



Secure video communication using firefly optimization and visual cryptography

Manoj Kumar¹ · Jyoti Aggarwal² · Anuj Rani³ · Thompson Stephan⁴ · Achyut Shankar⁵ · Seyedali Mirjalili^{6,7}

Published online: 4 October 2021

© The Author(s), under exclusive licence to Springer Nature B.V. 2021

Abstract

In recent years, we face an increasing interest in protecting multimedia data and copyrights due to the high exchange of information. Attackers are trying to get confidential information from various sources, which brings the importance of securing the data. Many researchers implemented techniques to hide secret information to maintain the integrity and privacy of data. In order to protect confidential data, histogram-based reversible data hiding with other cryptographic algorithms are widely used. Therefore, in the proposed work, a robust method for securing digital video is suggested. We implemented histogram bit shifting based reversible data hiding by embedding the encrypted watermark in featured video frames. Histogram bit shifting is used for hiding highly secured watermarks so that security for the watermark symbol is also being achieved. The novelty of the work is that only based on the quality threshold a few unique frames are selected, which holds the encrypted watermark symbol. The optimal value for this threshold is obtained using the Firefly Algorithm. The proposed method is capable of hiding high-capacity data in the video signal. The experimental result shows the higher capacity and video quality compared to other reversible data hiding techniques. The recovered watermark provides better identity identification against various attacks. A high value of PSNR and a low value of BER and MSE is reported from the results.

Keywords Video watermarking · RDH · Visual cryptography · Firefly algorithm · Privacy preserving · Optimization · Meta-heuristics Algorithm

1 Introduction

With the development of the Internet, an enormous amount of data is transmitted every day in various forms. The reckless growth and sharing of online video content bring copyright violation detection, video search, and retrieval problems. However, with the availability and use of powerful multimedia tools, the data can be easily accessed, modified, and redistributed on the Internet. This fast evolution of the digitalization of data poses new

✉ Seyedali Mirjalili
ali.mirjalili@gmail.com

Extended author information available on the last page of the article

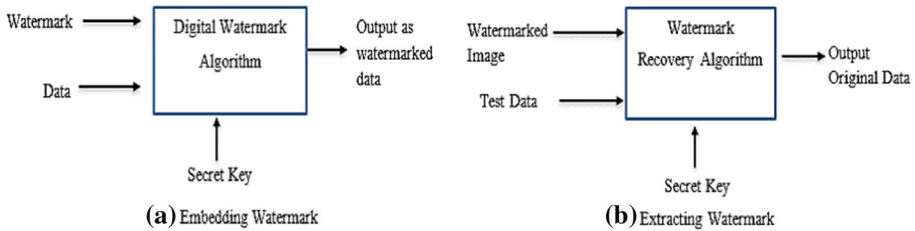


Fig. 1 A generalized approach of watermarking

challenges for managing and securing information. Therefore, the protection of digital data is highly required in the current digital society. Data hiding techniques hide some secret data into the cover medium without being detected. This is a method that can be considered to protect information. There exist various data hiding methods includes steganography, digital watermarking and so on (Jia et al. 2019).

Further, watermarking scheme can be classified based on watermark extraction ability and fragility and sensitivity of watermark. According to watermark extraction ability there are three watermarking schemes: blind, semi-blind and non-blind. In non-blind watermarking scheme, information of original host is required. Non-blind watermarking is practically limited because it requires extra storage to maintain the source image (Chang et al. 2007). In semi-blind scheme, some information of host and watermark is required but in blind watermarking scheme both host and watermarking information are not required. In blind watermarking, watermark information is extracted without prior knowledge of original information (Thakur et al. 2019; Thanki et al. 2019). As per the fragility and sensitivity of watermark, two types of watermarking scheme are there named as fragile and semi-fragile watermarking. Fragile watermarking is a verified solution to standard digital signature scheme, and it is used to verify the integrity of data to detect every possible change in image like adding or removal of any feature in image. In contrast, semi-fragile watermarking is used for minor data modifications like image compression and enhancement (Lu and Guo 2017).

Problems with identity protection are addressed using watermarking approaches. The main objective of these approaches is to meet properties such as robustness of watermark against various attacks, imperceptibility, security, and blindness w.r.t requirement of original data. To reveal the identity, the extraction of the watermarked symbol should be unambiguous to justify the authenticity of proprietary data (Kumar et al. 2016). A general approach of watermarking consists of two phases: embedding and an extraction procedure shown in Fig. 1. During the embedding phase, a processed watermark symbol or share or copyright information is embedded in the primary signal, which is limited to the owner. In addition, a reverse embedding procedure is performed to extract that copyright information so that the authenticity of data can be recognized (Katzenbeisser and Petitcolas 2000). Further, we suggested an entirely invisible watermarking instead of visible watermarking where no watermark symbol can be seen over hosted videos. In advance, most of the data hiding approaches can extract the watermark (embedded data) but at the same time will damage the covered signal. To overcome such an issue, the proposed work suggested a reversible data embedding approach capable of extracting additional information with image reconstruction without any distortion. Reversible data hiding can be performed by using two means, i.e., encrypted domain and plaintext domain. In this work, the host signal (video) is considered plain text while the embedded data (image) is encrypted. Reversible

data hiding with a visual secret sharing Scheme is implemented with firefly-based threshold optimization so that unique and best frames from a video can be considered to embed encrypted watermark share.

The rest of the paper is classified into five sections. Section 2 discusses the related watermarking techniques followed by the proposed method in Sect. 3. Section 4 discusses experimental results concerning the robustness of the proposed technique against various attacks and a comparison with other state-of-art techniques. Finally, the conclusions with future directions are provided in the last section of this paper.

2 Literature survey

Digital watermarking for identity privacy is a dynamic domain for research. In general, the watermark symbol is inserted either by directly modifying the host signal or modifying the transform domain's coefficients. There exist various methods for performing watermarking on images as well as on digital videos. In this section, we analyzed and presented recent works implemented in this area.

A novel approach was proposed for plane slicing based watermarking algorithm to embed colored watermark images on the color video using hybrid transforms like Contourlet Transform (CT), Discrete Wavelet Transform (DWT), and Singular Value Decomposition (SVD) (Agilandeewari and Ganesan 2016). As a result, a high level of robustness, good fidelity, and high value of PSNR are achieved. Eigenvector is also calculated at the receiver's end to check the authentication of the watermarked image. Two new watermarking approaches (VW16E and VW8F) were given for achieving a high degree of imperceptibility and temper detection. These approaches were compared with the other approaches for a range of video samples, and the result shows that the proposed approaches provide better detection capabilities and imperceptibility (Arab et al. 2016). Karmakar et al. (2016) proposed a DCT based rotation attack resistant video watermarking scheme. The algorithm was also implemented in MATLAB, and results were calculated for three different standard videos, which indicates that their method is vigorous against any rotation and video attacks. Asikuzzamanave et al. (2016) proposed a digital watermarking method for depth-image-based 3D videos that can extract the watermark from the left, right, and center of the videos. Experiment shows that the proposed approach was also effective against additive noise, baseline distance adjustment, and compression. Another non-blind color video watermarking scheme was proposed by Rasti et al. (2016). Their algorithm was checked against several signal processing attacks and compared with existing methods, and it was identified that the proposed algorithm is the robust method on public image data sets. Himeur and Boukabou (2018a) have designed a new watermarking system for uncompressed video sequences where DWT and SVD were used for low visual distortion. This approach had remarkable results against scaling, blurring, cropping, filtering, and H.264 compression. Zhao and Li (2018) proposed a three-dimensional histogram shifting for reversible data hiding, which can hide data into any image or video file. The demonstrated result shows that the embedding efficiency of the proposed scheme was much higher than the existing schemes. Wang et al. (2018) suggested a high-efficiency video coding-based watermarking scheme to embed the watermark in the quantized coefficients of the video files to remove the cumulative errors. The results were obtained for different values of quantization parameters, and it was observed that the proposed algorithm gave good results even when the quantization parameter values were greater than 40.

