p. 534–7.

[22] Huang H-Y, Yang C-H, Hsu W-H. A video watermarking technique based on pseudo-3-d dct and quantization index modulation. Inform Foren Secu 2010;5(4):625–37.

[23] Bassil Y. Image steganography based on a parameterized Canny edge detection algorithm. Int J Comput Appl 2012;60(4):0975–8887.

[24] Ritika R, Kaur S. Contrast enhancement techniques for images–a visual analysis. Int J Comput Appl 2013;64(17):20–5.