DOI: https://doi.org/10.33103/uot.ijccce.23.3.12

Review: Dual Method Cryptography and Steganography in Video Frames in IoT

Rawia Abdullah. Muhammed[1], Maisa'a Abid Ali Al-Dabbas[2], Ashwak Mahmood Alabaichi[3]
[1,2]Computer Sciences Department, University of Technology, Baghdad, Iraq
[3] Biomedical Engineering Department, University of Kerbala, Kerbala, Iraq
[1]rawyia_8080@yahoo.com, [2]maisaa.a.khodher@uotechnology.edu.iq, [3]ashwaq.alabaichi@gmail.com

Abstract— *The Internet of things (IoT) is one of those emerging technologies, which are going to rule the world in the next few decades. The IoT environment not only enables Human to Machine interaction but also fosters Machine to Machine connectivity. Numerous IoT devices have poor security and insufficient computing power, making them prime targets for hackers. The IoT environment uses lightweight cryptographic techniques to address security requirements. Another security method for IoT devices is steganography. In the contemporary Internet era, the ability to secure private information is crucial, and steganography offers this capability. Due to its great ability to conceal sensitive data, video has drawn the attention of numerous academics among all forms of digital media. The main goal of this work is to examine several methods for fusing video steganography and cryptography techniques. Additionally, a thorough investigation and evaluation of a variety of video steganography methods in both compressed and raw domains are also emphasized. The comprehensive analysis of prior material makes it easier to have in-depth knowledge while creating approaches that combine cryptography with steganography.*

Index Terms *— IoT, Lightweight, Video, Cryptography, Stenography*

I. INTRODUCTION

In recent years, the Internet of Things has grown in significance within the context of information and communication technologies. The Internet of Things is a network of dispersed components, each with a unique identity, that are linked over the internet. These "things," often referred to as "connected objects" or "smart things," like IP cameras, are integrated with a variety of software programs and processing capabilities that allow them to gather and exchange data with other devices or systems through the internet without the need for human interaction[1]. IoT devices have simplified lives, but little thought has been given to their security. Currently, developers are mostly focused on improving the capabilities of these gadgets and give little thought to securing them. Data flow on the IoT network must be protected since it may be attacked[2]. Numerous information-securing mechanisms, such as cryptography and information-hiding methods, have been presented, as can be shown in *Fig. 1* [3]. The two methods of information concealment are steganography and watermarking [4]. Watermarking is a technique for copyright protection that verifies the origin of multimedia (picture, video, or audio) [5]. To prove ownership, watermarking may be either visible or invisible. The technique of steganography involves hiding important information in multimedia for clandestine communication[6]. Data cannot easily be detected because of the invisible nature of the process. One of the efficient methods for ensuring the secrecy, integrity, authentication, and permission of data traveling via IoT devices is cryptography. It could also be a way to safeguard data that is being stored or sent over a network. However, because of their high resource requirements, traditional PC-based cryptography techniques are not compatible with IoT devices. To overcome these obstacles to secure communication in IoT devices, lightweight cryptography is a more

Received 15/January/2023; Accepted 21/February/2023

DOI: https://doi.org/10.33103/uot.ijccce.23.3.12

lightweight version of existing methods[7]. Therefore, by transforming the original data's shape, cryptography may significantly increase the security of the data. Cryptography, however, is unable to prevent security concerns on its own since its encrypted form attracts the attention of attackers and may be altered or hacked[8]. To avoid being discovered by an intrusive party, researchers have routinely employed data hiding to conceal the presence of vital data. Thus, a cryptography-steganography (Crypto-stego) mechanism is now popular, in which steganography and cryptography are used together to give dual method security for the data. In order to provide a comprehensive reference for further study in this area, the most current literature in the fields of video steganography and Crypto-stego has been examined in this work. In this paper, the limitations of the various state-of-the-art techniques are further examined.Also, the key contributions of this study include

- A thorough analysis of different video approaches.
- A review of various dual method schemes with advantages and disadvantages for each of them.

