International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6, August, 2019

# Efficient Security Based Video Watermarking Technique using Chaotic Encryption with Discrete Cosine Transform

**J. Udayakumar, G. Prabakaran, P.Elango**

***Abstract*: In this paper, a novel chaotic encryption-based blind digital video watermarking technique (DVWT) is presented for grayscale and color images. This method makes use of Discrete Cosine transform (DCT) prior to embed the watermark in the hosting video. The hosting video is split into frames of 8*8 nonoverlapping blocks before employing DCT, and watermark bit is implanted by altering the variations among the nearby DCT coefficients of neighboring blocks. Arnold transform is applied for chaotic encryption to offer extra security to the watermark. A set of three versions of the proposed model has been applied and the results are investigated. The experimental outcome confirms that the DCT-VWT is efficient on different image processing functions such as JPEG compression, sharpening, cropping, and median filtering. The comparative analysis ensures that the presented DCT for digital video watermarking technique (DCT-DVWT) is efficient under subjective as well as objective way.***

***Keywords*: Video watermarking; Chaotic Encryption; DCT; PSNR.***

## I. INTRODUCTION

In the past decade, Internet gains high significance in day to day life in several aspects. It converted the whole world to a global village recently by allowing massive data communication of digital data like document, image, video sequence, and so on. But, the advancement in recent technologies leads to more security issues since data can be altered or used with no prior authorization. The security issues might be risks may comprise of patent violations, piracy, hacking, unauthenticated generation and dissemination, data stealing and numerous other algebraic and disparity attacks [1]–[4]. Based on the Motion Picture Association of America (MPAA), millions of dollars and several thousands of jobs are gone yearly because of the copyright violations of movies, audio and software companies. In May 2014, 'Guardian' revealed that a yearly loss of 20.5 billion USD for violation in film industry. For verifying the loss, the US assembly announced a Stop Online Piracy Act (SOPA). Additionally, in patent and copy shield of multimedia data, the privacy and security are of ultimate significance. For instance, for medical images, the images and Electronic Patient Record (EPR) is transmitted to interested destinations through insecure channels of Internet [5]–[13]. A small variation of these medicinal images can leads to improper analysis and thus results in a deadly health difficulty. In these scenarios, the design of existing techniques for protected and trustworthy multimedia data is greatly required. As cryptography have been employed as a probable scheme to undertake few challenges, however, these approaches includes the adjustment in data visual and statistical way that frequently arouse distrust and tempt attacks [14]–[16]. Data hiding, make use of steganography [17]–[20] and watermarking techniques [21]–[23], have flourish as an efficient and substitute technique for security, authentication, and IPR challenges in multimedia data. Digital video watermarking technique (DVWT) is revealed as an important solution to protect IPR and authenticate content. It is a method to hide data in hosting media like video, images, etc., to make them invisible to human visual system (HVS). It makes sure the safety of the data concealed in the images/videos and carry on as a fundamental component to handle various multimedia related IPR issues. A digital watermark may be a company logo, doctor's signature, patient's data, etc. The performance of the watermarking method is fixed by different main variables such as robustness, payload, imperceptibility, and security [24]. There exists a tradeoff among the variables as explained by the prominent disagreement triangle [25]. Digital watermarking methods are partitioned to three kinds of watermarking attacks: robust, delicate or semi-delicate method [26]–[29]. Robust watermarks endure many image processing functions and are well suitable to protect copyright any verify ownership, whereas the delicate watermarks vanish when the watermarked media experiences a minor adjustment and are appropriate for authentication and integrity. Watermarks are normally embedded in two domains: pixel and transform coefficient domains. In the former type, the hosting image pixels are straightly modified based on the watermark bits. It is easily with high payload and low computation cost. In addition, many of the pixel domain approaches provide less robustness. In the latter method, the frequency coefficients of any transform are modified based on the watermark bits.

Revised Manuscript Received on October 30, 2019.
* Correspondence Author
**J. Udayakumar*,** Research scholar, Dept., of CSE,FEAT, Annamalai university, Chidambaram, India. Email: uday.ja@gmail.com
**Dr. G. Prabakaran,** Associate Professor, Dept., of CSE,FEAT, Annamalai university, Chidambaram, India. Email: gpaucse@yahoo.com
**Dr. P. Elango,** Assistant Professor Dept. of IT, PKIET, Karaikal, India. Email: elanalin74@gmail.com

They attain high robustness but with minimum computation complexity and minimum payload.

Discrete Wavelet Transform (DWT) and Discrete Cosine transform (DCT) are the important transforms comes under coefficient approaches [30]–[32]. A genetic algorithm (GA) based multi-watermarking methods make use of DWT and singular value decomposition (SVD) has been proposed [33]. They showed better robustness and imperceptivity, they fail to concentrate on security and computation complexity. From the different transform domain methods, DCT is found to be effective because of the less complexity. The DCT of an image can be computed by three ways: entire image, blocks of the image or determined in spatial domain. In every approach, watermark is embedded by the modification of DCT coefficients.

It is mainly categorized into DC, middle and higher frequency coefficients. To protect copyrights, the watermark should tolerate many image processing assaults; hence, it can be attained by inserting it in low frequency coefficients. As low frequency coefficients holds significant part of visual data of an image, consequently, adjustment of these coefficients results to poor quality of the watermarked image. To maintain authenticity, it is possible to embed watermark in high-frequency coefficients due to the fact that a small variation in the image will alter the high-frequency coefficients significantly. To attain optimum values of robustness and insensitive, the mid-frequency coefficients can be embedded into the watermark. Security in framework is a main concern in the digital image watermarking methods. To offer security, cryptographic approaches have been verified as a demanding factor, particularly for images in military and healthcare applications where privacy is a significant parameter. The traditional data encryption methods such as data encryption standard (DES), advanced encryption standard (AES), etc. have depicted poor performance on digital images because of the issues of correlation and redundancy.

At the same time, chaos based encryption methods offer better performance because of unique features like sensitiveness, periodicity, pseudorandom activities, and ergodic character. This leads to the common use of chaotic approaches and are available in the literature. Different watermarking methods have been developed with an intention to tackle IPR and security challenges. A detailed review of the stated work results to the fact that many of the reported work concentrates on the enhancement of only one parameter like security, payload, imperceptivity, and robustness or computation efficiency. Every watermarking approaches falls under two types: spatial based which alters the pixel values straightly and transform based method where the transform coefficients are selected as embedding locations. [34] presented a practical video watermarking method high quality video content.