A two-tier RDH-ED framework was proposed by Shah et al. (2018). It is proposed for 3D mesh models based on Homomorphic Paillier Cryptosystem. The proposed approach can produce better results with high embedding data capacity. Kulkarni and Kulkarni (2018) have given a video cryptography-based greyscale image watermarking scheme for two shares of the images and find out the results for three greyscale images. The proposed approach was satisfying the security, robustness, and blindness properties. Xu et al. (2018) implemented an efficient method for reversible data hiding in encrypted images based on 2-dimensional histogram modification. The proposed approach can be used in applications where high image quality and reversibility is required, like in cloud computing. Further, Bhardwaj et al. (2018) proposed a robust video watermarking approach base on coefficient difference using the frame selection method. The results were compared with existing approaches on different videos, and improvements are achieved in terms of robustness, but imperceptibility was compromised. An adaptive reversible data hiding method was implemented by Chuan et al. (2018) for encrypted images. The proposed method is better in terms of rate-distortion performance. Rajkumar and Vasuki (2019) produced a method to improve the watermark embedding capacity and the perceptual quality for a reversible watermarking scheme. They used a Gaussian filter as the first step while embedding the watermark. The peak points of the histogram are chosen for data hiding. High-frequency modification is done at pixel level where they embedded watermark. A secret key is used for the security of data. Security of the images is improved in the proposed method. Li et al. (2019) applied histogram shifting approach for data hiding in the images. The histogram shift is used for hiding data in JPEG images. The data bits are embedded in the high-frequency coefficients, which are obtained by histogram distribution. The optimal DCT coefficient is considered to embed secret messages. This method produced better results than other approaches in terms of embedding rate and visual quality of the images.

Malik and Reddlapalli (2019) proposed a watermarking scheme by integrating the concept of histogram and entropy, which results in better imperceptibility and robustness. The experiment was performed on the three well-known greyscale images as well. Senthilnathan et al. (2019) given SBRE-RDH crypto security-based encryption algorithm. Initially, the host image is divided into blocks in their method, and entropy is estimated for hiding the watermark. Further, the histogram shape method is used to hide watermark information. Their results are better than other algorithms to recover the hidden data and images without any error for large amount of data. For these reasons, it can be used in a cloud environment as well. Tang et al. (2019) implemented a reversible data hiding approach based on differential compression. Huffman coding was used to diminishes the size of embedding location maps. The proposed algorithm performs well in terms of data hiding capacity and computational time, but it was not suitable for JPEG images. Nasrullah et al. (2019) used Kd-tree to propose a joint and separable RDH system to provide better data hiding in compression and encryption domain. The cover signal is compressed with lifting-based integer wavelet transform (IWT) and set partition in hierarchical tree (SPHIT) encoding. Further, multiple shift operations are carried out to generate SPIHT bit-stream. These streams are arranged into a binary square matrix and shown to Kd-tree with random transformations to hide the data. Noor et al. (2019) proposed a watermarking scheme, which works along with DTT, R-PCA, and SVD approaches. CAT mapping scrambling is used to scramble the watermark logo. The original data is decomposed into low-rank and sparse components using R-PCA. DTT is applied for transformation to embed watermark data using SVD. Their technique is tested against various type of attacks to check the robustness. Kumar and Jung (2020) proposed a robust and reversible data hiding approach based on 2-layer insertion of data with reduced capacity-distortion trade-off. They first performed decomposition

of the image into two planes that is a higher significant bit (HSB) and a least significant bit (LSB), respectively. Further, prediction error expansion is used to hide secret watermark bits in the HSB plane. The experimental result gives better outputs. This method is also tested against various attacks. Altay and Ulutas (2021) have proposed a robust Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) based technique for copyright protection. Fibonacci-Lucas Transform (FLT) was also applied to binary watermark for providing more security of the watermarking scheme. A high robustness level against attacks was achieved in this approach. Alotaibi (2020) has introduced a three-level watermarking scheme to optimize hidden neurons in a deep belief network framework to enhance prediction accuracy. Ayubi et al. (2021) have proposed a new two-dimensional secure video watermarking scheme. They have also introduced an efficient algorithm based on IWT, DWT and CT transform. The result shows that the proposed algorithm was providing better visual quality based on PSNR and SSIM. Dogan (2016) proposed a new data hiding technique based on a genetic algorithm where different chaotic maps were used to the randomness of genetic function. Results of the proposed method were compared, and it was observed that gauss, logistic, and tent maps were faster than random functions.

From the literature, it has been observed that video watermarking is fragile against various geometrical attacks. Most of the researchers worked with videos without suggesting powerful encryption strategies. Their capacity and techniques to hide content over video frames are uniform and embed watermark content on every frame. This brings a major disadvantage for such techniques because during the extraction procedure after performing attacks, data recovery is lossy. Most techniques work with binary images as a watermark, but we used various images of varying sizes. To fill these gaps, we proposed a novel framework with high data embedding capacity and robustness because of the suggested optimization technique. Also, the share of the encrypted watermark is embedded in specific frames based on threshold instead of embedding data on each frame of the host signal. The conversion of video frames is not implemented to maintain the quality of the host signal. The demonstrated results show the effectiveness of the proposed framework, as discussed in subsequent sections.

3 Methodology

The proposed methodology is divided into four sub-sections, and watermarking workflow is shown in Fig. 2. In the first sub-section, video frames are extracted based on a threshold estimated using the Firefly algorithm. Then, the watermark is processed using visual cryptography. The third part performs data embedding into video frames using a reversible data hiding procedure. The watermark extraction after performing various attacks is performed in the fourth part of the proposed methodology. The subsequent section discusses the working of the proposed method.

The concept of reversible data hiding is used in this work. It can be classified into irreversible and reversible data hiding (RDH) techniques (Hou et al. 2021). RDH is used to completely recover the original data after correctly extracting the hidden data. The main motive of RDH to implement in this work is to achieve a higher embedding rate with less distortion. There are two different domains of RDH, i.e., spatial and encrypted. In spatial RDH algorithms focus is given on achieving the data embedding by exploiting the spatial correlation among pixels and their aim is to achieve visual quality as high as possible for a given embedding capacity. Even though there exist various techniques in RDH. One type