The remainder of the essay is structured as follows. Section II includes a comparison between cryptography and steganography. Lightweight cryptography is discussed in Section III. Section IV presented video steganography. Joint Crypto‑ stego schemes are discussed in section VI. The paper concludes in Section VII.

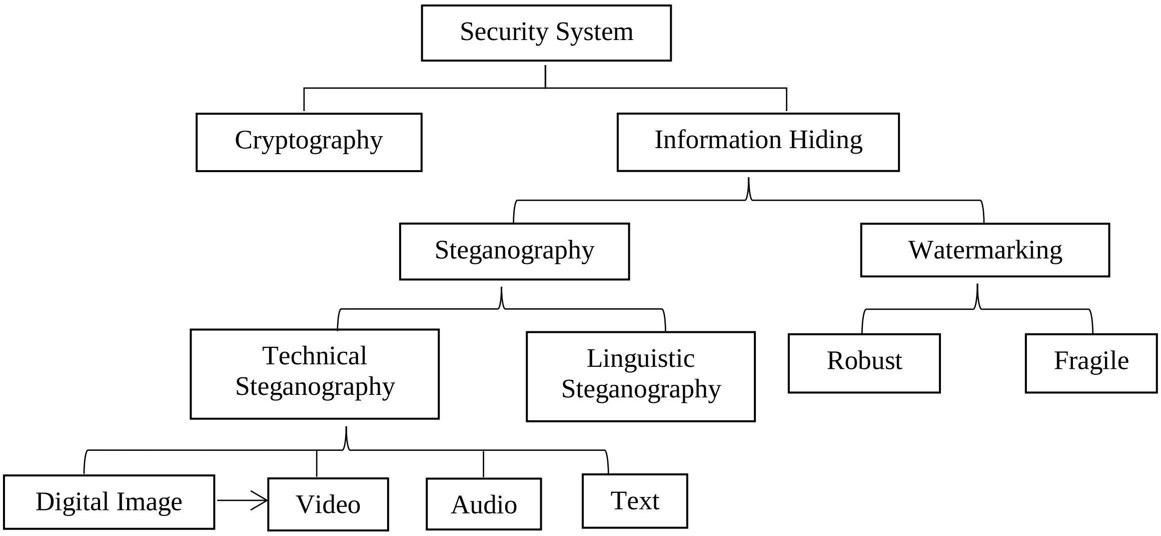

FIG. 1. DIFFERENT INFORMATION SECURING MECHANISMS [9].

II. COMPARISON BETWEEN CRYPTOGRAPHY AND STEGANOGRAPHY

Two security techniques, steganography, and cryptography have the goal of preserving sensitive information during transmission across an insecure channel. Because these two systems may be compared, they each have unique security characteristics. Table I. displays a comparative analysis of these security techniques.

TABLE I. COMPARATIVE ANALYSIS OF CRYPTOGRAPHY AND STEGANOGRAPHY

Characteristics	Cryptography	Steganography
Objective satisfied	Secret data are covert across	The whole communication channel is hidden
Objective dissatisfied	Communication channel	Communication is identified by the observer
Carrier object	A secret message (plain text) is retrieved by the third party	Audio (sound/speech), picture (frame), text (character), and video (sequence of frames)
Secret message	Image or Plain-text	Text, audio, image, video
Secret keys	Plain-text	Perhaps
Carrier information while extracting	Compulsory	Unnecessary

Received 15/January/2023; Accepted 21/February/2023

DOI: https://doi.org/10.33103/uot.ijccce.23.3.12

Output	Unnecessary	Steganogram
Level of Security depends on	Cryptogram	Embedding algorithms
Transparency of information	Secret keys	Invisible
Robustness	Visible	Against detection
Attacks	Against deciphering	Steganalysis
Quality assessment	Cryptanalysis	Capacity for concealment, invisibility, robustness, and embedding effectiveness