They employ a quantization index modulation method for low frequency components of full – frame DCT frames computed by decoding partially compressed videos. [35] introduced a fragile watermarking method for authenticating MPEG-4 AVC stream. [36] introduced a video watermarking method using SVD that is executed in the DWT domain. [37] presented a video watermarking method using discrete Fourier transform (DFT) and Radon transform. They partition the video series to a collection of images and determine the 1-dimensional DFT with the temporal direction of every group and lastly selects the maximum temporal frequencies to implant the watermark in the radon transform of chosen frames. [38] performed a 3D wavelet transform over the moving region of video by the use of a collection of pseudo random numbers, the watermark is embedded to the 3D wavelet coefficients of a number of definite sub-bands. [39] presented an efficient method using chaotic maps in DWT domain. The watermark signal to be employed undergoes encryption with the chaotic map. For developing a robust method, a set of wavelet coefficients of Iframes are chosen for embedding locations.

As far from the literature, there is no existence of a method that attains optimum solution which results to a secured, unnoticeable, robust and less complex method. In this paper, we present an optimum VWT which manages different challenges such as payload, security, invisibility, robustness, and so on. We proposed a DCT based video watermarking technique named as DCT-VWT by employing DCT prior to embedding phase. Chaotic encryption and Arnold transform are also used to increase the security level.

The major contributions are listed here.

- The DCT-VWT method is dynamic in nature in terms of grayscale as well as color images based on the application requirement.
- Inter-block coefficient correlation is used to embed watermarks in the image for facilitating effective robustness and payload.
- Watermark bits have been embedded by modifying the variation among two predefined DCT coefficients of the two neighboring blocks. The alteration is done in such a way that it is resistant to different image processing and geometric attacks.
- Nonlinear dynamics of chaos and Arnold transform is employed to improve watermark safety. The wide sections of this paper are given as follows.

The presented DCT-V method is explained in Section 2. The results are discussed in detail in Section 3 and the paper is ended in Section 4.

## II. THE PROPOSED METHOD

The processes involved in the projected DCT-VWT are demonstrated in Fig. 1. The two significant subsystems of projected systems are watermark security unit and watermark embedding unit. The securing unit focused at the process of enhancing the embedded watermark security in order to create unfeasible for an opponent to derive precise watermark even though it has some information of embedding technique. To reach an enhanced security, Arnold encryption and Chaotic theory are employed. In the following subsections, the geometrical preliminary of Chaos and Arnold encryption are demonstrated.

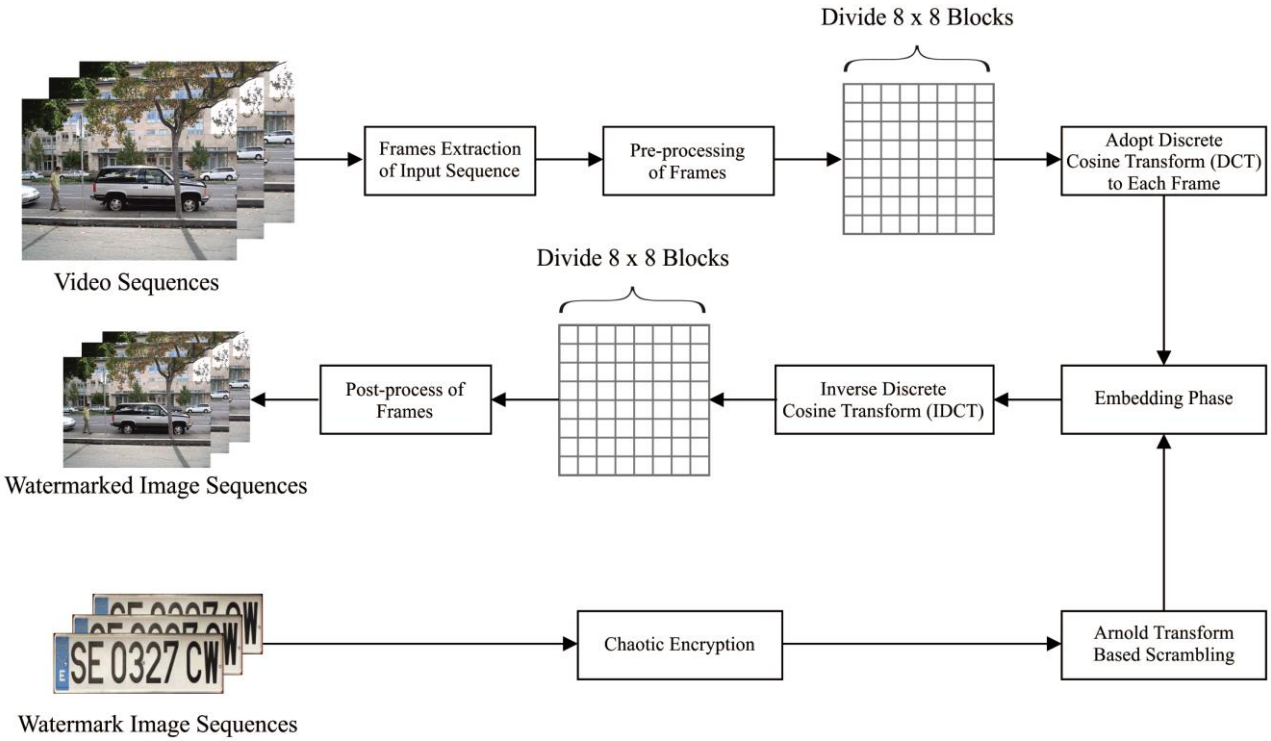


Fig. 1. Block diagram of the DCT-VWT

### A. Chaos and Arnold Encryption

For data encryption, a chaotic based encryption approach is an efficient technique. Dynamic behavior, irreversibility, pseudo-randomness are the qualities that the Chaos signals comprised of. For initial parameters, the systems comprising chaotic nature contain highly sensitivity nature. The output chaotic series is same as the white noise comprising arbitrary behavior with enhanced complexity and correlation and is described as

$$C_{n+1} = \mu \times C_n \times (1 - C_n) \quad (1)$$

Where $0 < \mu < 4$, especially μ is preset to rate 3.9 so as to reach high randomness and $0 < C_n < 1$ is the n$^{th}$ value produced from Eq. (1). Through adjusting the rate of n from 0 to L-1, various rates of $Cn$ can be gained. Here, L is the highest count of chaotic rates. We can derive the needed chaotic signal through setting the primary rates of μ and $C0$. The implication of chaotic encryption has been demonstrated to provide enhanced security, as it provides the joint benefit of security and speed. By using various encryption techniques, the data security can be enhanced, and one among the efficient method is Arnold transform. The Arnold transformation is geometrically demonstrated as

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (modN) \quad (2)$$

In two dimensional matrix, (x, y) and $(x,)$ demonstrate the encrypted image pixel coordinates and the input image. The transformed outcome in the pixel position modifications to produce an image that is chaotic and varies from the actual image. Arnold transform result to an encrypted image that comprises one to one association with actual image. It is not probable to break the Arnold encryption outcomes scrambled image without knowing the series employed as it contains a nature of pseudo-random. The encryption strength is based on the iteration numbers that can be described at the initial stage of the process. For decrypting the encrypted message, Inverse Arnold transform is employed by the Eq. (3).