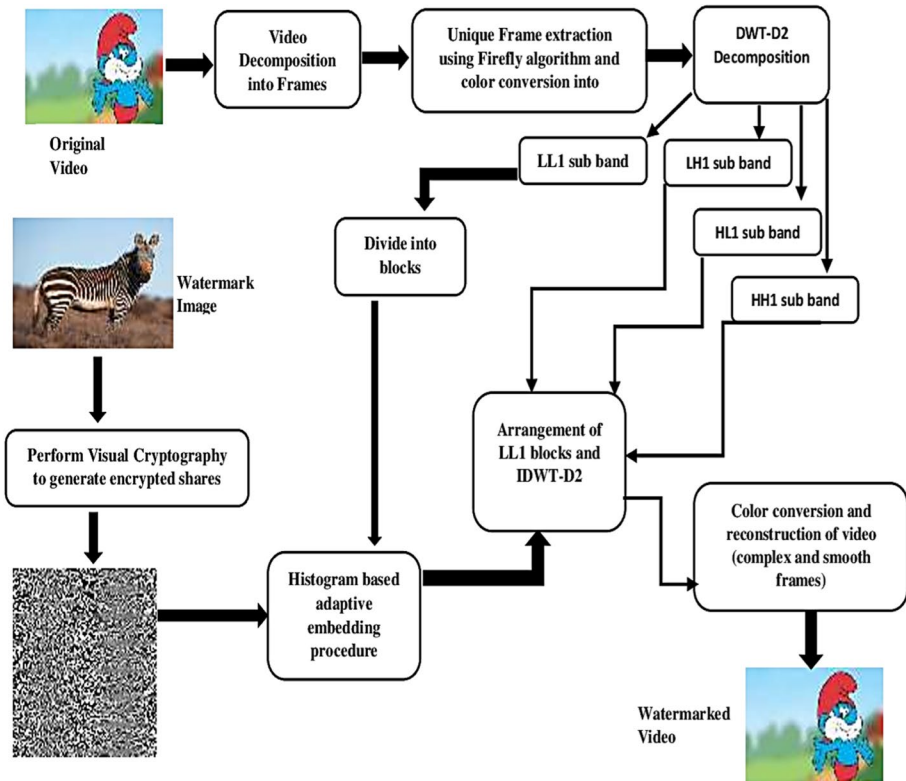


Fig. 2 Workflow of the suggested video watermarking system

of approach focuses on finding new embedding ways to deal with the prediction errors and reduce the embedding distortion, and other types of approaches focus on improving prediction accuracy (Weng et al. 2021). Here it is used to improve the watermark prediction accuracy after attempting various attacks.

3.1 Extraction and processing video frames for data embedding

The robustness and practicality of watermarking approach depend on the embedding and extraction processes. The first part of the proposed method is to extract complex frames from an input video. The video is divided into various frames, and further, frame complexity is estimated on processed frames. This frame complexity is further compared to the estimated threshold value computed by the Firefly algorithm. If the complexity of a particular frame is greater than the threshold is taken as a complex frame; else, the frame is ignored for hiding the watermark symbol. In the proposed algorithm, only complex frames are chosen to embed watermark rather than adding copyright information on every video frame.

The image frame complexity is measured using black and white border length. The more extended border is taken as a complex frame. The length of border (k_i) is estimated

by performing sum over the number of times there is a color change in all the rows and columns of the image. The frame complexity (\bar{c}) is estimated using Eq. 1.

$$\bar{c} = k/m \quad (1)$$

In the Eq. 1, k represents the total length of black and white border while m is estimated using (size of image \times number of bit planes). k_i is estimated for every block of extracted video frame.

3.1.1 Firefly algorithm (FA)

The Firefly algorithm was first proposed by Yang (2009) in 2009. The basic steps of this algorithm can be referred to from an initially proposed algorithm. Generally speaking, this algorithm is based on the swarm intelligence approach of the flashing behavior of fireflies. It assumes that the solution of an optimization problem can be considered fireflies whose brightness is proportional to the values of its objective function with provided problem space. These flies can produce lights, and that will help them to communicate and attract.

Optimization: The optimization problem depends on three factors: a function to optimize, a solution set to pick a value for the variable from, and an optimization rule (maximized or minimized). The optimization function of the algorithm is $f(x)$, where $x = (x_1, x_2, x_3, \dots, x_n)$. Three rules are followed in the proposed work.

- All the fireflies are unisexual and therefore can attract any firefly.
- Attractiveness is proportional to their brightness. The flies will attract to the highest intensity or brightness and this stay decreases with their distances increases.
- In case there exist no brighter firefly than a given one then it will move randomly.

For maximization problem, the intensity or brightness is proportional to the objective function value. For a specific location x , the intensity I of a firefly can be picked as $I(x) \propto f(x)$ for maximization where $Maxf(x)$ such that $x \in S \in R^n$. The solution for this is a member of set S which generates maximum value of objective function compare to all elements in set S . Another parameter which is attractiveness β is relative and arbitrated by former flies and therefore differ with distance d_{ij} between firefly i and j . Further, to understand the implemented FA algorithm in the proposed work, can also be referred from Mishra et al. (2014) with the difference in objective value for firefly. For the proposed work, it is defined as shown below:

$$objective = PSNR + \emptyset * [BER(w, w') + \sum_{i=1}^{At} BER(w, w'_i)]$$

Here w and w' are the original and extracted attacked watermark. At represents various attacks on the watermarked video frame and \emptyset is the additive weighting factor to balance the PSNR influence and chosen as per (Huang et al. 2010).

This is a stochastic method and cannot guarantee the best ideal solution in deterministic time but converges towards a rational time solution (Mustafa Bilgehan et al. 2017). In fact, this is a metaheuristic method and trade-off among randomization, and local search is measured by parameters. The firefly heuristic is based on the survival of the population, and randomized movement evades local optima. Moreover, the optimal solution continues until there are improvements in the objective function. To optimize a single objective

function effectively for better parameters estimation, we used the method. In addition, this algorithm is chosen to find a suitable threshold value based on extracted (populated) frames of a video based on parameters. Choosing a value is highly complex in scientific studies, and the use of this algorithm is uncomplicated and easy. This provides a better decision to choose a particular frame where a watermark symbol can be embedded compared to other optimization techniques. The outcome of the implemented algorithm gives a feasible set of video frames in which we are embedding data for further processing. The algorithm for estimating an optimized threshold value follows Algorithm 1.

Algorithm 1: Optimized threshold value estimation using Firefly algorithm

Objective Function: $f(x)$, where $x = (x_1, x_2, x_3, \dots, x_n)$
 Generate initial population x_i where $i = 1, 2, 3 \dots n$;
 Express light intensity I w.r.t relationship with $f(x)$
 Use interest coefficient as φ
 While ($n < MaxGeneration$) do
 for ($i = 1$ to n)do
 for ($j = 1$ to n) do
 if ($I_i > I_j$) then
 vary attractiveness with distance d by $\exp(-\varphi d)$
 move flies from i to j
 Estimate new solutions and update intensity
 Rank fireflies and find current best

This generates a best threshold value which is used further with \bar{c} for finding complex frames.

Further, the identified complex frames are transformed into wavelet domain (DWT) using 'Haar' wavelet algorithm. The *wavedec2* function with level = 1 is performed on the extracted frames. The implemented method derives horizontal, vertical and diagonal bands for a given frame. The LL sub-band are divided into blocks. Low frequency band is used to embed the encoded watermarked share because of its robustness against various attacks.

3.2 Processing of watermarked symbol using visual cryptography

A watermark image is taken in JPG format of different sizes and an RGB color map in the proposed method. Visual cryptography is performed to create a share from the input image. This converts the image in shares to create an encoded watermarked image (Failed 2013).

We perform visual cryptography based on (2,2) VC scheme where each pixel is in the relationship with two pixels. Using the proposed approach, two watermark shares $W1$ and $W2$ are generated. The user keeps one share as a key by using which the final watermarked video frame is generated while share two is embedded by performing merging operation using histogram-based bit shifting in complex frames obtained from step 3.1. The proposed process to generate an encrypted share is performed using the following steps.

