Received August 17, 2020, accepted August 27, 2020, date of publication September 3, 2020, date of current version September 16, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3021356

A New Video Steganography Scheme Based on Shi-Tomasi Corner Detector

RAMADHAN J. MSTAFA[1,2], (Member, IEEE), YOUNIS MOHAMMED YOUNIS[1], HAVAL ISMAEL HUSSEIN[1], AND MUHSIN ATTO[1]

[1]Department of Computer Science, Faculty of Science, University of Zakho, Duhok 42002, Iraq
[2]Department of Computer Science, College of Computer and IT, Nawroz University, Duhok 42001, Iraq

Corresponding author: Ramadhan J. Mstafa (ramadhan.mstafa@uoz.edu.krd)

ABSTRACT Recent developments in the speed of the Internet and information technology have made the rapid exchange of multimedia information possible. However, these developments in technology lead to violations of information security and private information. Digital steganography provides the ability to protect private information that has become essential in the current Internet age. Among all digital media, digital video has become of interest to many researchers due to its high capacity for hiding sensitive data. Numerous video steganography methods have recently been proposed to prevent secret data from being stolen. Nevertheless, these methods have multiple issues related to visual imperceptibly, robustness, and embedding capacity. To tackle these issues, this paper proposes a new approach to video steganography based on the corner point principle and LSBs algorithm. The proposed method first uses Shi-Tomasi algorithm to detect regions of corner points within the cover video frames. Then, it uses 4-LSBs algorithm to hide confidential data inside the identified corner points. Besides, before the embedding process, the proposed method encrypts confidential data using Arnold's cat map method to boost the security level. Experimental results revealed that the proposed method is highly secure and highly invisible, in addition to its satisfactory robustness against Salt & Pepper noise, Speckle noise, and Gaussian noise attacks, which has an average Structural Similarity Index (SSIM) of more than 0.81. Moreover, the results showed that the proposed method outperforms state-of-the-art methods in terms of visual imperceptibility, which offers excellent peak signal-to-noise ratio (PSNR) of average 60.7 dB, maintaining excellent embedding capacity.

INDEX TERMS Arnold's Cat map, corner detector, embedding capacity, imperceptibility, robustness, security, video steganography.

I. INTRODUCTION

Information security issues have increased dramatically in the past few years, as people began to worry about their data from being cracked over the Internet—for instance, piracy tracking, copyright protection, authenticity identification of digital works, and identity authentication. To address these issues, the science of steganography and cryptography has emerged [1]–[3]. Steganography is a science that takes video, image, audio, or other digital media as a medium and then conceals secret data into the medium through a particular algorithm. Whereas, cryptography is a science that converts a secret message into a meaningless form so that eavesdroppers cannot interpret it [4]–[7]. Although both steganography and cryptography attempt to protect data, the use of either one alone is not an ideal solution. Thus, sometimes, it is recommended that both approaches be integrated. In such a case, even if the attacker had doubts about the existence of the communication and managed to defeat the steganography technique, the attacker would still need to break the encrypted message to obtain the secret message [8]–[11].

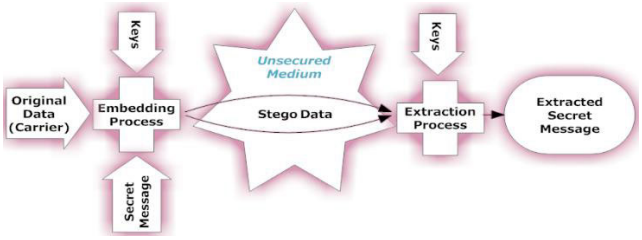

FIGURE 1. Generic diagram of steganography algorithm [12].

Fig. 1 illustrates, in general, the steps involved in the embedding and extraction process of any steganography algorithm. The efficiency of any successful steganography

The associate editor coordinating the review of this manuscript and approving it for publication was Md. Asikuzzaman.

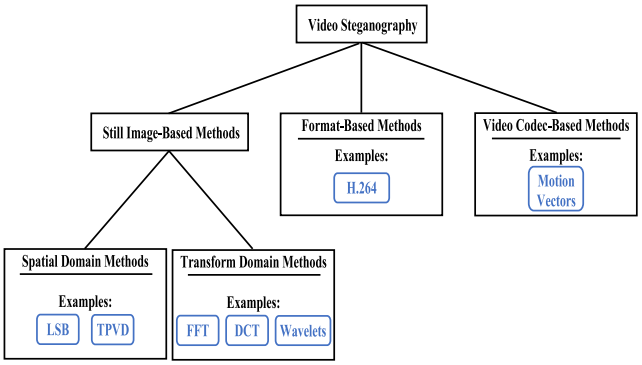

FIGURE 2. Three main categories of video steganography methods [24].

algorithms depends on four main factors: robustness, embedding capacity, security, and imperceptibility. Therefore, these factors should be taken into consideration when designing a new steganography algorithm as well as when improving the existing algorithms. Robustness refers to the resistance degree of the steganography algorithm against attacks and signal processing. Embedding capacity refers to the amount of data that can be embedded within the cover medium. Security refers to the inability of the attacker to extract the embedded data. Imperceptibility refers to the distortion degree in the original cover carrier due to the hiding process [13]–[15].

Compared to other digital media, digital video has more redundancy, providing a large capacity for hiding data. Besides, with the advent of the era of big data, a large amount of HD digital videos is transmitted over the Internet. Therefore, video steganography has attracted the attention of many researchers and has become a popular choice [12], [16]. Video steganography is the process of embedding a confidential message into a cover video. Where, it is used in many fields such as copyright protection, access control, medical systems, law enforcement [17]–[19].

In general, there are three main categories of video steganography methods, namely format-based methods, video codec-based methods, and still image-based methods [8], [20], [21]. Fig. 2 demonstrates these three different categories in a tree diagram. Still image-based methods transform video medium into frames and then apply methods of image steganography to the selected frames for data hiding purpose. These methods can be further categorized into two subcategories: transform domain methods and spatial domain methods. In the transform domain methods, the cover carrier is initially transformed into the frequency domain. Then, some coefficients of the frequency domain are selected to be replaced by the confidential message. Finally, the domain, with the altered coefficients, is converted back into the spatial domain. Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), and Discrete Fourier Transform (DFT) are some examples of the transform domain methods. On the other hand, spatial domain methods directly hide the confidential message into the cover carrier. Least Significant Bit (LSB) techniques are the most popular techniques of spatial domain methods due to their low computational complexity and simplicity [8], [22]–[24]. LSB techniques operate by substituting the confidential message bits with some LSBs of pixels from the video carrier frames. The second category of video steganography is format-based techniques. These techniques are designed for a particular video format by taking advantage of the compression strategy and structure of the format. H.264/AVC is an example of format-based techniques [25]. The third category of video steganography is video codec-based techniques. These techniques attempt to take advantage of the 3D nature of videos and exploit the third dimension, which is the time dimension t in embedding. This extra dimension provides some additional features, such as motion components and motion vectors [24], [26].

This paper proposes a new approach for hiding information within digital videos, which is based mainly on two well-known algorithms, namely Shi-Tomasi corner detector algorithm and Four Least Significant Bits (4-LSBs) algorithm. The proposed method first encrypts the secret information using Arnold's cat map algorithm. After that, it uses Shi-Tomasi algorithm to detect corner points regions in the Y (luminance) channel of each frame within the cover video. Finally, it embeds the secret information into each pixel of the detected regions using 4-LSBs algorithm.

The rest of the paper is structured as follows. Section II outlines some state-of-the-art methods related to video steganography. Section III explains Arnold's cat map algorithm and Shi-Tomasi corner detector as preliminaries. Section IV describes the proposed method in detail. Section V presents the experimental results with the discussion. Finally, section VI concludes the paper and suggests some future works.

II. RELATED WORKS

Due to the large capacity of digital videos for hiding sensitive data, video steganography has gained the attention of many researchers in the literature. This section reviews some recent video steganography methods that are closely linked to our proposed method.

M. Sadek *et al.* [27] presented a blind and robust approach to video steganography based on human skin areas of video frames. Their presented algorithm first detects the skin areas within each frame in the cover video to generate a skin-map. Then, it converts the skin map to a skin-block-map where skin pixels prone to error are ignored from the hiding process. Lastly, it applies a three-level of DWT on the blue and red color channels of each frame to embed the secret data within the coefficients of the identified skin pixels in the skin-block-map through quantization. Experimental results demonstrated that their proposed method achieves a high degree of imperceptibility.