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} (modN) \quad (3)$$

### B. Watermark and Cover Generation

Through the pre-processing unit, the input image 'I' is passed that plays as a grayscale image buffer and as a color images converter as demonstrated in Fig. 1. The pre-processing unit modifies the input RGB image into YCbCr image, where Y refers to luminance data, Cr refers to chrominance red image data and Cb refers to chrominance blue data. When comparing with chrominance data, luminance portion 'Y' acts as the watermark cover due to the part changing of the image gives low visible modifications to the original image. At the same time, in every plane, three watermarks are embedded to an RGB image. Then, the unit of pre-processing derives the RGB planes and then sorts entire three planes in a 2D matrix as every plane can be treated through the system as P × Q grayscale plane, where P and Q correspondingly demonstrates cover image row and column. Within a rate of −128 to 127, the values of resulting matrix are gained through subtracting 128 from the matrix.

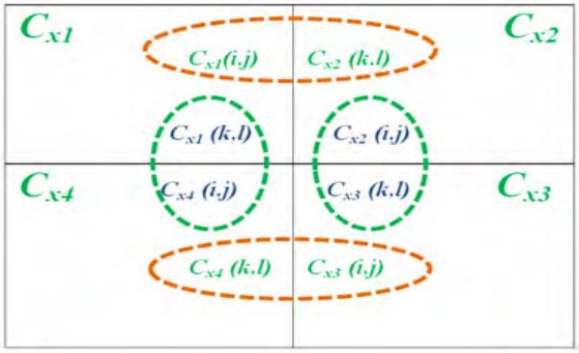


**Fig. 2. Coefficient selection**

The resulting matrix is segmented into 16×16 blocks after pre-processing. The number of blocks will be $\frac{P}{16} \times \frac{Q}{16}$, for an P × Q dimension input image. Let $B_x$ be a random block represented into 8 × 8 blocks, the block $B_x$ is classified additionally. As demonstrated in Figure 1, the four 8 × 8 blocks of block $B_x$ are demonstrated by $B_{x1}$, $B_{x2}$, $B_{x3}$ and $B_{x4}$. Hence, the sum of 8×8 blocks is equivalent to $4 \times \frac{P}{16} \times \frac{Q}{16}$. The sum of bits that can be inserted into a host image is equivalent to the sum of 8 × 8 blocks. The projected method uses DCT coefficient correlation advantages of neighboring blocks. Hence, every block DCT is estimated. As demonstrated in Fig. 2, let DCT coefficient blocks with respect to block $B_x$ be demonstrated through $C_{x1}$, $C_{x2}$, $C_{x3}$ and $C_{x4}$. The difference among two already selected DCT coefficients of two neighboring blocks is estimated for embedding a watermark bit and is expressed as

$$D = C_{xy}(i,j) - C_{xy+1}(k,l) \quad (4)$$

In a sub-block and $l \leq i, j, k, l \leq 8$, x = 1,2,3,4, . . . .,$\frac{P}{16} \times \frac{Q}{16}$, where $(i,j) \neq (k,l)$, provides chosen coefficient whose rate demonstrates to the 16 × 16 pixel blocks the coefficient belongs while as y = 1,2,3,4. Let us assume $i, j, k$ and l as 3, 3, 3 and 2 for the present task. From this fig. 2, $C_{x5} = C_{x1}$ as 4 Mod y = 0 as is absolute. It is obvious from fig. 2 and eq. (3), to embed the initial watermark bit the variation among coefficient selected from Block $C_{x1}$, $C_{x2}$, $C_{x3}$ and $C_{x4}$, $C_{x1}$ and a coefficient selected from block $C_{x2}$ is estimated. At the same time, block $C_{x2}$, block $C_{x3}$ and block $C_{x4}$ are chosen to embed second watermark bit and blocks $C_{x4}$ and $C_{x1}$ are chosen to embed fourth bit. The modulation is done with difference 'D' in order to data bit that are to be embedded. To enhance the security prior to watermark embedding 'w', two-level watermark encryption is done. Initially, in order to below equations, chaos encryption is implied to the watermark.

$$C'(x) = round(C(x) \times 10^4) \quad (5)$$

$$C''(x) = round(C(x) \times 10^4 \quad (6)$$

$$b(x) = xorofallthebitsofC''(x) \quad (7)$$

Through the chaos equation (6), 'C' refers to the series that is produced. Through multiplying $C$ with 104, $C'$ refers to the four digit integer and it is rounded to the closer integer, $C''$ refers to the binary representation of series $C'$ and 'b(x)' refers to binary bit produced from $C''(x)$ in order to eq.(7), through XOR-ing entire bits of $C''(x)$. The chaos series length has been taken as one lakh, and in this series, only pre-chosen 4096 rates are employed. Through XOR operation among the series of 'b' and 'w', the initial watermark encryption level is reached and expressed in equation (8).

$$w_{e1} = w(x)XORb(x) \quad (8)$$

After the initial encryption level, '$w_{e1}$' is the watermark image. To derive the second encrypted watermark level '$w_e$', the Arnold transform is done on series '$w_{e1}$'

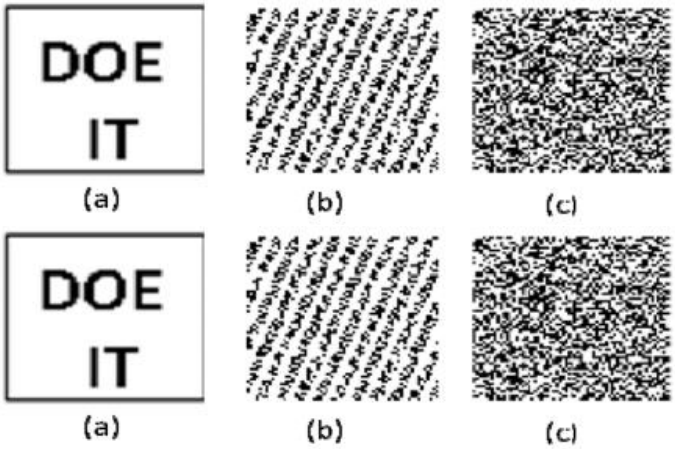


**Fig. 3. (a) Original watermark, (b) first level encrypted watermark and (c) second level encrypted watermark**

In Fig. 3, the encrypted and input watermarks are demonstrated. The main benefit of the two techniques of encryption is that it does not require a huge key overhead. To decrypt at the receiver end,

the iteration counts, logistic mapping and initial value are the key elements that are employed. Once the rates of μ, $C_0$, and L are known the watermark security is not high and we can project correct series through eq. 1 and therefore decryption is done simply. For Various attribute selection, we employed various keys to secure the attributes. To a rate of 1.34 to 3.9, the logistic parameter 'μ' is constrained and is estimated through employing an 8-bit key as expressed below:

$$\mu = 1.35 + \frac{decimal(K_1)}{100} \quad (9)$$

Where $K_1$ refers to an 8-bit key which provides security to the logistic parameter. At the same time, the primary rate of $C_0$ is estimated by employing a four-bit key $K_2$is expressed as

$$C_0 = 0.1 + \frac{decimal(K_2)}{17} \quad (10)$$

The $C_0$ value varies among 0.1 and 0.9. In the chaotic sequence, the sum of chaotic rates 'L' is estimated through using a 19-bit key $K_3$,as expressed by

$$L = 4096 + decimal(K_3) \quad (11)$$

The chaotic series 'C' is classified into chunks, every chunks of 2048 sample long. Let the sum of chunks be $n_c$. Only two chunks are chosen over the other chunks and to choose every chunk, eight bits are employed. To choose two chunks, a sum of 16 bits are needed. Let $K_4$ demonstrate the one chunk address then the second chunks address is estimated as

$$K_4 = n_c - decimal(K_4) \quad (12)$$

The second chunk address is demonstrated by $K_5$. To create a series of 4096 rate, these two chunks are merged that is precisely the watermark length. At the initial level, for encryption, the Eqs. (5)-(8) are employed. The only key for Arnold transform is the iteration number that is chosen through 6-bit key $K_6$ at the second encryption level. To improve the watermark security, a master key K of 53 bits is employed.

$$K = K_1 : K_2 : K_3 : K_4 : K_5 : K_6 \quad (13)$$

## C. WATERMARK EMBEDDING

As demonstrated in Fig. 1, there is a need to embed four bit encrypted watermark in one among every pair of DCT blocks for a 16 × 16 block which is given. For '1' and '0' bits embedding, fig. 5 and 6 correspondingly demonstrates the flow chart. Based on the pre-embedding variance among two coefficients for hiding bits '1', the 'D' is considered as zone 2 or zone 5. The coefficients $C_{xy}(i,j) and C_{xy+1}(k,l)$ are changed if 'D' lies in zone 1 or 3 in a manner that the variation among it attains zone 2 that it is closer zone. Over bit '1' data is to be carried out in either zone 2 or zone 5. Through changing the variation to the closer zone there is reduction in image quality by little when comparing with the adjacent. At the same time, the difference remains in zone 2 to embed bit '0' and it is changed to zone 1, then it is changed as zone 4, if it remains in either zone 5 or zone 3. In zone 4 or zone 1, the bit '0' data is saved. Through a guard band of 2S, the variant zone for specified bit are distinguished where S refers to the strength while embedding which it supports for proposed watermarking system robustness and is shown in figure 3, 5 and 6. To the watermark, this guard band brings additional robustness. From 5 to 20 ranges, the S rate in this task has been selected. To the rate of S, the system robustness is relative directly when imperceptivity is relative inversely to S. As demonstrated in Fig. 1, IDCT of every changed after complete embedding. Through the operations of IDCT that involve addition of 128 to every element of changed Blocks B∗x as the intensity of the pixel varies from 0 to 255. In circumstances like converting resulting matrix into three planes and luminance component embedding that commonly three-color planes for watermarked color image, it involves YCbCr to RGB conversion. The final image that is watermarked is created after completing of post-processing operations.

## D. WATERMARK EXTRACTION

Watermarked image is partitioned into 8×8 blocks and16×16 blocks are done by the following phases such as pre-processing. Similar to the process of watermark embedding, DCT computation is carried out. For extracting watermarks, the DCT coefficients that are changed while embedding are employed. Through analyzing the variation among the two preset coefficients, watermark bit is gained. Bit '1' is gained if the variation remains in zone 5 or zone 2 during bit '0' is obtained. The data bearing zone present a 2S guard band that is distinguishing it from every other; therefore, S is assumed as zero for extraction; hence image processing operations may not tend to wrong extraction of bit, as difference in transition from zone boundaries. This is reason for the system robustness. To gain actual watermark image, process of decrypting is used after deriving entire bits from hosting image.

# III. EXPERIMENTAL RESULTS AND DISCUSSION

To validate the presented DCT-VWT, a detailed investigation on diverse grayscale and color images, every individual 512 × 512 in sizes as shown in Figs. 4 and 5 [42]. The logo, as depicted in Fig.4, has been employed for watermarking grayscale images and the logos shown in Fig. 5 has been employed for color images. Every three binary logos are 64×64 in size. The objective results of the proposed method have been investigated by the use of various objective image quality indices such as Peak Signal to Noise Ratio (PSNR) and structural similarity (SSIM). The higher value of PSNR and SSIM implies better results. Higher NCC and lower BER show that the system is highly resilient to attacks. PSNR can be defined as follows.

$$\text{PSNR} = 20\log_{10}\frac{\max|P_{i,j}|}{\text{RMSE}} \quad (14)$$

where $\max|P_{i,j}|$ indicates the maximum pixel value where it is set to be 1 for bi-level images and 255 for gray scale images. To represent better similarity among two images, the value of PSNR lies between 20 to 40. SSIM is a complementary metric of the traditional measures such as PSNR and MSE. It is a HVS dependent metric for the identification of structural similarity between the reference and distorted images [14]. It is a procedure to model the distortion of the image through the integration of contrast sensitivity function (CSF), channel decomposition, loss in correlation and luminance. The value of SSIM ranges between 0 and 1. The value nearer to 1 indicates higher similarity among two images and the value closer to 0 represents poor resemblance.

$$\text{SSIM} = \frac{(2\mu_x\mu_x+C_1)(2\sigma_{xy}+C_2)}{(\mu_x^2+\mu_x^2+C_1)(\sigma_x^2+\sigma_x^2+C_2)} \quad (15)$$


**Fig. 4. Test grayscale video sequence**

*Retrieval Number F8113088619/2019©BEIESP*
*DOI: 10.35940/ijeat.F8113.088619*
*Journal Website: www.ijeat.org*