1. Me of the watermarked image I' is obtained after performing conversion from RGB to gray. This is performing using $Mean = mean(Grayscale(I'))$.
2. A seed value is used and a random map is estimated. This is denoted by the value Seed-map.

$$Seedmap = Rand(Row, Col) \times Seed$$

3. Further, the grayscale image is changed to a binary level which is denoted as BW. This is performed using the function `im2bw` with a threshold value as 0.5. The yield image changes all pixels (black (0) and white (1)) grounded on threshold. The function to estimate BW is defined as $BW = im2bw(Grayscale(I), 0.5)$.
4. A novel binary level map is setup that is two times the size of the input image and is denoted by $BW1$. The rules shown in Table 1 is used to generate the shares.


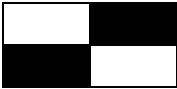

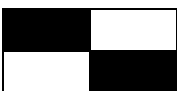
An image gained after this process is used as an encoded sereshare ESI .

In the proposed approach, during the embedding of data, bits underflow and overflow problem is controlled by modifying the pixel values. The pixel with values 0 and 255 represents the underflow and overflow values, respectively. Under this scenario, the pixel value with 0 is changed to 1 and value of 255 is changed to 254, and 1 is stored in the estimated array l . Other modified pixels (0 or 255) during embedding data are stored as 1 in the same array. This is implemented to minimize data loss.

3.3 Data embedding procedure using histogram bit shifting

After performing the watermark image encryption, we hide encrypted bits in the host video in this procedure. To achieve the reversibility, the idea of histogram shifting is used. This process is divided into two steps namely, histogram generation and modification by adding encrypted share using histogram shifting. This is performed as per steps 3 and 4 of the embedding algorithms. The confidential data hiding in complex video

Table 1 Rules to generate the visual cryptographic shares

Rule	Mean	BW	Block
1	$I(Row, Col) < Mean$	$BW(Row, Col) = 0$	
2	$I(Row, Col) < Mean$	$BW(Row, Col) = 1$	
3	$I(Row, Col) \geq Mean$	$BW(Row, Col) = 0$	
4	$I(Row, Col) \geq Mean$	$BW(Row, Col) = 1$	

frames is performed. Input video frame is named as *CVF* of size $M \times N$ and encrypted watermark share as *ESI*. The final output of this step is watermarked video frame *WVF*. Finally, these frames are combined with those frames which are not used for performing watermarking, i.e., complex watermarked frames are merged with smooth frames and finally, a watermarked video signal is generated. The whole process is well explained using below shown steps.

3.3.1 Embedding algorithm

1. The *CVF* is divided into blocks CVF_b of size $r \times c$. The number of blocks is estimated using Eq. 2.

$$n = M \times N / r \times c \tag{2}$$

2. For selected CVF_b , the absolute difference frame block of size $r \times (c - 1)$ is calculated using Eq. 3.

$$FAD_b = |CVF_b(i, j) - CVF_b(i, j + 1)| \text{ for } 0 \leq i, j \leq r - 1, c - 2, b \leq n \tag{3}$$

3. For all FAD_b , histogram is generated with maxima max_b and minima min_b w.r.t every block b . $min\ima = \min |max_b - min_b|$ and maxima consist of all positive and negative maxima.
4. In this step, the pixel values between max_b and min_b of *CVF* block are incremented and decremented w.r.t neighbor pixels as per histogram peaks. Under these conditions, the FAD_b can be expressed as Eq. 4 and 5 while the conditions for i, j and b remain same as Eq. 3.

$$FAD'_b(i, j) = \begin{cases} FAD_b(i, j) + 1 & \text{if } FAD_b(i, j) > max_b \\ FAD_b(i, j) & \text{otherwise} \end{cases} \tag{4}$$

$$FAD'_b(i, j) = \begin{cases} FAD_b(i, j) - 1 & \text{if } FAD_b(i, j) < min_b \\ FAD_b(i, j) & \text{otherwise} \end{cases} \tag{5}$$

5. Here, secret bits of *ESI* is embedded in the shifted histogram image blocks FAD'_b by modifying max_b . The new frame is represented by FAD''_b and performed using Eq. 6.

$$FAD''_b = \begin{cases} FAD'_b(i, j) + m & \text{if } FAD'_b(i, j) = max_b \\ |FAD'_b(i, j)| + m1 & \text{if } FAD'_b(i, j) = -max_b \\ FAD'_b(i, j) & \text{otherwise} \end{cases} \tag{6}$$

$m1 \in \{0 \text{ to } 2^l \text{ and } l = \log_2(d')\}$ d' is the difference between negative and positive maxima of frame block.

6. The watermarked video frame *WVF* blocks are finally generated using *CVF* and FAD''_b . This is achieved using Eq. 7 and 8.

$$WVF_b(i, 0) = \begin{cases} CVF_b(i, 0) & \text{if } CVF_b(i, 0) < CVF_b(i, 1) \\ CVF_b(i, 1) + FAD_b''(i, 0) & \text{otherwise} \end{cases} \quad (7)$$

$$WVF_b(i, 0) = \begin{cases} CVF_b(i, 0) + FAD_b''(i, 0) & \text{if } CVF_b(i, 0) < CVF_b(i, 1) \\ CVF_b(i, 1) & \text{otherwise} \end{cases} \quad (8)$$

7. For remaining pixels in the watermarked video frame, the mapping of FAD_b'' is done with WVF_b as per neighbor pixel relationships.

3.4 Data extraction algorithm (reversible approach)

In this section, the encrypted image is extracted from the watermarked video WVF . After extracting that $BW1$ share of encrypted image is further composite with $BW2$ to restore the original watermark. The input to this algorithm is extracted unique watermarked video frames. The frames which are considered to recover the watermark image is complex frames, as these frames are chosen based on estimated threshold for watermarking. The following extraction procedure is performed to achieve the desired result. The Extraction process is shown in Fig. 3, where extraction of unique frames is carried out. Further, DWT is applied with reversible histogram-based method which gives one share of the watermark symbol. Then this symbol is merged with another share obtained implementing visual cryptography so that a final watermark can be generated. This is an invertible process w.r.t Sect. 3.3 algorithm working.