K. Niu *et al.* [28] proposed a new reversible technique for video steganography using cover videos with H.264/AVC extension. They used Histogram Shifting (HS) of motion vector values to conceal the secret data within the identified reference frames of the cover video. In their proposed technique, the hidden information can be restored from the

compressed cover video in a lossless format. The results revealed that their proposed algorithm achieves higher invisibility and capacity than other existing techniques in the literature.

K. Rajalakshmi and K. Mahesh [29] introduced a novel approach for video steganography, called Zero Level Binary Mapping (ZLBM). Their proposed method first converts the cover video into frames. After that, it utilizes Fuzzy Adaptive Median Filtering (FAMF) technique to exclude the impulse noise from the frames. Then, it employs the block-wise pixel grouping method to group the pixels within the refined frames. In the end, it embeds the secret data using ZLBM method and encodes it using patch wise code formation method. Experimental results demonstrated that their proposed method performs better than other related approaches in terms of PSNR rate.

Y. Liu *et al*. [30] suggested a new and robust technique for video steganography based on the H.265/High-efficiency video coding pattern. Before the embedding process, their presented method encrypts the confidential data using BCH code approach. To restrict the intra-frame deformation drift, they used three groups of the prediction directions. After that, they embedded the encrypted secret data into the multi-coefficients of the selected four by four luminance discrete sine transform blocks, which meet the groups. Experimental results revealed that their proposed method obtains better visual quality than the methods studied earlier.

M. Hashem Zadeh [31] recommended an efficient approach for video steganography based on the salient and dynamic areas of a cover video. His algorithm identifies the dynamic regions based on motion clues of the feature points where the areas of interest are determined consequently. To conceal the secret data within the designated areas, he used the least-significant-bit substitution technique. Experimental results showed that his proposed method attains a higher hiding capacity when compared to the state-of-the-art approaches in the literature.

The major limitation of the existing video steganography methods in protecting sensitive data is the difficulty to guarantee a good trade-off between imperceptibility and robustness. Thus, this paper proposes a video steganography method that operates in the special domain using Shi-Tomasi corner detector algorithm and 4-LSBs algorithm to overcome the limitations of the pervious works. The reason for using corner detection points rather than other types of detection points is that its high robustness against different types of attacks and its ability to ensure high imperceptibility. Besides, it gives an acceptable embedding capacity. Furthermore, to increase the security level of the proposed method, Arnold's cat map algorithm is used before the embedding process.

III. PRELIMINARIES

This section explains Arnold's cat map algorithm and Shi-Tomasi corner detector algorithm in detail. This is due to the use of these two algorithms in the proposed method.

A. ARNOLD'S CAT MAP

Arnold's cat map, also referred to as Arnold's transformation, is one of the chaotic maps that operates in the discrete-time domain, which can be used only with square images. It was discovered by Vladimir Arnold in the 1960s using an image of a cat; hence the name came from. This method applies a transformation to an image so that it rearranges its pixels randomly. However, if iterated sufficient times, ultimately, the original image reappears. The number of considered iterations is known as Arnold's period. The period depends on the size of the image; for instance, images with different sizes may have different Arnold's period [32]–[34]. Arnold's transformation can be expressed mathematically as in Eq. (1).

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

where (x', y') is the new pixel location, (x, y) is the original pixel location, and N is the size of the square image. Cat map has two exemplary features that bring chaotic movement, namely tension and fold. Tension refers to the process of multiplying a matrix by x, y to enlarge x, y. Whereas, fold refers to the process of bringing back x, y within the unit matrix by using "*mod N*" [34]–[37].

Eq. (1) is employed to apply Arnold's transformation to every pixel in the image. When all the pixels, in the image, are transformed, the resulting image will appear in a meaningless form. At certain steps of iterations, if the resulting image reaches the expected target (for instance, up to the secret key), the requested scrambled image will be obtained. The decryption of image depends on the transformation periods (for instance, the number of iterations to be followed = Arnold's period − secret key). Fig. 3 shows the results of a cat image whose size is 150×150 after being transformed by Arnold's transformation using different iteration steps.

B. SHI-TOMASI CORNER DETECTOR

Shi-Tomasi algorithm, also referred to as Good Features to Track, is one of the corner detection approaches that is widely used in the field of computer vision to select certain types of features from an image. It is an improved version of Harris corner detector [39], [40]. Therefore, we start by illustrating Harris corner detector, and then we highlight the improvement aspect of this algorithm.

Harris corner detector is an eigenvalue-based feature point detector, which is the most widespread corner detector due to its strong invariance to image noise and rotation. It is based on the local auto-correlation function of a signal which measures the local changes of the signal with patches shifted by a small amount in different directions [41]–[43]. Given a shift $(\Delta x, \Delta y)$ and a point (x, y), the auto-correlation function can be defined [44] as in Eq. (2).

$$E\,(u, v) = \sum_x \sum_y \mathrm{w}(x, y)\,[I\,(x+u, y+v) - I(x, y)]^2 \tag{2}$$

where:

- E refers to the sum of squared differences between the original and moved window.

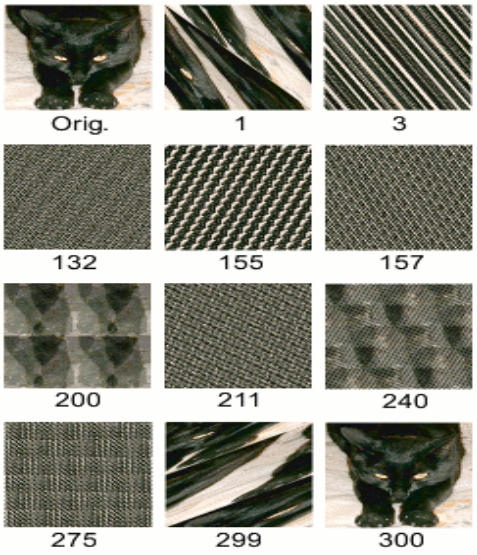

FIGURE 3. Sample mapping on a cat image of 150 × 150 pixels. The number shows the iteration step; after 300 iterations, the original cat image reappears [38].

- u refers to the window's displacement in the x-direction.
- v refers to the window's displacement in the y-direction.
- w (x, y) refers to the weighting function of the window at position (x, y), either a gaussian or a window of ones.
- $I\ (x + u, y + v)$ refers to the intensity of the moved window.
- $I(x, y)$ refers to the intensity of the original window.

Eq. (2) can be further expanded using Taylor's series and rewritten as in Eq. (3).

$$E\ (u, v) \approx \sum_x \sum_y \mathrm{w}(x, y) \left[I\ (x, y) + uI_x + vI_y - I\ (x, y)\right]^2 \tag{3}$$

Eq. (3) can also be rewritten in a matrix form as in Eq. (4).

$$E\ (u, v) \approx \begin{bmatrix} u & v \end{bmatrix} \left(\sum_x \sum_y \mathrm{w}(x, y) \begin{bmatrix} I_x^2 & I_x I_y \\ I_x I_y & I_y^2 \end{bmatrix} \right) \begin{bmatrix} u \\ v \end{bmatrix} \tag{4}$$

Eq. (4) can be further simplified as in Eq. (5).

$$E\ (u, v) \approx \begin{bmatrix} u & v \end{bmatrix} A \begin{bmatrix} u \\ v \end{bmatrix} \tag{5}$$

where A represents Harris-Matrix and is defined as in Eq. (6).

$$A = \sum_x \sum_y \mathrm{w}(x, y) \begin{bmatrix} I_x^2 & I_x I_y \\ I_x I_y & I_y^2 \end{bmatrix} \tag{6}$$

Measures of corner response (R) can be calculated [45] as in Eq. (7).

$$R = Det\ (A) - K\ (Trace\ (A))^2 = \lambda_1 \times \lambda_2 - K\ (\lambda_1 + \lambda_2)^2 \tag{7}$$

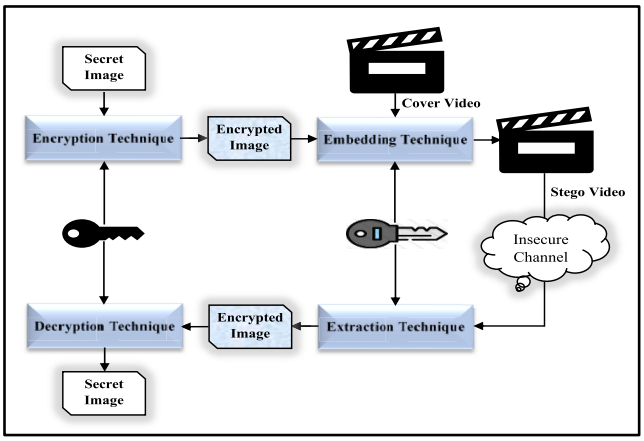

FIGURE 4. Generic design of the proposed method.

where $Det(A) = \lambda_1 \times \lambda_2$, $Trace\ (A) = \lambda_1 + \lambda_2$, λ_1 and $\lambda_2$are eigenvalues of (A), and (k) is a constant value.