*Published By:*
*Blue Eyes Intelligence Engineering*
*& Sciences Publication*

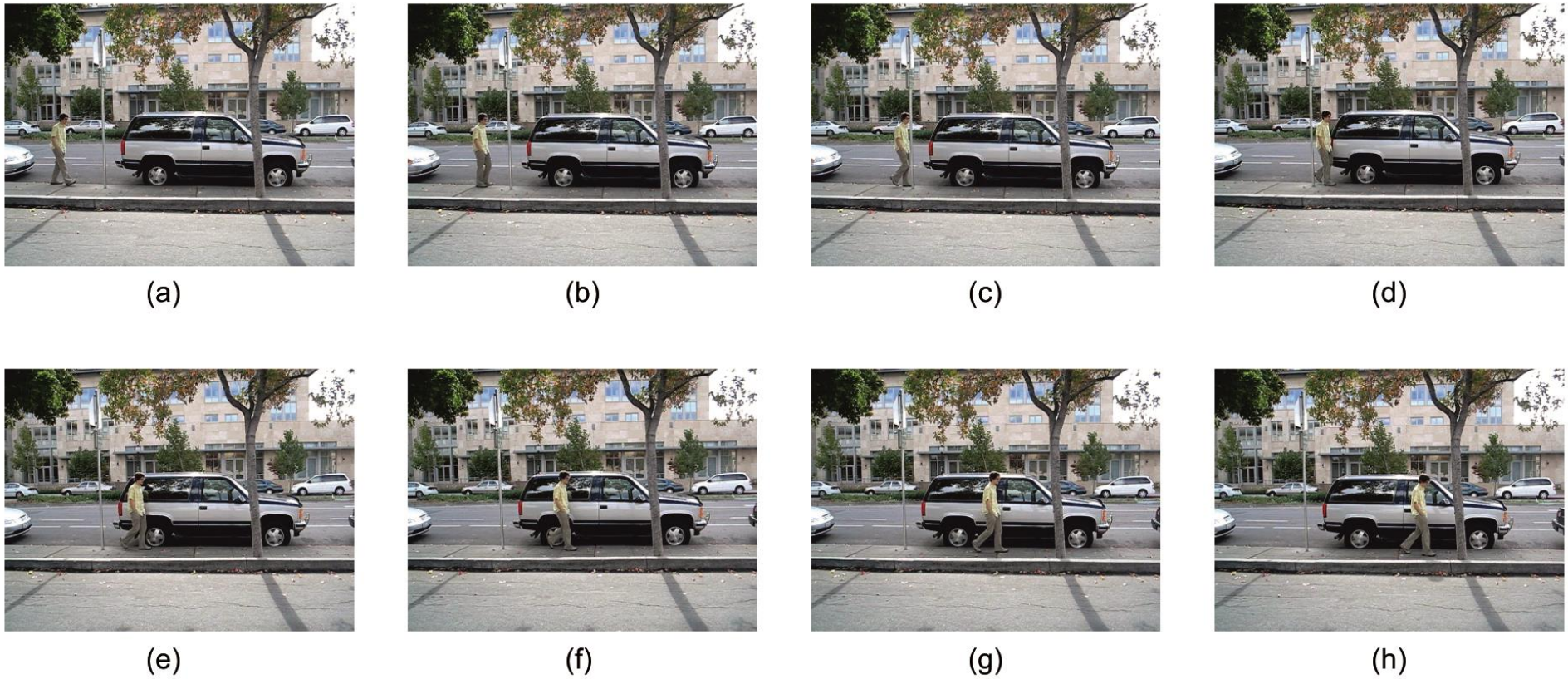


Fig. 5. Test color video sequence

*Retrieval Number F8113088619/2019©BEIESP*
*DOI: 10.35940/ijeat.F8113.088619*
*Journal Website: www.ijeat.org*

*Published By:*
*Blue Eyes Intelligence Engineering*
*& Sciences Publication*

Table 1 provides the results attained by the proposed method under various levels of S with respect to PSNR and SSIM. From the table, it is apparent that the DCT-VWT produces a maximum PSNR ranges between 41.28 to 45.89 under grayscale video sequences. The different grayscale watermarked video sequence and the corresponding extracted at S=5 are placed in Fig. 6. From the values, it is clear that the high objective quality interms of PSNR and high subjective quality interms of SSIM is attained by the proposed method is shown in Fig. 6. The DCT-VWT model. It is observed that the maximum performance is attained with the decreasing S values. From this Fig. 6, it is apparent that the proposed method achieved a better reconstructed video quality from the hosting video sequence with the maximum PSNR and SSIM values. For instance, while extracting the secret number plate video sequence from the Mandrill video sequence, a maximum of 45.89 PSNR and 0.9934 SSIM is achieved. Similarly, for the applied hosting Lena video sequence and secret medical video sequence, a maximum PSNR value of 46.78 and SSIM of 0.9978 is obtained. In the same way, for the applied video sequence, the proposed method attains better extraction.

**Table 1** Quality assessment for grayscale video sequence at s=5,10,15,20

| Video frame | S=5 | | S=10 | | S=15 | | S=20 | |
|---|---|---|---|---|---|---|---|---|
| | **PSNR (dB)** | **SSIM** | **PSNR (dB)** | **SSIM** | **PSNR (dB)** | **SSIM** | **PSNR (dB)** | **SSIM** |
| **4.2.03** | 45.89 | 0.9934 | 43.98 | 0.9854 | 42.47 | 0.9733 | 41.28 | 0.9584 |
| **4.2.04** | 46.78 | 0.9978 | 42.91 | 0.9843 | 40.32 | 0.9648 | 39.65 | 0.9542 |
| **4.2.07** | 43.13 | 0.9916 | 41.90 | 0.9732 | 40.93 | 0.9721 | 39.27 | 0.9632 |
| **5.1.12** | 45.90 | 0.9932 | 40.82 | 0.9907 | 39.98 | 0.9873 | 37.47 | 0.9736 |
| **5.1.14** | 46.32 | 0.9989 | 41.23 | 0.9754 | 40.21 | 0.9654 | 36.29 | 0.9549 |
| **5.2.08** | 44.91 | 0.9935 | 42.93 | 0.9841 | 41.45 | 0.9644 | 40.30 | 0.9437 |
| **5.3.01** | 45.88 | 0.9982 | 42.80 | 0.9742 | 40.27 | 0.9643 | 39.24 | 0.9512 |
| **boat.512** | 51.78 | 0.9993 | 46.77 | 0.9892 | 43.29 | 0.9721 | 41.83 | 0.9641 |

**Table 2** Quality assessment for color video sequence at s=5,10,15,20

| Video Frame | S=5 | | S=10 | | S=15 | | S=20 | |
|---|---|---|---|---|---|---|---|---|
| | **PSNR (dB)** | **SSIM** | **PSNR (dB)** | **SSIM** | **PSNR (dB)** | **SSIM** | **PSNR (dB)** | **SSIM** |
| 0001 | 47.89 | 0.9945 | 46.20 | 0.9873 | 44.92 | 0.9632 | 43.20 | 0.9573 |
| 0011 | 48.57 | 0.9967 | 47.29 | 0.9746 | 45.31 | 0.9532 | 44.43 | 0.9423 |
| 0021 | 48.32 | 0.9989 | 46.30 | 0.9832 | 46.12 | 0.9467 | 45.21 | 0.9321 |
| 0031 | 49.30 | 0.9934 | 47.23 | 0.9633 | 45.38 | 0.9521 | 44.19 | 0.9469 |
| 0041 | 53.29 | 0.9923 | 48.40 | 0.9792 | 46.22 | 0.9601 | 45.38 | 0.9532 |
| 0051 | 51.20 | 0.9957 | 48.37 | 0.9856 | 47.27 | 0.9683 | 46.83 | 0.9590 |
| 0061 | 49.09 | 0.9989 | 47.21 | 0.9809 | 45.38 | 0.9736 | 44.29 | 0.9639 |
| 0071 | 48.36 | 0.9921 | 47.34 | 0.9750 | 45.28 | 0.9643 | 44.24 | 0.9468 |