III. LIGHTWEIGHT CRYPTOGRAPHIC

The branch of contemporary cryptography known as lightweight cryptography (LWC) includes cryptographic algorithms designed for use in ubiquitous devices with limited resources, such as sensors, RFID tags, and medical equipment[10]. Because IoT devices lack processing capacity, must develop efficient encryption methods to protect data [11]. When implementing cryptography in any resource-constrained IoT device, LWC algorithms have three essential aspects that must be taken into account: physical cost, performance, and security. Each of these characteristics is also mentioned in terms of memory requirements, physical space requirements, and implementation costs. Processing power is measured in terms of latency, speed, and block/key length. As a security measure, alternative attack models, such as side-channel and fault-injection assaults, are also considered. The first two characteristics are achieved by LWC algorithms by providing simple round functions on the tiny block (≤ 64bit) using a tiny key (≤ 80bit) with simple key scheduling. The adoption of one of the six internal structures to be resistant to security threats completely leads to the final but crucial quality, security. There are two types of LWC asymmetric and symmetric cipher (block cipher, stream cipher, and hash function) [7]. Because many modern applications, such as secure radio frequency identification (RFID) tags, smart cards, wireless sensor networks (WSN), etc., heavily rely on lightweight encryption approaches. In this article, the author reviews current advancements in symmetric and asymmetric ciphers. Several surveys and reviews have been published in numerous international publications; some of these works are mentioned here for readers' convenience. To secure communication on the IoT, M. Tausif et al. [12] analyzed 13 lightweight ciphers. In other words, it offers a foundation to improve the cipher in several areas, including code size, memory capacity, and execution speed. J. Patil et al. [13] presented the $LiCi$ block cipher, a lightweight block cipher method. The suggested remedy withstands differential and linear attacks. Compressive sensing has been proposed by A. Aziz et al. [14] as a method of IoT lightweight security. Compressive sensing was used to encrypt the data in this investigation, which encourages energy saving. By taking advantage of the protocol's flaws, K. Wang et al. [15] offered ways to increase the security of an existing lightweight authentication mechanism for RFID. A fresh collection of curves called NUMS was introduced by Z. Liu et al. [16] and used to create a quick and effective ECC implementation. It offers asymmetric ciphers a better implementation. S. Raza et al. [17] have developed Tiny IKE which is a lightweight version of the IKEv2.

IV. STRUCTURE WISE CLASSIFICATION OF LWC

Cryptographic algorithms can be classified into two main categories, symmetric key, and asymmetric key cipher. Symmetric key uses a single key for both encryption and decryption of the data, whereas asymmetric cipher uses two different keys to encrypt and decrypt the data. Symmetric key cryptography is safe and comparatively fast, the only downside of symmetric key encryption is the sharing of the key between the communicating parties without compromising it. But this could be overcome by pre-sharing the key through a trusted third party. Also, it ensures confidentiality, data integrity, and authentication of the data. Asymmetric cryptography uses two private-public key pairs. It ensures confidentiality and integrity by making use of the public key of the receiver and further

Received 15/January/2023; Accepted 21/February/2023

DOI: https://doi.org/10.33103/uot.ijccce.23.3.12

ensures authentication by using the sender's private key (as a digital signature) to encrypt the data. At the other end, the receiver decrypts it by using the sender's public key first and then using his/her private key. The only disadvantage of asymmetric encryption is its large key which increases the complexity and slows down the process [7].

V. VIDEO STEGANOGRAPHY

As was previously mentioned, steganography may include several cover carrier objects and a hidden message, including text, audio, images, and video. Steganography, often known as video steganography, is a relatively new technique that primarily uses video as a cover to conceal a significant quantity of hidden information. Based on video compression, may be divided into two primary domains: uncompressed and compressed video domains, as illustrated in *Fig. 2*. It may also be divided into spatial and frequency domains[18]. Uncompressed video steganography has received a lot of attention; nevertheless, it is less resistant to compression, noise augmentation, and decryption and has a smaller payload capacity. Additionally, uncompressed video steganography is unable to profit from the digital cover being employed, and suitable preprocesses might be added to secret messages to increase the steganography's security and resilience. As a result, the researcher's primary area of interest is video steganography across a compressed domain. Medical, military, or intelligence communications, personal information systems, and many more industries need information confidentiality to avoid unauthorized access[19]. IoT systems are becoming more prevalent in the area of transferring digital data, where each system is made to provide a certain function. The information gathered at the perception layer determines how the services are delivered. It is the $IoT's$ lowest layer. Devices with limited resources or wireless sensor networks (WSNs) make up the perception layer. The majority of these devices employs wireless media for transmission and is widely used. These devices are vulnerable to node manipulation due to open deployment. A wireless signal may also be intercepted and the information being delivered altered relatively easily. Information security is crucial because services are crucial, and if the information is intercepted or altered, there might be significant financial and human losses.