Depending on the value of R, a point is deemed to be a [46]:

- Corner: if both $\lambda_1 \& \lambda_2$ are large, $\lambda_1 \approx \lambda_2$; E increases in all directions.
- Edge: if $\lambda_2 \gg \lambda_1$ or $\lambda_1 \gg \lambda_2$
- Flat: if both $\lambda_1 \& \lambda_2$ are small; E is almost constant in all directions.

Shi-Tomasi algorithm detects a corner using two eigenvalues as the Harris-Stephen algorithm does, but it calculates R function differently. In the Shi-Tomasi algorithm, R is calculated as follows:

$$R = \min\ (\lambda_1, \lambda_2) \tag{8}$$

If R is greater than a predetermined threshold, then the selected point is regarded as a corner point [39].

Shi-Tomasi algorithm produces feature points that are more stable and accurate for tracking than the Harris-Stephens algorithm. On the contrary, it results in higher computational demands [42].

IV. THE PROPOSED METHOD

This section describes the proposed video steganography method, which is based on the corner points regions of Shi-Tomasi algorithm and 4-LSBs algorithm. Shi-Tomasi algorithm with a predetermined threshold is used to detect corner points regions (i.e., Region of Interests (ROIs)) in Y (luminance) channel of each frame within the cover video. Whereas, 4-LSBs algorithm is used to embed the secret message in each pixel of the detected regions. To increase the security level of the proposed method, Arnold's cat map algorithm is used to encrypt the secret message before the embedding process. Here, the proposed method uses a square image with RGB color space as a secret message.

Before implementing the proposed method, both the sender and receiver should, in advance, agree upon the cover video, the shared secret key, the image size, and the threshold value. Where the cover video is a video in which the secret message is hidden in it, the shared secret key represents the key used in

Arnold's cat map algorithm, the image size represents the size of the secret image to be embedded/extracted, the threshold value represents the value used in Shi-Tomasi corner detector algorithm to detect corner points in the frames of the cover video where different threshold values result in different corner points.

Fig. 4 gives a generic design of the proposed method. Message encryption, message embedding, message extraction, and message decryption for the proposed method are explained in the following subsections.

A. MESSAGE ENCRYPTION AND EMBEDDING

Fig. 5 demonstrates the block diagram of message encryption and message embedding for the proposed method. In this stage, the cover video, the threshold value, the shared secret key, the secret image, and the image size are the inputs, and the stego-video is the output. The image size must be square and set by the user due to the use of Arnold's cat map algorithm that only accepts a square image as input. Before the embedding process, the secret image is encrypted with the shared secret key using Arnold's cat map encryption algorithm as described in section III-A. Here, the shared secret key indicates the number of iterations used to scramble the secret image. After that, the encrypted image is partitioned into three images representing Red, Green, and Blue color channels, respectively. Each of these images is then transformed into binary bits. Next, the binary bits of the three images are concatenated to form a single sequence of binary bits that represents the encrypted image. To embed the binary bits obtained from the encryption process inside the cover video, first, the cover video is partitioned into frames. Each Frame is then partitioned into Y (luminance), U (Cb blue chrominance), V (Cr red chrominance) channels. After that, Shi-Tomasi algorithm with a predetermined threshold is applied to the Y channel of each frame in the subsequent processes to detect corner points regions (i.e., ROIs) in them as described in section III-B. Next, the binary bits are embedded in each pixel of the detected regions using 4-LSBs algorithm. Then, the Y, U, V channels of each frame are transformed back into their original color space. Finally, the frames are transformed into a video known as a stego video.

B. MESSAGE EXTRACTION AND DECRYPTION

Fig. 6 demonstrates the block diagram of message extraction and message decryption for the proposed method. In this stage, the cover video, the stego video, the threshold value, the shared secret key, and the image size are the inputs, and the secret image is the output. Here, Shi-Tomasi algorithm cannot be applied to the Y channel of each frame within the stego video due to the change in pixels values during the embedding process, which will result in different corner points regions (i.e., ROIs). Therefore, the cover video is needed to identify locations of the pixels where the binary bits are hidden in them. To extract the embedded binary bits from the stego video, the cover video, first, is partitioned into frames. Each Frame is then partitioned into Y (luminance), U (Cb blue chrominance), V (Cr red chrominance) channels. After that, Shi-Tomasi algorithm with a predetermined threshold is applied to the Y channel of each frame in the subsequent processes to detect corner points regions (i.e., ROIs) in them as described in section III-B. Then, the embedded binary bits are extracted from pixels of the Y channel of each frame within the stego video in the subsequent processes, so that their locations are equal to the detected locations in the previous step. Next, the extraction process terminates when the length of the obtained binary bits is equal to the length of the (image size $\times$ 3) in binary bits. Here "$\times$ 3" is used because the secret image contains three channels with the same size (red, green, and blue, respectively). Afterward, the extracted binary bits are transformed into three images of size $\boldsymbol{n} \times \boldsymbol{n}$. The three images are then transformed into one image with RGB color space. The image obtained from the extraction process is then decrypted with the shared secret key using Arnold's cat map decryption algorithm as described in section III-A. Here, the number of iterations to be followed to decrypt the image is equal to Arnold's period minus the shared secret key. Where Arnold's period represents the number of considered iterations in a given square image. The image obtained from the decryption process is known as a secret image.

The following is a numerical example that elaborates of how our proposed algorithm works in detail. Assume the secret message is a color image of dimension **5** by **5**, and the cover video data consists of 30 frames per second where each frame has a resolution of **7** by **5**. Assume, the corner points detector has extracted **two** feature points in the Y component of the first frame. The embedding process will take place as the following:

Red channel values of the secret image.

32	8	15	67	155
1	61	194	109	249
20	97	64	164	151
211	91	130	66	180
198	11	180	177	63

Firstly, the red channel pixels' values will be converted from decimal ($P_1 = 32, P_2 = 8, P_3 = 15, P_4 = 67, P_5 = 155)_{10}$ to 8-bit binary values ($P_1 = 00100000, P_2 = 00001000, P_3 = 00001111, P_4 = 01000011, P_5 = 10011011)_2$.

In this assumption the first frame has two feature points, the first feature point is $FP_1(197)_{10} = (11000101)_2$. The four LSBs of FP_1 are (0101) as ordered 1^{st} (1) 2^{nd} (0) 3^{rd} (1) 4^{th} (0). The second corner point has the value $FP_2(43)_{10} = (00101011)_2$. The four LSBs of FP_2 are (1011) and as ordered 1^{st} (1) 2^{nd} (1) 3^{rd} (0) 4^{th} (1).

Y-part of the first frame shows two detected feature points

83	157	239	252	33	3	125
112	18	36	116	43	2	154
52	1	10	161	6	20	83
155	29	159	2	13	214	206
36	197	172	21	87	246	21

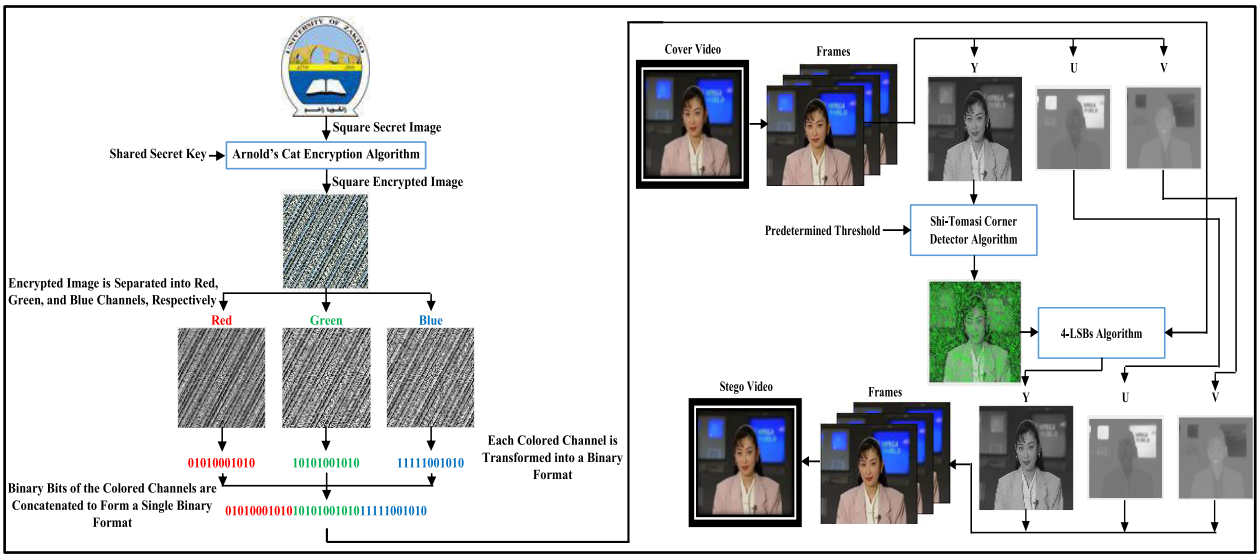

FIGURE 5. Block diagram of message encryption and message embedding for the proposed method.