**Fig. 6. Quality assessment for gray scale video sequence**

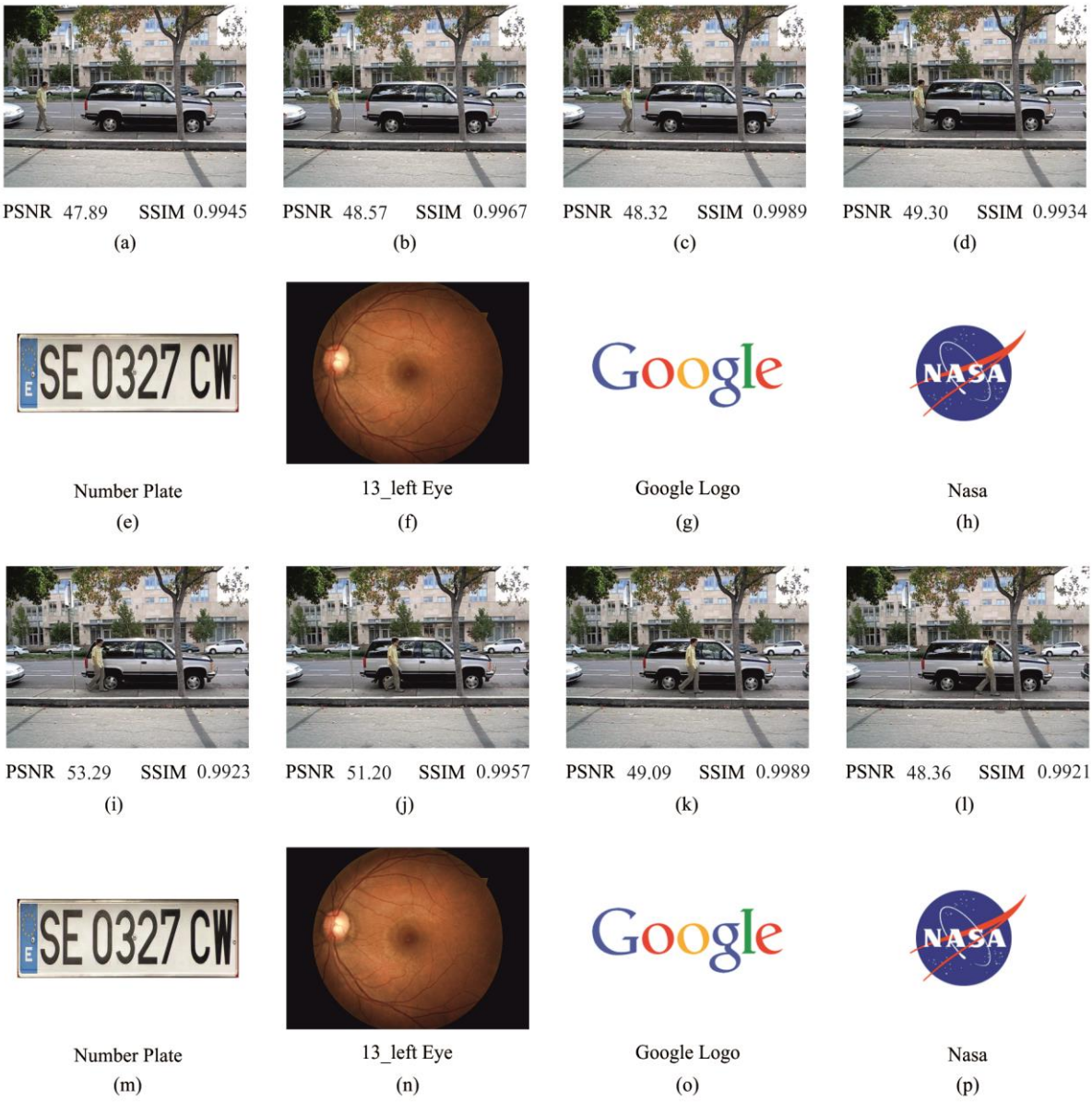


**Fig. 7. Quality assessment for color video sequence**

A comparison of the proposed DCT-VWT is made with varying strength value S. From the table, it can be seen that the proposed method attains a maximum PSNR value and SSIM value under minimum value of S. Fig. 7 illustrates diverse watermarked video sequences and the respective extraction under S=5. These values indicate that the proposed model shows effective results while extracting the hidden video sequence from the hosting video sequence. From the figure, it is clearly shown that the maximum values of PSNR and SSIM are achieved on all the applied video sequences. For instance, while extracting the secret number plate video sequence from the vehicle video sequence, a maximum of 47.89 PSNR and 0.9945 SSIM is obtained. Likewise, for the applied hosting vehicle video sequence and secret medical video sequence, a maximum PSNR value of 48.57 and SSIM of 0.9967 is obtained. In continue with, it shows superior performance on all the applied video sequences. In the same way, for the applied video sequences, the proposed method attains better extraction.

A comparative study of different methods on the grayscale video sequence is shown in Fig. 8 interms of PSNR. From this figure, it is exhibited that a maximum PSNR values are attained by the varying S values of the proposed method. In addition, it is also noted that the presented method shows better results with a higher PSNR values of 45.89, 43.98, 42.47 and 41.28 for different values of S (S=5, 10, 15 and 20). At the same time, the existing methods manage to perform well with the minimum PSNR value of 38.56. These values confirm that the DCT-VWT has better results over the compared methods. Fig. 9 shows the comparative analysis of diverse methods on the applied color video sequence. Figure depicts that the maximum results of the proposed DCT-VWT under different values of S. Moreover, it is noted that the presented method shows better results with a higher PSNR values of 47.89, 46.2, 44.91 and 43.2 for different values of S (S=5, 10, 15 and 20). At the same time, the existing methods manage to perform well with the minimum PSNR value of 40.17. These values confirm that the DCT-VWT has better results over the compared methods.