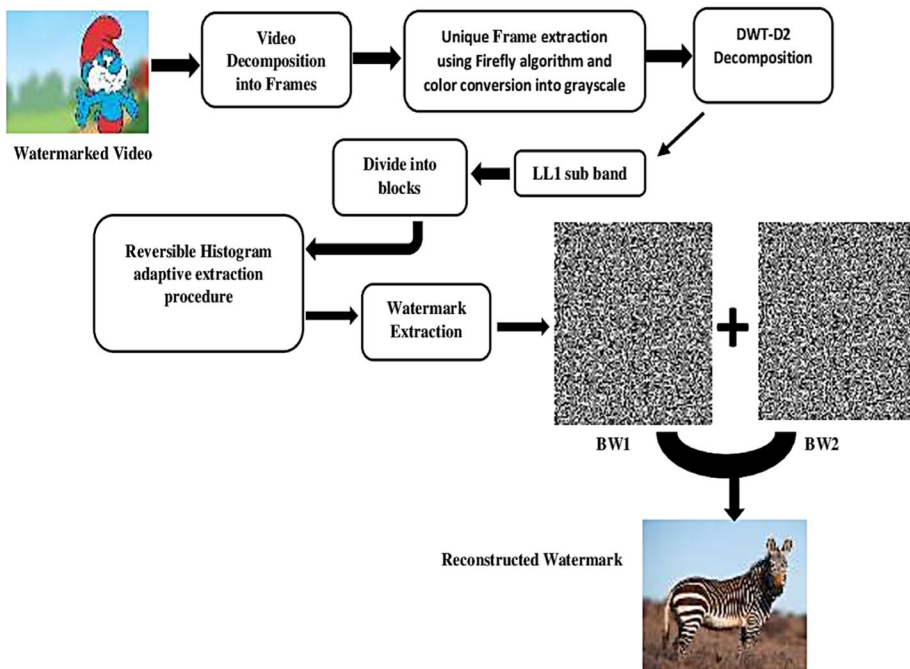


Fig. 3 Block diagram for watermark extraction procedure

3.4.1 Extraction algorithm

1. The watermarked video frames are divided into block as per step 1 of embedding algorithm.
2. The difference video frame block R_eFAD_b is estimated from watermarked frame by implementing Eq. 9 as per condition used in Eq. 3. The values of max_b and min_b are also estimated in this step.

$$R_eFAD_b(i, j) = |WVF_b(i, j) - WVF_b(i, j + 1)| \quad (9)$$

3. The R_eFAD_b is visited and embedded bits of encrypted share is extracted using Eq. 10.

$$m = \left\{ \begin{array}{ll} \text{Extracted as 0} & \text{if } R_eFAD_b(i, j) = max_b \\ \text{Extracted as 1} & \text{if } R_eFAD_b(i, j) = max_b + 1 \end{array} \right\} \quad (10)$$

Rest of the bits are also extracted in array l as did in step 5 of embedding procedure and converted into binary. Also, the positive maxima and negative minima is estimated.

4. Also, the reverse of FAD'_b is estimated in $R_eFAD'_b$ using Eq. 11.

$$R_eFAD'_b = \left\{ \begin{array}{ll} R_eFAD_b(i, j) - 1 & \text{if } R_eFAD_b(i, j) = max_b + 1 \\ R_eFAD_b(i, j) & \text{if } R_eFAD_b(i, j) = max_b \end{array} \right\} \quad (11)$$

The value of negative maxima is estimated if the bits of $R_eFAD_b(i, j)$ is from the range $-max_b$ to $-max_{b-1}$.

5. In this step, the WVF is obtained by using reverse shifting operations.

Finally, watermark symbol is extracted from attacked video frames.

4 Results

The evaluation of the suggested system is carried out in MATLAB R2019a as platform with intel i3 processor 8th Generation and 4 GB RAM. The experiment is performed using $\beta_0 = 1$, $\alpha = 0.01$ and light absorption coefficient $\gamma = 1.0$ with initial fireflies as 20. The value of \emptyset is 25. To compute the objective function the value of At is 11 in this work. And, based on the convergence of FA analysis, it is evident that FA converge to local position based on condition if $0 < \beta_0 < 1$. The algorithm converges to averaged position p of its attractive neighbor if the condition for β_0 is satisfied. The performance of the method is tested against different type of attacks.

To generate the experimental results, different types of images with erratic sizes and videos are used as shown in Table 2. The details of the images and video as dataset can be accessed from "<https://github.com/wssmanojkumar/Watermaking-Sample-dataset>" for testing purpose. Using this dataset, a total of 25 cases can be generated for evaluation purpose. The quality and robustness of the approach is estimated using performance parameters such as peak signal-to-noise-ratio (PSNR) and bit error rate (BER). PSNR objective is to evaluate the fidelity/ quality of the watermarked video and BER is used to test the robustness against various attacks. The value of PSNR is estimated using Eq. 12 while MSE and BER is calculated using Eqs. 13 and 14 respectively.

Table 2 Sample images and videos used for evaluating the proposed approach

Videos					
Images	 Case (1)	 Case (2)	 Case (3)	 Case (4)	 Case (5)

$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE} \quad (12)$$

The MSE in Eq. 12 is calculated using Eq. 13. Where O_{ij} is the original pixel value and M_{ij} is the marked pixel value.

$$MSE = \frac{1}{512 \times 512} \sum_{i=1}^{512} \sum_{j=1}^{512} (O_{ij} - M_{ij})^2 \quad (13)$$

$$BER(w, w') = \frac{\sum_{i=1}^N \sum_{j=1}^M w(i, j) \otimes w'(i, j)}{N \times M} \times 100\% \quad (14)$$

here w and w' are the original and extracted watermarks and N and M are the rows and columns of watermark images.









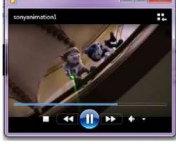

The videos used for watermarking are .wmv and images are .jpg and .png format. The quality is measured based on samp rate and frame rates. The used video is of 320×240 size with 30Fr/sec. Two channels are used to create the videos with an auto sample rate of 48.00 kHz. While images are of varying sizes ranging from 650×550 to 630×434 . For .png images bit depth is 32 while for .jpg it is 72dpi.

A total of 11 attacks are performed on the blind watermarked signal. For evaluating the technique, five types of cases are discussed in this section. Watermark image is embedded in all the videos and performance is estimated likewise. A sample result is given in Table 3.

From this table, it is evident that the suggested system is able to keep good imperceptibility as the values of PSNR are good after performing watermarking. The estimated mean error is also less for the watermarked video. A comparative estimation for input MSE and output MSE is shown in Fig. 4. From the figure, we can depict that the difference between the initial MSE for all the cases and the output MSE is significantly less. Test case 2 shows the minimum difference, which is 0.013, while the maximum is obtained in test case 3 which is 2.735.

The effectiveness of our approach under various attacks is shown in Fig. 5, in which BER is estimated for all used cases. It is evident from the results that even after performing various attacks on the watermarked video, there are negligible differences in original BER and estimated BER. The results show that the maximum distortion in bit

Table 3 Performance of projected technique with all cases as per Table 2 data

Cover Video	Image	Estimated Avg. PSNR	Estimated MSE
 Case (1)		56.346	29.190
 Case (2)		58.127	30.238
 Case (3)		61.638	23.982
 Case (4)		58.228	28.462
 Case (5)		54.376	31.235

error is under quantization attack (0.33) while minimum under frame blending (0.002). In the figure, x axis shows the performed attacks while y axis shows BER values. Further, the BER value differences with proposed visual cryptography and without visual cryptography is also shown in Fig. 6.

The results of Fig. 6 are obtained under different attacks on the encrypted or non-encrypted data. The simulation shows that by implementing a layer of visual encryption, we can further enhance the security and therefore results in less losses in the data in terms of BER. This shows that the proposed method also enhances the security parameter. In this approach, the bit error is less among watermarked and non-watermarked frames i.e., the number of errors is less with visual cryptography than that without visual cryptography. Therefore, the robustness of this method good because of visual cryptography.

A sample of executed GUI of the proposed approach is shown in Fig. 7. The figure shows video under an attack and extraction of the watermark from an image with BER.