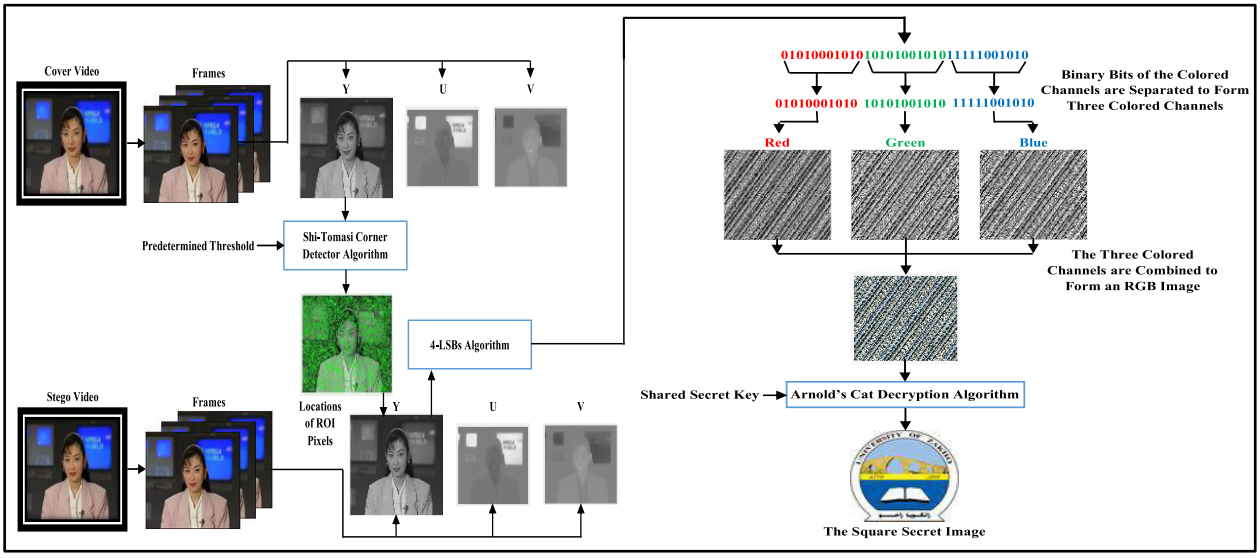

FIGURE 6. Block diagram of message extraction and message decryption for the proposed method.

Embedding process in each video frame can be done by replacing 4-LSBs of each feature point FP with 4-bits of each pixel in the secret image. The following is the embedding process of two feature points in the Y component of the first frame. At the beginning, the first part of the secret message (P_1) in the red color $P_1(32)_{10} = (00100000)_2$ will be embedded into the first feature point. As a result, the first stego feature point value (SFP_1) will change from $FP_1(197) = 11000101$ to $SFP_1(192)_{10} = (1100\ 0000)_2$. Next, the second part of the secret message (P_1) in the red color $P_1(32)_{10} = (00100000)_2$ will be embedded into the second feature point $FP_2(43) = 00101011$. The second feature point after embedding process will be $SFP_2(34)_{10} = (0010\ 0010)_2$ as shown below:

83	157	239	252	33	3	125
112	18	36	116	34	2	154
52	1	10	161	6	20	83
155	29	159	2	13	214	206
36	192	172	21	87	246	21

V. EXPERIMENTAL RESULTS

This section provides a detailed performance analysis of the proposed method. First, the dataset and evaluation metrics used in our experiments are presented. After that, the results of the proposed method are highlighted. Finally, comparisons of the proposed method with other methods presented in the literature are shown and discussed.

FIGURE 7. Set of test videos used for experimental results.

TABLE 1. Description of 15 cover videos in detail.

YUV Video Sequence	Format	Number of frames	Resolution	Video Size in Pixels
Akiyo	CIF	300	352×288	30,412,800
Carphone	QCIF	382	176×144	9,681,408
Coastguard	CIF	300	352×288	30,412,800
Container	CIF	300	352×288	30,412,800
Flower	CIF	250	352×288	25,344,000
Foreman	CIF	300	352×288	30,412,800
Hall Monitor	CIF	300	352×288	30,412,800
Mobile	CIF	300	352×288	30,412,800
Mother and D	CIF	300	352×288	30,412,800
News	CIF	300	352×288	30,412,800
Paris	CIF	1065	352×288	107,965,440
Silent	CIF	300	352×288	30,412,800
Suzie	QCIF	150	176×144	3,801,600
Tempete	CIF	260	352×288	26,357,760
Waterfall	CIF	260	352×288	26,357,760

A. DATASET

A dataset containing 15 commonly used video sequences, in the 4:2:0 YUV format, was used to evaluate the proposed video steganography method. This dataset was obtained from reference [47]. Fig. 7 shows the first frame for each cover video used in this work. Besides, Table 1 gives a detailed description of all these cover videos. The secret message was chosen to be an image of the logo of the University of Zakho of size 318 by 318 as shown in the Fig. 8.

Our work was implemented using MATLAB (R2017b) software program on a personal computer with the following specifications: Windows 10 Pro 64-bit operating system, Intel Core i7 2nd Generation (8 CPUs) 2.2GHz, Random Access Memory (RAM): 6144MB DDR3, Video RAM (VRAM): Radeon 6000 series 2034MB.

B. EVALUATION METRICS

The challenge of improving/innovating any video steganography methods is to embed as much information as possible in the cover video with a minimum noticeable difference in the stego video. Thus, the proposed method was evaluated and compared with state-of-the-art approaches using two metrics, namely embedding capacity and imperceptibility. Embedding

TABLE 2. The number of corner points detected, with different video sequences, using the Shi-Tomasi algorithm with a threshold of 0.00005.

YUV Video Sequence	Number of Frames	Detected Corner Points
Akiyo	300	494511
Carphone	382	137443
Coastguard	300	642023
Container	300	553588
Flower	250	381339
Foreman	300	539275
Hall Monitor	300	594343
Mobile	300	475314
Mother and Daughter	300	644720
News	300	285108
Paris	1065	1511612
Silent	300	572228
Suzie	150	67797
Tempete	260	432046
Waterfall	260	596114

FIGURE 8. University of Zakho logo as a secret image.

capacity refers to the maximum amount of information that can be hidden inside the cover video [27], [48], which is measured in bits-per-pixel (bpp) and calculated as in Eq. (9).

$$\textit{Embedding Capacity} = \frac{\textit{Numberof embedded bits}}{\textit{Cover video size in pixels}} \times 100\%\,(bpp) \quad (9)$$

The second metric, imperceptibility, is evaluated by measuring the visual quality of the stego-videos. Usually, to measure this metric, the Peak Signal-to-Noise Ratio (PSNR) is used, which is measured in decibels (dB) and calculated as in Eq. (10). PSNR values falling below 30 dB indicate that the human eye can notice the distortion. Hence, a good steganography algorithm should seek for 40 dB or more [29], [49].

$$PSNR = 10 \times \log_{10}\left(\frac{MAX_A^2}{MSE}\right)(dB) \quad (10)$$

Here, MSE refers to the mean squared error and is calculated as in Eq. (11).