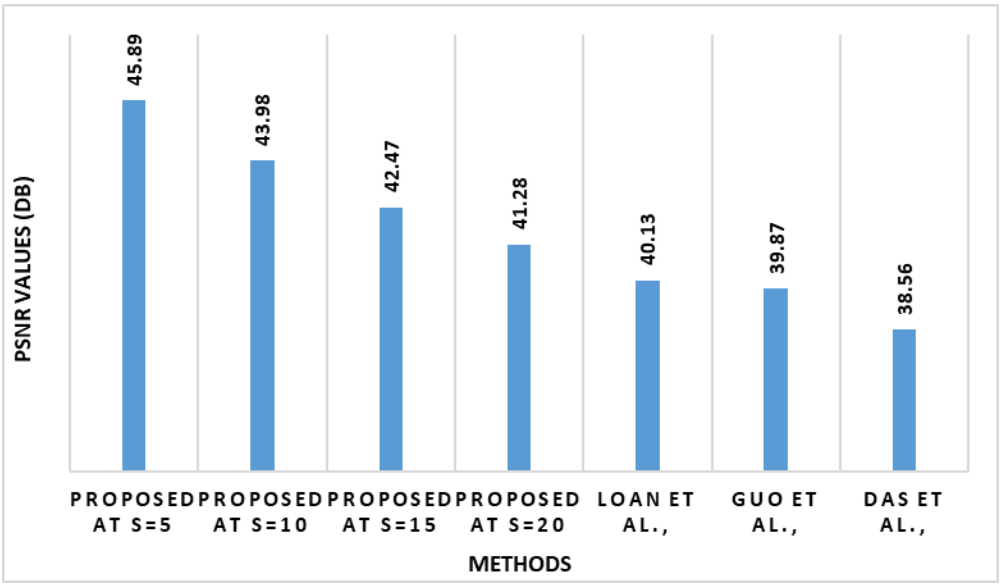


**Fig. 8. Grayscale Images**

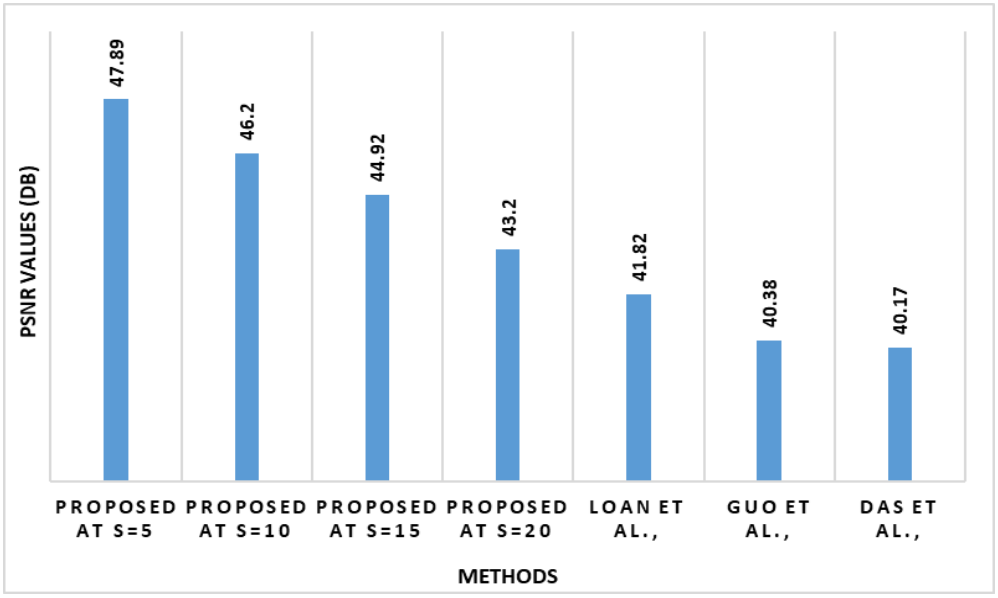


**Fig. 9. Color Images**

## IV. CONCLUSION

Security is a main concern in the digital video watermarking methods. Discrete Wavelet Transform (DWT) and Discrete Cosine transform (DCT) are most commonly used transforms for the coefficient domain watermarking approaches. In this paper, we present an optimum watermarking method which manages different challenges such as payload, security, invisibility, robustness, and so on. In this paper, we have presented a DCT based video watermarking technique named as DCT-VWT for both color as well as grayscale images. Chaotic encryption and Arnold transform are also used to increase the security level. The presented model is validated on the benchmark video sequences and a comparative results investigation is made. The outcome of the experiments clearly verified the superiority of the DCT-VWT over existing methods. In future, the performance of the DCT-VWT is enhanced by the application of DWT instead of DCT.

## REFERENCES

1. H. Tao, L. Chongmin, J. M, Zain, and A. N. Abdalla, ‘‘Robust image watermarking theories and techniques: A review,’’ J. Appl. Res. Technol., vol. 12, no. 1, pp. 122–138, Feb. 2014.
2. S. Voloshynovskiy, S. Pereira, T. Pun, J. J. Eggers, and J. K. Su, ‘‘Attacks on digital watermarks: Classification, estimation based attacks, and benchmarks,’’ IEEE Commun. Mag., vol. 39, no. 8, pp. 118–126, Aug. 2001.
3. H. Nyeem, W. Boles, and C. Boyd, ‘‘Digital image watermarking: Its formal model, fundamental properties and possible attacks,’’ EURASIP J. Adv. Signal Process., vol. 2014, p. 135, Dec. 2014.
4. N. Zivic, ‘‘Watermarking for Image Authentication,’’ in Robust Image Authentication Presence Noise, 1st ed. Cham, Switzerland: Springer, 2015, pp. 43–47. [Online]. Available: http://www.springer.com/in/book/9783319131559