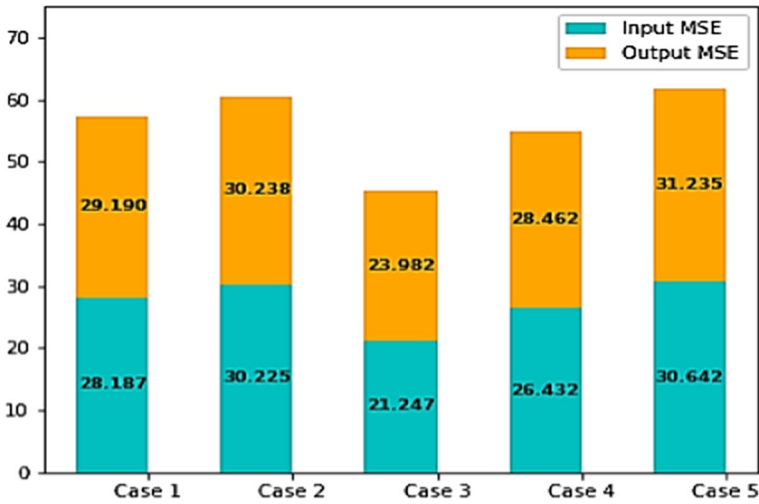


Fig. 4 A comparison between input MSE and estimated MSE

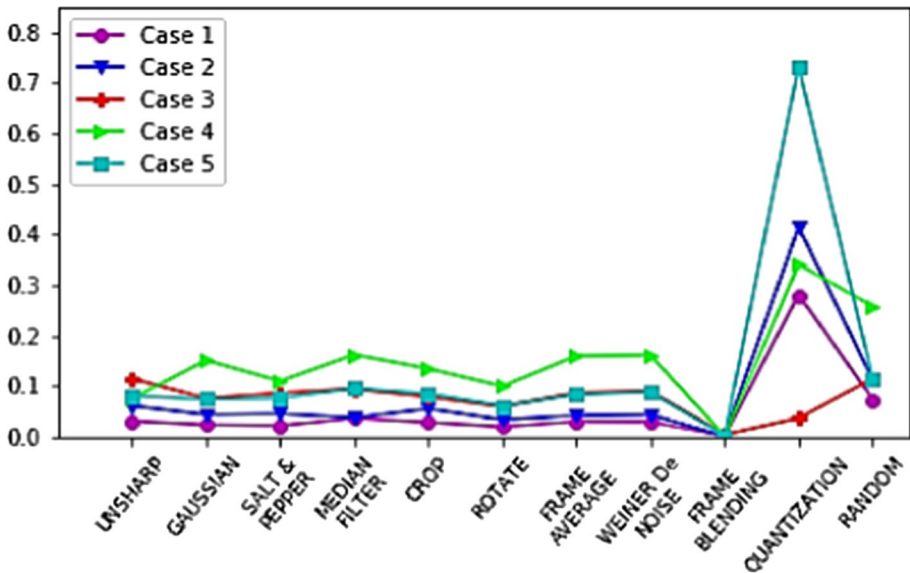


Fig. 5 BER estimation under various attacks

The GUI (a) of Fig. 7 is used to select various types of attacks on input video. Also, all the estimated parameters results are shown for these attacks. On the other side, GUI (b) showing the extracted watermark after all attacks with an estimated bit error rate.

These results are adequate to demonstrate that the implemented video watermarking system is robust against geometrical attacks and keeps high imperceptibility and payload capacity after embedding watermark image share. A comparison between various watermarking techniques under these two parameters are shown in Fig. 8. After embedding the

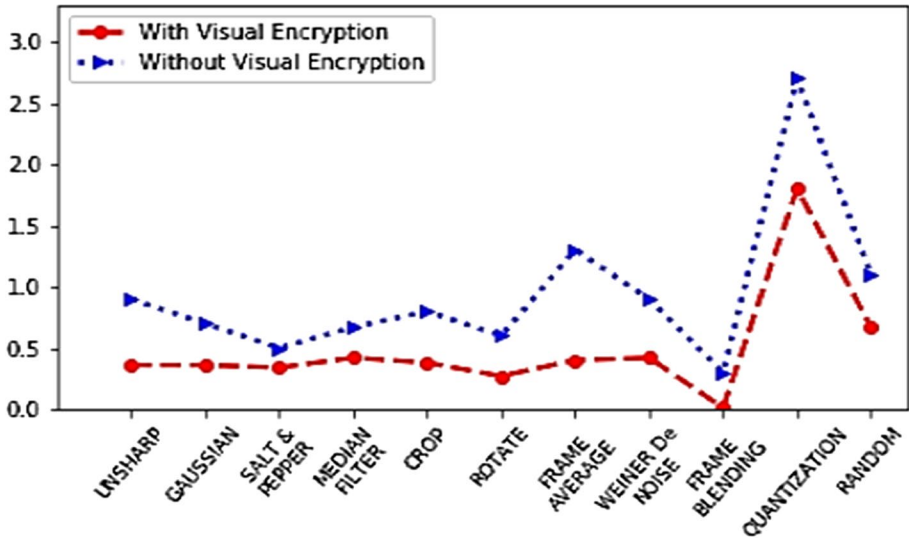


Fig. 6 BER comparison using visual cryptography and without cryptography

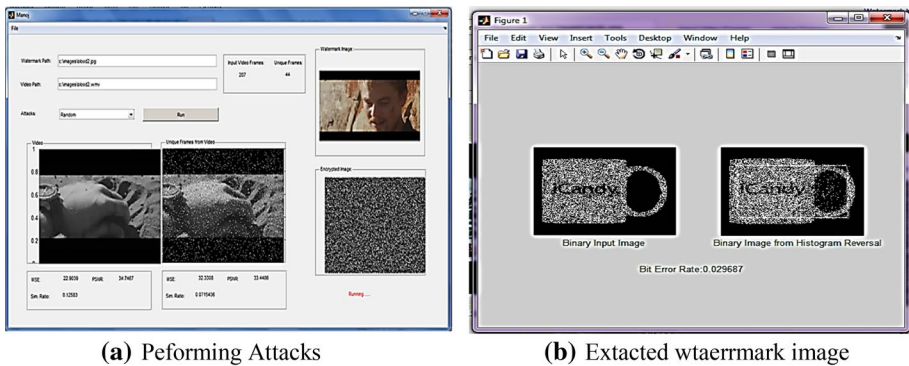


Fig. 7 A sample of GUI shows performing attacks in a and extraction of watermark in b

watermark, there are no visible artifacts can be seen in the watermarked video frames. If we compare the estimated PSNR for this video watermarking system to other similar approaches, this method outperforms and maintains high data imperceptibility. Even though there are very few techniques in the literature that uses this kind of video watermarking approach. Therefore, this method brings better results are contribute substantially to the video watermarking domain.