$$MSE = \frac{\sum_{i=0}^{a-1}\sum_{j=0}^{b-1}\sum_{k=0}^{c-1}[A\,(i,j,k) - B(i,j,k)]^2}{a \times b \times c} \quad (11)$$

where A and B represent the original and stego frames, respectively, a and b represent the resolution of the given video, c

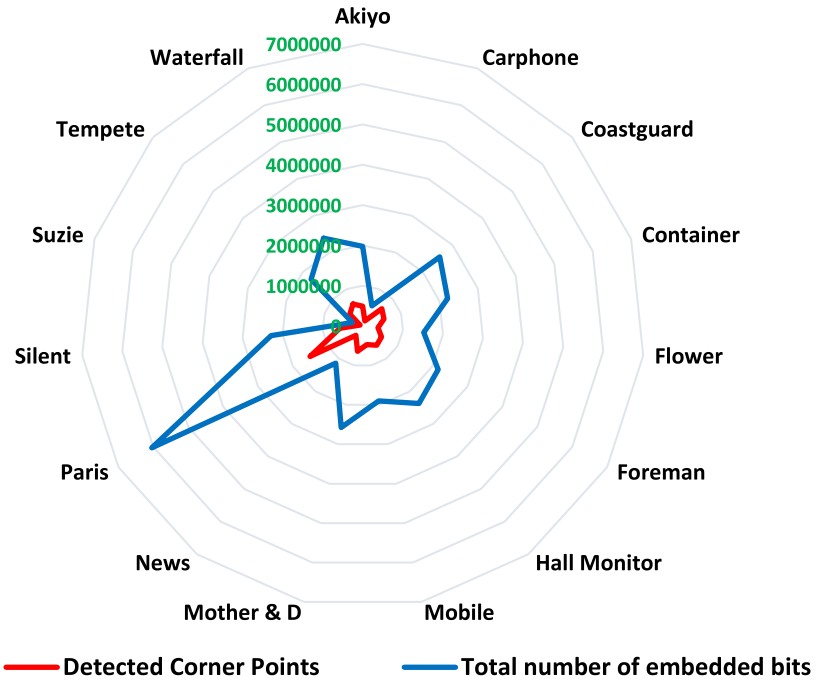

FIGURE 9. Performance analysis of the proposed method in terms of detected points and embedded bits.

TABLE 3. Performance analysis of the proposed method, with different video sequences, in terms of embedding capacity and PSNR.

YUV Video Sequence	Video Size in Pixels	Detected Corner Points	Total number of embedded bits	Embedding Capacity (bpp)	PSNR (dB)
Akiyo	30,412,800	494511	1,978,044	0.065	62.361
Carphone	9,681,408	137443	549,772	0.057	57.261
Coastguard	30,412,800	642023	2,568,092	0.084	62.129
Container	30,412,800	553588	2,214,352	0.073	62.090
Flower	25,344,000	381339	1,525,356	0.060	61.179
Foreman	30,412,800	539275	2,157,100	0.071	62.309
Hall Monitor	30,412,800	594343	2,377,372	0.078	62.088
Mobile	30,412,800	475314	1,901,256	0.063	62.008
Mother and Daughter	30,412,800	644720	2,578,880	0.085	61.967
News	30,412,800	285108	1,140,432	0.037	62.263
Paris	107,965,440	1511612	6,046,448	0.056	67.616
Silent	30,412,800	572228	2,288,912	0.075	62.239
Suzie	3,801,600	67797	271,188	0.071	53.196
Tempete	26,357,760	432046	1,728,184	0.066	61.490
Waterfall	26,357,760	596114	2,384,456	0.090	61.448
Average				**0.069**	**61.440**

refers to the number of channels that exist in the given color space (for RGB color space, $c = 3$). MAX_A represents the highest pixel value in frame A.

Finally, to evaluate the performance of the proposed method against different types of attacks (such as Gaussian noise, Speckle noise, and Salt & Pepper noise), the robustness metric was used. This metric computes the similarity ratio between the original message and the extracted message. Here, the structural similarity index (SSIM) function was used to measure this metric, which is expressed mathematically as in Eq. (12). Higher similarity values indicate better quality of the extracted image [50].

$$SSIM = \frac{\left(2\mu_O\mu_E + C_1\right)\left(2\sigma_{OE} + C_2\right)}{\left(\mu_O^2 + \mu_E^2 + C_1\right)\left(\sigma_O^2 + \sigma_E^2 + C_2\right)} \tag{12}$$

where O represents the original image, E represents the extracted image, μ_O and σ_O represent the mean and standard deviation values of pixels in image O, respectively, μ_E and σ_E represent the mean and standard deviation values of pixels in

image E, respectively, C_1 and C_2 refer to a fixed value, σ_{OE} represents the covariance between O and E images.

C. RESULTS OF THE PROPOSED METHOD

This section shows the performance of the proposed method in terms of embedding capacity, PSNR, and SSIM on 15 cover videos. Here, before the embedding process, we detected the corner points of each cover video using Shi-Tomasi algorithm with a threshold of 0.00005 to embed the secret data into them. The reason for selecting the threshold of 0.00005 was based on empirical tests in which we could detect more corner points in each cover video without affecting the quality of the stego video. Moreover, we used 4-LSBs method for embedding the secret information within the cover videos.

Table 2 shows the number of corner points detected in each cover video. From Table 2, it is clear that the number of detected corner points varies from one cover video to another. As it is also evident from Table 2 that both Paris and Suzie cover videos obtained the highest and the lowest number of detected corner points, which are 1511612 and 67797, respectively. This is due to the difference in frames' scenes and the number of frames in each cover video.

The performance of the proposed method in terms of embedding capacity and PSNR on 15 cover videos has been summed up in Table 3. From Table 3, it can be seen that the videos "Waterfall", "Mother and Daughter", "Coastguard", "Hall Monitor", "Silent", "Container", "Foreman", and "Suzie" provide a higher embedding capacity rate than other videos. This is because the corner points in these cover videos are abundant. The embedding capacity obtained for the low-corner points videos "Tempete", "Akiyo", "Mobile", "Flower", "Carphone", "Paris", and "News" is not as good as the embedding capacity obtained for other videos. This is expected due to the lack of corner points found in these cover videos, where the area of the extracted ROI is very little. It is also evident from Table 3 that the average of embedding capacity in all videos used is 0.069. This indicates that the proposed method can hide an acceptable amount of information. Moreover, as shown in Table 3, the PSNR values of all videos used are greater than or equal to 53.196 dB. This shows the high perceptual invisibility of the proposed method. It can also be noted from Table 3 that the average value of PSNR in all videos used is 61.440 dB. This confirms that the proposed method is highly imperceptible. Accordingly, we can deduce that the proposed method provides a high degree of imperceptibility with an acceptable embedding capacity. Fig. 9 illustrates the performance analysis of the proposed method in terms of the total number of detected corner points and the total number of the embedded bits in each tested video. It is obvious from Fig. 9 that the embedding capacity of each cover video increases whenever the detected corner points increase.

Fig. 10 demonstrates the performance of the proposed method in terms of SSIM rate with and without noises on 15 cover videos. From Fig. 10, it can be noticed that the SSIM rate is almost "1" in all cover videos when no noise is added to them. This indicates that the secret data can be recovered by losing a little bit of data. It can also be seen from Fig. 10 that when Salt and Pepper noise with a density of 0.002 is added to the cover videos, the proposed method can still provide a high SSIM rate, which is very close to the SSIM rate of cover videos without noises. However, the SSIM rate decreases when the density of Salt and Pepper noise increases. Moreover, from Fig. 10, It can also be noted that when Gaussian noise is incorporated into the cover videos, the proposed method obtains the SSIM rate of less than 0.78 (Flower video), which is still acceptable. But, when Speckle noise is incorporated into the cover videos, the proposed method obtains the SSIM rate of less than 0.71 (News video), which degrades the performance of the proposed method. Fig. 11 shows the extracted secret images from five cover videos (Akiyo, Carphone, Coastguard, Container, and Flower) after different attacks have been applied on them.

We can conclude from Fig. 10 that the proposed method is robust when the cover videos are free of noises, however, the proposed method degrades when noises are incorporated into the cover videos. Besides, the proposed method performs better with Salt and Pepper than other types of noises.

TABLE 4. Part I: Part II: Part III: Comparison of the proposed method with other existing approaches in terms of PSNR.