5. S. A. Parah, F. Ahad, J. A. Sheikh, and G. M. Bhat, ''Hiding clinical information in medical images: A new high capacity and reversible data hiding technique,'' J. Biomed. Inf., vol. 66, pp. 214–230, Feb. 2017, doi: http://doi.org/10.1016/j.jbi.2017.01.006.
6. S. A. Parah, F. Ahad, J. A. Sheikh, and G. M. Bhat, ''A new reversible and high capacity data hiding technique for E-healthcare applications,'' Multimed Tools Appl., vol. 76, no. 3, pp. 3943–3975, Feb. 2017.
7. S. A. Parah, J. A. Sheikh, J. A. Akhoon, N. A. Loan, and G. M. Bhat, ''Information hiding in edges: A high capacity information hiding technique using hybrid edge detection,'' Multimed Tools Appl., vol. 77, no. 1, pp. 185–207, 2018, doi: 10.1007/s11042-016-4253-x.
8. S. A. Parah, F. Ahad, J. A. Sheikh, N. A. Loan, and G. M. Bhat, ''Information hiding in medical images: A robust medical image watermarking system for E-healthcare,'' Multimed Tools Appl., vol. 76, no. 8, pp. 10599–10633, Apr. 2017.
9. R. Eswaraiah and E. S. Reddy, ''Robust medical image watermarking technique for accurate detection of tampers inside region of interest and recovering original region of interest,'' IET Image Process., vol. 9, no. 8, pp. 615–625, 2015.
10. M. Benyoussef, S. Mabtoul, M. E. Marraki, and D. Aboutajdine, ''Robust ROI watermarking scheme based on visual cryptography: Application on mammograms,'' J. Inf. Process. Syst., vol. 11, no. 4, pp. 495–508, Dec. 2015.
11. L. Gao, T. Gao, G. Sheng, and S. Zhang, ''Robust medical image watermarking scheme with rotation correction,'' in Intelligent Data analysis and its Applications. Cham, Switzerland: Springer, 2015, pp. 283–292
12. K. Muhammad, J. Ahmad, S. Rho, and S. W. Baik, ''Image steganography for authenticity of visual contents in social networks,'' Multimedia Tools Appl., vol. 76, no. 18, pp. 18985–19004, 2017. [Online]. Available: https://doi.org/10.1007/s11042-017-4420-8
13. A. Kanso and M. Ghebleh, ''An efficient and robust image encryption scheme for medical applications,'' Commun. Nonlinear Sci. Numer. Simulat., vol. 24, nos. 1–3, pp. 98–116, Jul. 2015.
14. K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, and S. W. Baik, ''A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image,'' Multimedia Tools Appl., vol. 75, no. 22, pp. 14867–14893, 2016
15. M. M. Abd-Eldayem, ''A proposed security technique based on watermarking and encryption for digital imaging and communications in medicine,'' Egyptian Informat. J., vol. 14, no. 1, pp. 1–13, Mar. 2013.
16. J. B. Lima, F. Madeiro, and F. J. R. Sales, ''Encryption of medical images based on the cosine number transform,'' Signal Process., Image Commun., vol. 35, pp. 1–8, Jul. 2015.
17. B. Li, J. He, J. Huang, and Y. Q. Shi, ''A survey on image steganography and steganalysis,'' J. Inf. Hiding Multimedia Signal Process., vol. 2, no. 2, pp. 142–172, 2011.
18. W. Luo, F. Huang, and J. Huang, ''Edge adaptive image steganography based on LSB matching revisited,'' IEEE Trans. Inf. Forensics Security, vol. 5, no. 2, pp. 201–214, Jun. 2010
19. K. Muhammad, J. Ahmad, N. U. Rehman, Z. Jan, and M. Sajjad, ''CISSKA-LSB: Color image steganography using stego key-directed adaptive LSB substitution method,'' Multimedia Tools Appl., vol. 76, no. 6, pp. 8597–8626, 2017.
20. K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, and S. W. Baik, ''Image steganography using uncorrelated color space and its application for security of visual contents in online social networks,'' Future Generat. Comput. Syst., vol. 2, Nov. 2016. [Online]. Available: https://doi.org/10.1016/j.future.2016.11.029
21. S. Das and M. K. Kundu, ''Effective management of medical information through ROI-lossless fragile image watermarking technique,'' Comput. Methods Programs Biomed., vol. 111, no. 3, pp. 662–675, 2013.
22. D. Bouslimi, G. Coatrieux, M. Cozic, and C. Roux, ''A joint encryption/watermarking system for verifying the reliability of medical images,'' IEEE Trans. Inf. Technol. Biomed., vol. 16, no. 5, pp. 891–899, Sep. 2012.
23. I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography, 2nd ed. San Francisco, CA, USA: Morgan Kaufmann, 2007.
24. C. I. Podilchuk and E. J. Delp, ''Digital watermarking: Algorithms and applications,'' IEEE Signal Process. Mag., vol. 18, no. 4, pp. 33–46, Jul. 2001
25. S. A. Parah, J. A. Sheikh, and G. M. Bhat, ''On the realization of a secure, high capacity data embedding technique using joint top-down and downtop embedding approach,'' Comput. Sci. Eng., vol. 49, pp. 10141–10146, Aug. 2012
26. C. C. Chang, P. Y. Lin, and J. S. Yeh, ''Preserving robustness and removability for digital watermarks using subsampling and difference correlation,'' Inf. Sci., vol. 179, no. 13, pp. 2283–2293, Jun. 2009.
27. S. Bravo-Solorio and A. K. Nandi, ''Secure fragile watermarking method for image authentication with improved tampering localisation and selfrecovery capabilities,'' Signal Process., vol. 91, no. 4, pp. 728–739, Apr. 2011.
28. X. Wu, ''Reversible semi-fragile watermarking based on histogram shifting of integer wavelet coefficients,'' in Proc. DEST, Cairns, Australia, 2007, pp. 501–505
29. Z. Ni, Y. Q. Shi, N. Ansari, W. Su, Q. Sun, and X. Lin, ''Robust lossless image data hiding designed for semi-fragile image authentication,'' IEEE Trans. Circuits Syst. Video Technol., vol. 18, no. 4, pp. 497–509, Apr. 2008.
30. C.-C. Lai and C.-C. Tsai, ''Digital image watermarking using discrete wavelet transform and singular value decomposition,'' IEEE Trans. Instrum. Meas., vol. 59, no. 11, pp. 3060–3063, Nov. 2010.
31. C. I. Podilchuk and W. Zeng, ''Image-adaptive watermarking using visual models,'' IEEE J. Sel. Areas Commun., vol. 16, no. 4, pp. 525–539, May 1998.
32. A. Benoraira, K. B. Mahammed, and N. Boucenna, ''Blind image watermarking technique based on differential embedding in DWT and DCT domains,'' EURASIP J. Adv. Signal Process., p. 55, Dec. 2015, doi: 10.1186/s13634-015-0239-5.
33. N. Mohananthini and G. Yamuna, ''Comparison of multiple watermarking techniques using genetic algorithms,'' J. Electr. Syst. Inf. Technol., vol. 3, no. 1, pp. 68–80, May 2016.
34. Th. Rupachandra Singh, Kh. Manglem Singh, Sudipta Roy, "Video watermarking scheme based on visual cryptography and scene change detection," Int. . Electron. Commun. (AEU) 67, pp. 645-651, 2013.
35. Osama S. Faragallah, , "Efficient video watermarking based on singular value decomposition in the discrete wavelet transform domain," Int. . Electron. Commun. (AEU) 67, pp. 189-196, 2013.
36. Liu Y, Zhao J., "A new video watermarking algorithm based on 1D DFT and Radon transform," Signal Process (Elsevier), 90:626-39, 2010.
37. M. Masoumi, S. Amiri, "A blind scene-based watermarking for video copyright protection," Int. . Electron. Commun. (AEU) 67, pp. 528-535, 2013.
38. Mohamed, M.A., Aboutaleb, M., Abdel-Fattah, M.G. and Samrah, A.S., 2015. Hybrid watermarking scheme for copyright protection using chaotic maps cryptography. *International Journal of Computer Applications*, *126*(4).
39. Loan, N.A., Hurrah, N.N., Parah, S.A., Lee, J.W., Sheikh, J.A. and Bhat, G.M., 2018. Secure and robust digital image watermarking using coefficient differencing and chaotic encryption. *IEEE Access*, *6*, pp.19876-19897.