The results plotted in this section depict that the proposed method can fill the research gap discussed above. The capacity of hiding data and the robustness of the technique against various attacks is highly attained. The optimization and encryption used in the proposed work make it more secure and novel for data embedding, where attacks rarely affect hidden watermark information as presented through the results. With the proposed system, the quality of the final watermarked video is also decent and unique. Further, when the algorithm is applied to extract the keyframes (Threshold-based), a frame is considered true

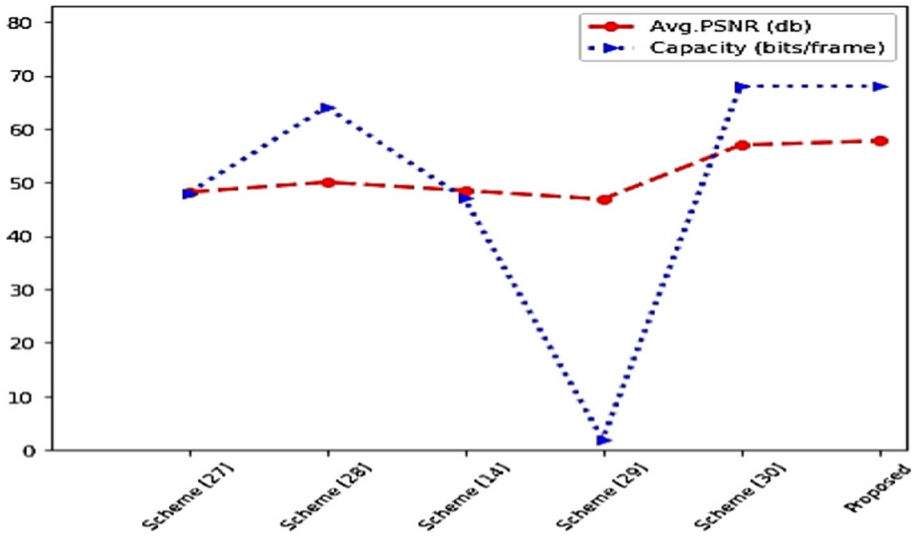


Fig. 8 Performance of proposed approach using avg. PSNR and watermark bits embedding capacity

positive if that frame is selected as keyframe by the proposed method and user and false positive if the frame is considered by the implemented method only. A false negative frame is that frame that is selected as a keyframe by the user but not by the approach. Using this information, we also computed Precision, Recall and F-measure. These are estimated using Eqs. 15–17.

$$Recall = \frac{n_{TP}}{n_{TP} + n_{FN}} \tag{15}$$

$$Precision = \frac{n_{TP}}{n_{TP} + n_{FP}} \tag{16}$$

$$F = 2 \frac{Recall \times Precision}{Recall + Precision} \tag{17}$$

Using these equations, the output of various parameters for the proposed method and other approaches is shown in Table 4.

From these results, it is identified that the proposed technique results are acceptable based on these metrics. All the metrics are estimated from all five cases of videos + watermark images, and accessed average values are shown for the proposed method in Table 4.

Table 4 Comparison between recall, precision and F-measure

	Furini et al. (2010)	Ejaz et al. (2014)	Dang et al. (2015)	Himeur and Boka-bau (2018b)	Proposed method
Recall	0.68	0.86	0.96	0.95	0.96
Precision	0.66	0.82	0.95	0.93	0.94
F-measure	0.64	0.84	0.95	0.94	0.95

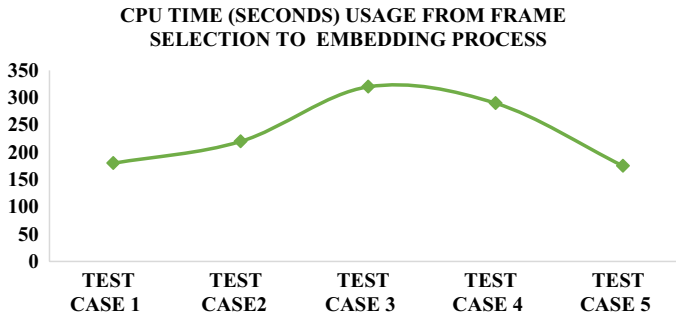


Fig. 9 CPU utilization for used test cases

Figure 9 compiles the results of CPU time computation for all the test cases using proposed approach. The results depict that time complexity usage is less because of convergence for finding an optimal video frame. The compile-time starts from the frame selection to the embedding process and finally returning the watermarked video. Maximum compilation time is taken by case 3 (320 Sec.) of the proposed work, while the fastest execution is for case 5 (175 s.) while the difference is 40 s. between test cases 2 and 4. This might be due to the number of frames estimated and video length for a particular video. In the proposed work, we presented time is not individually estimated for like frame extraction or specific embedding capacity instead involves the whole process.

5 Conclusion

In the proposed paper, a robust video watermarking system is suggested for which a watermark share is embedded on complex frames in a blind manner. These complex frames are extracted based on Firefly based optimization method. Instead of embedding watermarks share on all the video frames, the proposed method chooses unique complex frames based on a threshold value. Further, an adaptive histogram bit shifting based method is suggested which hides watermark share in LL band of video frames. In addition, visual cryptography is implemented to encode watermark before embedding/hiding in the DWT domain and this brings robustness and security in the approach. The experimental results are encouraging in terms of various parameters such as imperceptibility, payload capacity, MSE and BER. Furthermore, our approach is tested against 11 type of attacks and reported minimum bit errors. Finally, the demonstrated result shows that the proposed technique can accomplish digital video watermarking satisfactorily compared to other state-of-art techniques. In the future, this technique can also be tested again other geometrical attacks. Also, the technique can be improved for embedding watermark in the compressed video stream.

References

- Agilandeewari L, Ganesan K (2016) A robust color video watermarking scheme based on hybrid embedding techniques. *Multimed Tools Appl* 75:8745–8780
- Alotaibi SS (2020) Optimization insisted watermarking model: hybrid firefly and Jaya algorithm for video copyright protection. *Soft Comput.* <https://doi.org/10.1007/s00500-020-04833-8>