PART I

YUV Video	Ref. [27]	Proposed Method	YUV Video	Ref. [28]	Proposed Method
Carphone	50.6	57.2613	Carphone	37.48	57.2613
Foreman	50.5	62.3089	Coastguard	34.27	62.1286
Suzie	46	53.1957	Container	37.49	62.0896
			Foreman	36.04	62.3089
			Mobile	31.28	62.0077
			News	37.76	62.2625
Average	**49.033**	**57.589**	**Average**	**35.72**	**61.343**

PART II

YUV Video	Ref. [29]	Proposed Method	YUV Video	Ref. [30]	Proposed Method
Coastguard	34.77	62.1286	Carphone	38.63	57.2613
Container	36.67	62.0896	Container	38.42	62.0896
Mobile	34.88	62.0077	Foreman	37.32	62.3089
News	37.64	62.2625	Mobile	39.9	62.0077
			News	38.89	62.2625
			Paris	38.92	67.6163
Average	**35.99**	**62.122**	**Average**	**38.68**	**62.258**

PART III

YUV Video	Ref. [31]	Proposed Method
Coastguard	51.65	62.1286
Flower	47.31	61.1791
Foreman	53.13	62.3089
Mother and Daughter	54.56	61.9673
Suzie	54.46	53.1957
Tempete	52.31	61.4898
Waterfall	52.73	61.4478
Average	**52.307**	**60.531**

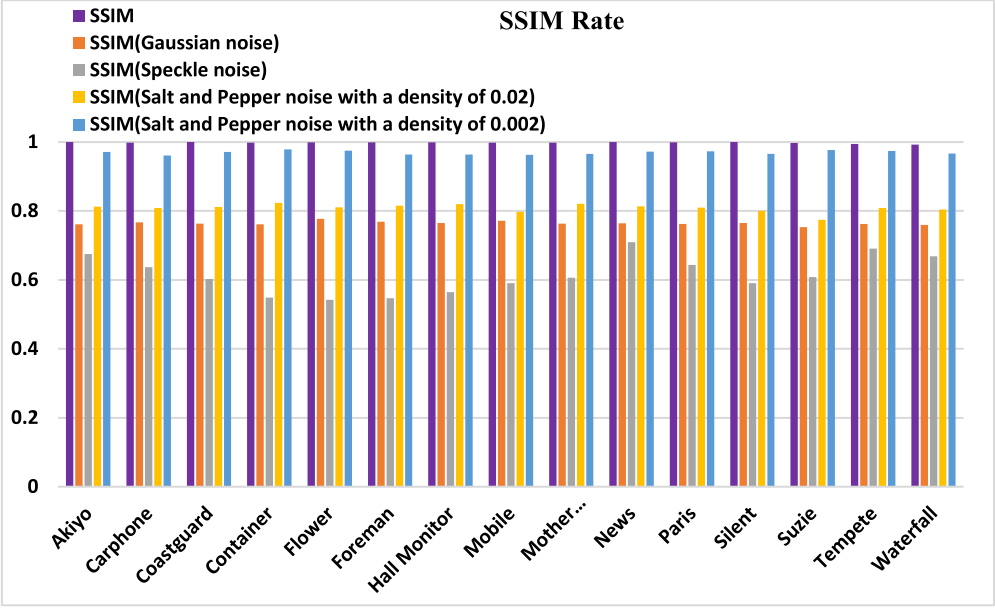

FIGURE 10. Performance analysis of the proposed method, with different video sequences, in terms of SSIM against free noise, Gaussian noise, Speckle noise, Salt and Pepper noise with density of 0.02, Salt and Pepper noise with density of 0.002, respectively.

Videos / Nosie	Secret Image Recovered from Akiyo	Secret Image Recovered from Carphone	Secret Image Recovered from Coastguard	Secret Image Recovered from Container	Secret Image Recovered from Flower
Gaussian noise	SSIM= 0.761	SSIM= 0.766	SSIM= 0.762	SSIM= 0.761	SSIM= 0.776
Speckle noise	SSIM= 0.675	SSIM= 0.636	SSIM= 0.602	SSIM= 0.548	SSIM= 0.542
Salt and Pepper noise (Density=0.02)	SSIM= 0.812	SSIM= 0.808	SSIM= 0.811	SSIM= 0.824	SSIM= 0.810
Salt and Pepper noise (Density=0.002)	SSIM= 0.971	SSIM= 0.961	SSIM= 0.970	SSIM= 0.978	SSIM= 0.975

FIGURE 11. Extracted secret images from first five cover videos (Akiyo, Carphone, Coastguard, Container, and Flower) in terms of SSIM against Gaussian noise, Speckle noise, Salt and Pepper noise.

TABLE 5. Part I: Part II: Comparison of the proposed method with other existing approaches in terms of total number of embedded bits.

PART I

YUV Video	Ref. [27]	Proposed Method	YUV Video	Ref. [28]	Proposed Method
Carphone	27,016	549,772	Carphone	21,466	549,772
Foreman	82,730	2,157,100	Coastguard	22,207	2,568,092
Suzie	31,496	271,188	Container	17,608	2,214,352
			Foreman	21,093	2,157,100
			Mobile	28,273	1,901,256
			News	10,346	1,140,432
Average	**47,081**	**992,687**	**Average**	**20,165**	**1,755,167**

PART II

YUV Video	Ref. [31]	Proposed Method
Coastguard	9,407,904	2,568,092
Flower	15,206,409	1,525,356
Foreman	10,543,104	2,157,100
Mobile	7,009,392	1,901,256
Mother and Daughter	3,556,304	2,578,880
Suzie	381,940	271,188
Tempete	5,438,451	1,728,184
Waterfall	5,911,859	2,384,456
Average	**7,181,920**	**1,889,314**

In addition, the proposed method with Gaussian noise obtains a higher SSIM rate than with Speckle noise. This is due to the noise nature in changing pixels values of the frames, where the pixels values of the extracted ROI get changed.

D. COMPARISONS WITH OTHER APPROACHES

In this section, the perceptual invisibility and the embedding capacity of the proposed method were compared with the proposed methods in the literature. The methods presented in [27]–[31] were chosen for comparison with the proposed method in terms of PSNR rate. To make the comparison fair, we used the same videos as those used in the methods presented in [27]–[31]. Tables 4 (Part I and Part II) list the PSNR rates obtained by the methods presented in [27]–[30] and the proposed method. The average results are bold-faced. From Tables 4 (Part I and Part II), it is evident that the proposed method attains the highest PSNR rate compared to the methods presented in [27]–[30] across all videos used. It is also clear from Table 3 that the average values of PSNR rate obtained by the proposed method is much better than the methods presented in [27]–[30]. This is about 8.556, 25.623, 26.132, and 23.578 dBs better than the average values of PSNR rate presented in [27]–[30], respectively. To further validate the efficacy of the proposed method in terms of visual imperceptibility, the proposed method was compared with the method presented in [31]. As shown in Table 4 (Part III), the proposed method outperforms the method presented in [31] in terms of average value of PSNR rate. Although the method presented in [31] is better than the proposed method when ''Suzie'' video is used but the differences between them is too little, which is 1.2643 dB.

It is worthy to mention that the proposed algorithm has a linear time complexity O(N) which will grow in direct proportion to the size of the secret data.

The methods presented in [27], [28], [31] were chosen for comparison with the proposed method in terms of the total number of embedded bits. Table 5 (Part I and Part II) list the total number of embedded bits obtained by the methods presented in [27], [28], [31] and the proposed method. The average results are bold-faced. From Tables 5 (Part I), it can be seen that the proposed method attains the highest total number of embedded bits compared to the methods presented in [27], [28] across all videos used. It can also be noticed from Tables 5 (Part I) that the average value of the total number of embedded bits obtained by the proposed method is much higher than those obtained by the methods presented in [27], [28]. This is about 21 and 87 times better than the average values of the total number of embedded bits presented in [27] and [28], respectively. To further validate the efficiency of the proposed method in terms of the total number of embedded bits, the proposed method was compared with the method presented in [31]. As shown in Table 5 (Part II), the method presented in [31] outperforms the proposed method in terms of average value of the total number of embedded bits. Although the method presented in [31] is better than the proposed method but the proposed method is still better in terms of visual imperceptibility.

Although the embedding capacity and visual quality are contradictions, the proposed algorithm have made an excellent balance between both factors. From the results obtained, we can deduce that the proposed method attains an acceptable embedding capacity and obtains better visual imperceptibility than those methods presented in [27]–[31].

VI. CONCLUSIONS AND FUTURE DIRECTIONS

This paper proposes a video steganography method based on the corner points regions and Arnold's cat map algorithm. The proposed method encrypts the secret information using Arnold's cat map algorithm prior to the embedding process to improve the security of the secret information. For hiding the encrypted secret data, the proposed method first detects the ROI in frames of the cover video using Shi-Tomasi corner detector algorithm with a predefined threshold. After that, the proposed method hides the encrypted secret information into the ROI using 4-LSBs algorithm. From the experimental results, it is clear that the proposed method outperforms state-of-the-art methods presented in [27]–[31] in terms of visual imperceptibility. In addition, it can be seen from the results that the proposed method performs better than the methods presented in [27], [28] in terms of embedding capacity. Although the method presented in [31] outperforms the proposed method in terms of embedding capacity, the proposed method is still better in terms of visual imperceptibility. Furthermore, the given results showed the acceptable range with regard to robustness against artificial noises (Gaussian noises, Speckle noises and Salt and Pepper noises with a density of (0.02, and 0.002)). For future works, different corner

point detector algorithms can be investigated, and the level of security can be increased by using one of the available public-key cryptography instead of Arnold's cat map algorithm.

REFERENCES

[1] Y. Yang, Z. Li, W. Xie, and Z. Zhang, "High capacity and multilevel information hiding algorithm based on pu partition modes for HEVC videos," *Multimedia Tools Appl.*, vol. 78, no. 7, pp. 8423–8446, Apr. 2019, doi: 10.1007/s11042-018-6859-7.

[2] 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, Nov. 2016, doi: 10.1007/s11042-015-2671-9.

[3] A. Sahu, K. Lakshmaiah, G. Swain, and K. Lakshmaiah, "Dual stego-imaging based reversible data hiding using improved LSB matching," *Int. J. Intell. Eng. Syst.*, vol. 12, no. 5, pp. 63–73, Oct. 2019.

[4] A. T. Bhole and R. Patel, "Steganography over video file using random byte hiding and LSB technique," in *Proc. IEEE Int. Conf. Comput. Intell. Comput. Res. (ICCIC)*, Dec. 2012, pp. 5–10, doi: 10.1109/ICCIC.2012.6510230.

[5] R. J. Mstafa and K. M. Elleithy, "A novel video steganography algorithm in the wavelet domain based on the KLT tracking algorithm and BCH codes," in *Proc. Long Island Syst., Appl. Technol.*, May 2015, pp. 1–7, doi: 10.1109/LISAT.2015.7160192.

[6] A. K. Sahu and G. Swain, "High fidelity based reversible data hiding using modified LSB matching and pixel difference," *J. King Saud Univ.–Comput. Inf. Sci.*, to be published, doi: 10.1016/j.jksuci.2019.07.004.

[7] M. Ma, D. He, M. K. Khan, and J. Chen, "Certificateless searchable public key encryption scheme for mobile healthcare system," *Comput. Electr. Eng.*, vol. 65, pp. 413–424, Jan. 2018.

[8] M. M. Sadek, A. S. Khalifa, and M. G. M. Mostafa, "Video steganography: A comprehensive review," *Multimedia Tools Appl.*, vol. 74, no. 17, pp. 7063–7094, Sep. 2015, doi: 10.1007/s11042-014-1952-z.

[9] R. Das and T. Tuithung, "A novel steganography method for image based on Huffman encoding," in *Proc. 3rd Nat. Conf. Emerg. Trends Appl. Comput. Sci. (NCETACS)*, Mar. 2012, pp. 14–18, doi: 10.1109/NCETACS.2012.6203290.

[10] R. J. Mstafa and K. M. Elleithy, "A new video steganography algorithm based on the multiple object tracking and Hamming codes," in *Proc. IEEE 14th Int. Conf. Mach. Learn. Appl. (ICMLA)*, Dec. 2015, pp. 335–340, doi: 10.1109/ICMLA.2015.117.

[11] A. Shehab, M. Elhoseny, K. Muhammad, A. K. Sangaiah, P. Yang, H. Huang, and G. Hou, "Secure and robust fragile watermarking scheme for medical images," *IEEE Access*, vol. 6, pp. 10269–10278, 2018, doi: 10.1109/ACCESS.2018.2799240.

[12] R. J. Mstafa and K. M. Elleithy, "A video steganography algorithm based on Kanade-Lucas-Tomasi tracking algorithm and error correcting codes," *Multimedia Tools Appl.*, vol. 75, no. 17, pp. 10311–10333, Sep. 2016, doi: 10.1007/s11042-015-3060-0.

[13] M. Douglas, K. Bailey, M. Leeney, and K. Curran, "An overview of steganography techniques applied to the protection of biometric data," *Multimedia Tools Appl.*, vol. 77, no. 13, pp. 17333–17373, Jul. 2018, doi: 10.1007/s11042-017-5308-3.

[14] R. J. Mstafa and K. M. Elleithy, "A high payload video steganography algorithm in DWT domain based on BCH codes (15, 11)," in *Proc. Wireless Telecommun. Symp. (WTS)*, Apr. 2015, pp. 1–8, doi: 10.1109/WTS.2015.7117257.

[15] R. J. Mstafa and K. M. Elleithy, "A highly secure video steganography using Hamming code (7, 4)," in *Proc. IEEE Long Island Syst., Appl. Technol. (LISAT) Conf.*, May 2014, pp. 1–6, doi: 10.1109/LISAT.2014.6845191.

[16] M. Zeeshan, M. Majid, I. F. Nizami, S. M. Anwar, I. Ud Din, and M. K. Khan, "A newly developed ground truth dataset for visual saliency in videos," *IEEE Access*, vol. 6, pp. 20855–20867, 2018.

[17] R. J. Mstafa, K. M. Elleithy, and E. Abdelfattah, "Video steganography techniques: Taxonomy, challenges, and future directions," in *Proc. IEEE Long Island Syst., Appl. Technol. Conf. (LISAT)*, May 2017, pp. 1–6, doi: 10.1109/LISAT.2017.8001965.

[18] R. J. Mstafa and K. M. Elleithy, "An efficient video steganography algorithm based on BCH codes," in *Proc. ASEE*, 2015, pp. 1–10, doi: 10.13140/RG.2.1.4202.7363.

[19] Y. Liu, S. Liu, Y. Wang, H. Zhao, and S. Liu, "Video steganography: A review," *Neurocomputing*, vol. 335, pp. 238–250, Mar. 2019, doi: 10.1016/j.neucom.2018.09.091.

[20] M. Shirali-Shahreza, "A new method for real-time steganography," in *Proc. 8th Int. Conf. Signal Process.*, vol. 4, 2006, doi: 10.1109/ICOSP.2006.345954.

[21] M. K. Khan, M. Zakariah, H. Malik, and K.-K.-R. Choo, "A novel audio forensic data-set for digital multimedia forensics," *Austral. J. Forensic Sci.*, vol. 50, no. 5, pp. 525–542, Sep. 2018.

[22] 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, Mar. 2017, doi: 10.1007/s11042-016-3383-5.

[23] R. J. Mstafa, K. M. Elleithy, and E. Abdelfattah, "A robust and secure video steganography method in DWT-DCT domains based on multiple object tracking and ECC," *IEEE Access*, vol. 5, pp. 5354–5365, 2017, doi: 10.1109/ACCESS.2017.2691581.

[24] T. Rabie and M. Baziyad, "The pixogram: Addressing high payload demands for video steganography," *IEEE Access*, vol. 7, pp. 21948–21962, 2019, doi: 10.1109/ACCESS.2019.2898838.

[25] T. Stütz and A. Uhl, "A survey of H.264 AVC/SVC encryption," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 22, no. 3, pp. 325–339, 2012, doi: 10.1109/TCSVT.2011.2162290.

[26] A. K. Sahu and G. Swain, "Reversible image steganography using dual-layer LSB matching," *Sens. Imag.*, vol. 21, no. 1, p. 1, Dec. 2020.

[27] M. M. Sadek, A. S. Khalifa, and M. G. M. Mostafa, "Robust video steganography algorithm using adaptive skin-tone detection," *Multimedia Tools Appl.*, vol. 76, no. 2, pp. 3065–3085, Jan. 2017, doi: 10.1007/s11042-015-3170-8.

[28] K. Niu, X. Yang, and Y. Zhang, "A novel video reversible data hiding algorithm using motion vector for H.264/AVC," *Tsinghua Sci. Technol.*, vol. 22, no. 5, pp. 489–498, Sep. 2017, doi: 10.23919/TST.2017.8030538.