- Altay SY, Ulutaş G (2021) Self-adaptive step firefly algorithm based robust watermarking method in DWT-SVD domain. *Multimed Tools Appl*. <https://doi.org/10.1007/s11042-020-10251-7>
- Arab F, Abdullah SM, Hashim SZM, Mana AA, Zamani M (2016) A robust video watermarking technique for the tamper detection of surveillance systems. *Multimed Tools Appl* 75:10855–10885
- Asikuzzaman M, Alam MJ, Lambert AJ, Pickering MR (2016) Robust DT CWT-based DIBR 3D video watermarking using chrominance embedding. *IEEE Trans Multimed* 18(9):1733–1748
- Ayubi P, Barani M, Valandar M, Irani B, Sadigh R (2021) A new chaotic complex map for robust video watermarking. *Artif Intell Rev* 54(2):1237–1280
- Bhardwaj A, Verma VS, Jha RK (2018) Robust video watermarking using significant frame selection based on coefficient difference of lifting wavelet transform. *Multimed Tools Appl* 77(2018):19659–19678
- Cao Z, Wang L (2019) A secure video watermarking technique based on hyperchaotic Lorentz system. *Multimed Tools Appl* 78(2019):26089–26109
- Chang C, Chou YC, Lu TC (2007) A semi-blind watermarking based on discrete wavelet transform. In: *International conference on information and communications security*, Berlin, Heidelberg
- Chuan Q, Wei Z, Fang C, Xinpeng Z, Chin-Chen C (2018) Separable reversible data hiding in encrypted images via adaptive embedding strategy with block selection. *Signal Process* 153(2018):109–122
- Dang C, Radha H (2015) RPCA-KFE: Key frame extraction for video using robust principal component analysis. *IEEE Trans Image Process* 24(11):3742–3753
- Doğan S (2016) A new data hiding method based on chaos embedded genetic algorithm for color image. *Artif Intell Rev* 46(1):129–143
- Ejaz N, Mehmood I, Baik SW (2014) Feature aggregation based visual attention model for video summarization. *Comput Electr Eng* 40(3):993–1005
- Kumar M, Hensman A (2013) Robust digital video watermarking using reversible data hiding and visual cryptography. In: *24th IET Irish signals and systems conference*, Ireland
- Lu ZM, Guo SZ (2017) *Lossless information hiding in images*. Syngress
- Furini M, Geraci F, Montangero M et al (2010) STIMO: STill and MOving video storyboard for the web scenario. *Multimed Tools Appl* 46:47. <https://doi.org/10.1007/s11042-009-0307-7>
- Himeur Y, Boukabou A (2018a) A robust and secure key-frames based video watermarking system using chaotic encryption. *Multimed Tools Appl* 77:8603–8627
- Himeur Y, Boukabou A (2018b) A robust and secure key-frames based video watermarking system using chaotic encryption. *Multimed Tools Appl* 77(7):8603–8627
- Hou J, Ou B, Tian H, Qin Z (2021) Reversible data hiding based on multiple histograms modification and deep neural network. *Signal Process Image Commun* 92:11618
- Huang H-C, Chen Y-H, Abraham A (2010) Optimized watermarking using swarm-based bacterial foraging. *J Inf Hiding Multimed Signal Process* 1(1):51–58
- Jia Y, Yin Z, Zhang X, Luo Y (2019) Reversible data hiding based on reducing invalid shifting of pixels in histogram shifting. *Signal Process* 163(2019):238–246
- Karmakar A, Phadikar A, Phadikar BS, Maity GK (2016) A blind video watermarking scheme resistant to rotation and collusion attacks. *J King Saud Univ Comput Inf Sci* 28(2):199–210
- Katzenbeisser S, Petitcolas F (2000) *Information hiding techniques for steganography and digital watermarking*, United States: information hiding techniques for steganography and digital watermarking
- Kulkarni P, Kulkarni G (2018) Visual cryptography based grayscale image watermarking in DWT domain. In: *2018 Second international conference on electronics, communication and aerospace technology (ICECA)*, Coimbatore, India
- Kumar M, Srivastava S, Hensman A (2016) A hybrid novel approach of video watermarking. *Int J Signal Process Image Process Pattern Recognit* 9(10):395–406
- Kumar R, Ki-Hyun J (2020) Robust reversible data hiding scheme based on two-layer embedding strategy. *Inf Sci* 512:96–107
- Li Z, Chen X-W, Ma J (2015) Adaptively imperceptible video watermarking based on the local motion entropy. *Multimed Tools Appl* 74(2015):2781–2802
- Li Y, Yao S, Yang K, Tan Y-A, Zhang Q (2019) A high-imperceptibility and histogram-shifting data hiding scheme for JPEG images. *IEEE Access* 7:73573–73582
- Malik S, Reddlapalli RK (2019) Histogram and entropy based digital image watermarking scheme. *Int J Inf Technol* 11(2019):373–379
- Mishra A, Agarwal C, Sharma A, Bedi P (2014) Optimized gray-scale image watermarking using DWT-SVD and firefly algorithm. *Expert Syst Appl* 41(17):7858–7867
- Mustafa Bilgehan I, Mustafa U, Guzin U (2017) A new reversible database watermarking approach with firefly optimization algorithm. *Math Prob Eng*. <https://doi.org/10.1155/2017/1387375>
- Nasrullah N, Sang J, Mateen M, Akbar MA, Xiang H, Xia X (2019) Reversible data hiding in compressed and encrypted images by using Kd-tree. *Multimed Tools Appl* 78:17535–17554

- Noor R, Khan A, Sarfaraz A, Mehmood Z, Cheema AM (2019) Highly robust hybrid image watermarking approach using Tchebichef transform with secured PCA and CAT encryption. *Soft Comput* 23(2019):9821–9829
- Rajkumar R, Vasuki A (2019) Reversible and robust image watermarking based on histogram shifting. *Clust Comput* 22:12313–12323
- Rasti P, Samiei S, Agoyi M, Escalera S, Anbarjafari G (2016) Robust non-blind color video watermarking using QR decomposition and entropy analysis. *J Vis Commun Image Represent* 38(2016):838–847
- Senthilnathan T, Prabu P, Sivakumar R, Sakthivel S (2019) An enhancing reversible data hiding for secured data using shuffle block key encryption and histogram bit shifting in cloud environment. *Clust Comput* 22(2019):12839–12847
- Shah M, Zhang W, Hu H, Zhou H, Mahmood T (2018) Homomorphic encryption-based reversible data hiding for 3D mesh models. *Arab J Sci Eng* 43:8145–8157
- Singh TR, Singh KM, Roy S (2013) Video watermarking scheme based on visual cryptography and scene change detection. *AEU-Int J Electron C* 67(8):645–651
- Tang Z, Xu S, Yao H, Qin C, Zhang X (2019) Reversible data hiding with differential compression in encrypted image. *Multimed Tools Appl* 78(2019):9691–9715
- Thakur S, Singh A, Ghrera S, Elhoseny M (2019) Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications. *Multimed Tools Appl* 78(3):3457–3470
- Thanki R, Kothari A, Trivedi D (2019) Hybrid and blind watermarking scheme in DCuT–RDWT domain. *J Inf Secur Appl* 46:231–249
- Wang C, Shan R, Zhou X (2018) Anti-HEVC recompression video watermarking algorithm based on the all phase biorthogonal transform and SVD. *IETE Tech Rev* 35(2018):42–58
- Weng S, Zhang C, Zhang T, Chen K (2021) High capacity reversible data hiding in encrypted images using SIBRW and GCC. *J Vis Commun Image Represent* 75:102932
- Xu D, Chen K, Wang R, Su S (2018) Separable reversible data hiding in encrypted images based on two-dimensional histogram modification. *Secur Commun Netw*. <https://doi.org/10.1155/2018/1734961>
- Yang X (2009) Nature-inspired metaheuristic algorithms. Luniver press
- Youssef SM, ElFarag AA, Ghatwary NM (2014) Adaptive video watermarking integrating a fuzzy wavelet-based human visual system perceptual model. *Multimed Tools Appl* 73(2014):1545–1573
- Zhao J, Li Z (2018) Three-dimensional histogram shifting for reversible data hiding. *Multimed Syst* 24:95–109

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Authors and Affiliations

Manoj Kumar¹ · Jyoti Aggarwal² · Anuj Rani³ · Thompson Stephan⁴ · Achyut Shankar⁵ · Seyedal Mirjalili^{6,7}

Manoj Kumar
wss.manojkumar@gmail.com

Jyoti Aggarwal
itsjyotiagarwal1@gmail.com

Anuj Rani
anuanuj1989@gmail.com

Thompson Stephan
thompsonscse@gmail.com

Achyut Shankar
ashankar2711@gmail.com

¹ School of Computer Science, University of Petroleum and Energy Studies (UPES), Dehradun, India

² Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun, India

- ³ Department of Computer Science, G L Bajaj Institute of Technology and Management, Greater Noida, India
- ⁴ Department of Computer Science and Engineering, Faculty of Engineering and Technology, M. S. Ramaiah University of Applied Sciences, Bangalore, Karnataka, India
- ⁵ Department of Computer Science and Engineering, Amity University, Noida, India
- ⁶ Centre for Artificial Intelligence Research and Optimisation, Torrens University Australia, Fortitude Valley, Brisbane, QLD 4006, Australia
- ⁷ Yonsei Frontier Lab, Yonsei University, Seoul, South Korea