[29] K. Rajalakshmi and K. Mahesh, "ZLBM: Zero level binary mapping technique for video security," *Multimedia Tools Appl.*, vol. 77, no. 11, pp. 13225–13247, Jun. 2018, doi: 10.1007/s11042-017-4942-0.

[30] Y. Liu, H. Zhao, S. Liu, C. Feng, and S. Liu, "A robust and improved visual quality data hiding method for HEVC," *IEEE Access*, vol. 6, pp. 53984–53996, 2018, doi: 10.1109/ACCESS.2018.2869148.

[31] M. Hashemzadeh, "Hiding information in videos using motion clues of feature points," *Comput. Electr. Eng.*, vol. 68, pp. 14–25, May 2018, doi: 10.1016/j.compeleceng.2018.03.046.

[32] A. M. Elshamy, M. A. Abdelghany, A. Q. Alhamad, H. F. A. Hamed, H. M. Kelash, and A. I. Hussein, "Secure VoIP system based on biometric voice authentication and nested digital cryptosystem using chaotic Baker's map and Arnold's cat map encryption," in *Proc. Int. Conf. Comput. Appl. (ICCA)*, Sep. 2017, pp. 140–146, doi: 10.1109/COMAPP.2017.8079739.

[33] O. Wahballa, A. Wahaballa, F. Li, I. I. Idris, and C. Xu, "Medical image encryption scheme based on Arnold transformation and ID-AK protocol," *Int. J. Netw. Secur.*, vol. 19, no. 5, pp. 776–784, 2017, doi: 10.6633/IJNS.201709.19(5).15.

[34] N. A. Abbas, "Image encryption based on independent component analysis and Arnold's cat map," *Egyptian Informat. J.*, vol. 17, no. 1, pp. 139–146, Mar. 2016, doi: 10.1016/j.eij.2015.10.001.

[35] M. Hamidi, M. E. Haziti, H. Cherifi, and M. E. Hassouni, "Hybrid blind robust image watermarking technique based on DFT-DCT and Arnold transform," *Multimedia Tools Appl.*, vol. 77, no. 20, pp. 27181–27214, Oct. 2018, doi: 10.1007/s11042-018-5913-9.

[36] M. Mahesh, D. Srinivasan, M. Kankanala, and R. Amutha, "Image cryptography using discrete Haar wavelet transform and Arnold cat map," in *Proc. Int. Conf. Commun. Signal Process. (ICCSP)*, Apr. 2015, pp. 1849–1855, doi: 10.1109/ICCSP.2015.7322844.

[37] A. A. Abd El-Latif, B. Abd-El-Atty, M. S. Hossain, M. A. Rahman, A. Alamri, and B. B. Gupta, "Efficient quantum information hiding for remote medical image sharing," *IEEE Access*, vol. 6, pp. 21075–21083, 2018.

[38] Wikiwand. (2019). *Arnold's Cat Map*. Accessed: Jan. 13, 2019. [Online]. Available: https://www.wikiwand.com/en/Arnold%27s_cat_map#

[39] R. A. Khan, S. Islam, and R. Biswas, "Automatic detection of defective rail anchors," in *Proc. 17th Int. IEEE Conf. Intell. Transp. Syst. (ITSC)*, Oct. 2014, pp. 1583–1588, doi: 10.1109/ITSC.2014.6957919.

[40] S. Wu, A. Oerlemans, E. M. Bakker, and M. S. Lew, "A comprehensive evaluation of local detectors and descriptors," *Signal Process., Image Commun.*, vol. 59, pp. 150–167, Nov. 2017, doi: 10.1016/j.image.2017.06.010.

[41] D. M. Cho, P. Tsiotras, G. Zhang, and M. J. Holzinger, "Robust feature detection, acquisition and tracking for relative navigation in space with a known target," in *Proc. AIAA Guid. Navig. Control Conf.*, 2013, pp. 1–18, doi: 10.2514/6.2013-5197.
[42] B. Pribyl, A. Chalmers, and P. Zemck, "Feature point detection under extreme lighting conditions," in *Proc. 28th Spring Conf. Comput. Graph. (SCCG)*, 2012, vol. 1, no. 212, pp. 143–150, doi: 10.1145/2448531.2448550.
[43] A. A. Abd EL-Latif, B. Abd-El-Atty, and S. E. Venegas-Andraca, "A novel image steganography technique based on quantum substitution boxes," *Opt. Laser Technol.*, vol. 116, pp. 92–102, Aug. 2019.
[44] M. Babiker, O. O. Khalifa, K. K. Htike, A. Hassan, and M. Zaharadeen, "Harris corner detector and blob analysis featuers in human activty recognetion," in *Proc. IEEE 4th Int. Conf. Smart Instrum., Meas. Appl. (ICSIMA)*, Nov. 2017, pp. 1–5, doi: 10.1109/ICSIMA.2017.8312025.
[45] V. A, N. Aklecha, Meghana, K. N. B. Murthy, and S. Natarajan, "On detectors and descriptors based techniques for face recognition," *Procedia Comput. Sci.*, vol. 132, pp. 908–917, May 2018, doi: 10.1016/j.procs.2018.05.106.
[46] H. A. Kadhima and W. A. Araheemah, "A comparative between corner-detectors (Harris, Shi-Tomasi & FAST) in images noisy using non-local means filter," *J. Al-Qadisiyah Comput. Sci. Math.*, vol. 11, no. 3, pp. 86–93, 2019.
[47] Video Test Media. (2019). *YUV Video Sequences Dataset*. Accessed: Mar. 3, 2019. [Online]. Available: https://media.xiph.org/video/derf/
[48] R. J. Mstafa and K. M. Elleithy, "An ECC/DCT-based robust video steganography algorithm for secure data communication," *J. Cyber Secur. Mobility*, vol. 5, no. 3, pp. 167–194, 2017, doi: 10.13052/jcsm2245-1439.531.
[49] R. J. Mstafa and K. M. Elleithy, "Compressed and raw video steganography techniques: A comprehensive survey and analysis," *Multimedia Tools Appl.*, vol. 76, no. 20, pp. 21749–21786, Oct. 2017, doi: 10.1007/s11042-016-4055-1.
[50] A. K. Moorthy and A. C. Bovik, "Efficient motion weighted spatio-temporal video SSIM index," *Proc. SPIE*, vol. 7527, Feb. 2010, Art. no. 75271I, doi: 10.1117/12.844198.

RAMADHAN J. MSTAFA (Member, IEEE) received the B.Sc. degree in computer science from the University of Salahaddin, Erbil, Iraq, in 2003, the M.Sc. degree in computer science from the University of Duhok, Duhok, Iraq, in 2008, and the Ph.D. degree in computer science and engineering from the University of Bridgeport, Bridgeport, Connecticut, USA, in 2017.

He is currently a Lecturer with the University of Zakho, Iraq. His research interests include image processing, mobile communication, wireless sensor networks, security, watermarking, and steganography. He also has more than 14 years of teaching experience in different universities and technical institutes in Iraq. He has published several papers in international journals and conferences in his areas of expertise. He has a role as reviewer in many prestige journals such as IEEE TRANSACTIONS, Elsevier, Springer, Springerplus, MDPI, and PLOS ONE international journals. He is a member of several technical and honorary societies such as IEEE computer society and ACM.

YOUNIS MOHAMMED YOUNIS was born in Duhok, Iraq, in 1990. He received the bachelor's degree in computer science and the master's degree in computer science from Zakho University, Iraq, in 2014 and 2019, respectively. He is currently working as a Lecturer with the Faculty of Science, Zakho University, Duhok, Iraq. His areas of interest are information security and information hiding.

HAVAL ISMAEL HUSSEIN was born in Mosul, Iraq, in 1989. He received the bachelor's and master's degrees in computer science from Zakho University, Iraq, in 2013 and 2018, respectively. He is currently working as a Lecturer with the Faculty of Science, Zakho University, Duhok, Iraq. His areas of interest are information security and machine learning.

MUHSIN ATTO received the B.S. degree in computer science from Duhok University, Duhok, Iraq, in 2004, the M.Sc. degree from Uppsala University, Sweden, in 2009, and the Ph.D. degree from the School of Systems Engineering, University of Reading, U.K. He has published more than ten papers in different international Journals and Conferences. One of his papers was selected as a best paper in conference. He is currently a Lecturer with the University of Zakho, Iraq. His research interests are in the areas of wireless sensor networks, mobile networks, and ad-hoc networks with emphasis on designing MAC and routing protocols providing the required quality of services for different applications.