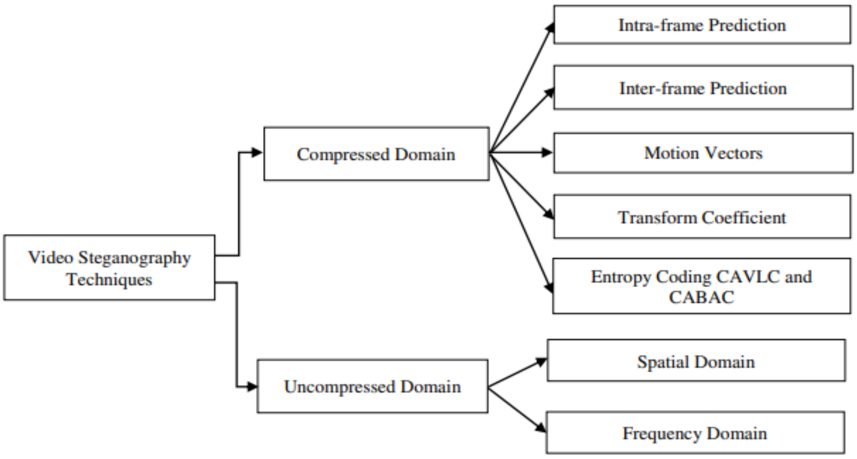

FIG. 2. VIDEO STEGANOGRAPHY TECHNIQUES [20].

According to Symantec's Internet Security Threat Report (ISTR) 2019[21]; In December 2018, there were over 4 million crypto-jacking attacks, and around 4800 websites were infected with form-jacking attacks. Attacks on IoT devices were mostly caused by worms and bots. Ronen et al. [22] proof of concept attacks on IoT devices show how vulnerable they are. S.TVs, smart tablets, light bulbs, and other IoT devices may all be attacked using these vulnerabilities by knowledgeable

Received 15/January/2023; Accepted 21/February/2023

DOI: https://doi.org/10.33103/uot.ijccce.23.3.12

hackers. The ability for secure communication between sender and recipient is therefore made possible by the efficient use of video steganography in several sectors. The following section has described the various steganography methods in both compressed and uncompressed domains.

A. Video Steganography in the Compressed Domain

Data compression is crucial for the transmission and storage of digital information from a sender to a receiver in the modern day, particularly when improving visual quality. While data is being sent over the network, it speeds things up and uses less memory. The majority of applications that permit compressed video profit from its advantages as well. Moving Picture Experts Group (MPEG-1, 2, and 4), Advanced Video Coding (AVC), also known as H.264, and High-Efficiency Video Coding (HEVC), also known as the H.265 video codec, are only a few of the coding standards that may be used to compress video. With the improvement in hiding capacity, similarity, and resilience, video steganography takes use of this compression to hide sensitive information[19]. There are different techniques of video steganography in the compressed domain; they are intra-frame prediction, inter-frame prediction, motion vector estimation, transform coefficients, and entropy coding[23]. In the compressed domain, these techniques have a few Characteristics and limitations that are listed in Table II.

TABLE II. CHARACTERISTICS AND LIMITATIONS OF DATA CONCEALING IN A COMPRESSED DOMAIN [19]

Venues for data hiding	Characteristics	Limitations
Intra frame prediction	The computational complexity is moderate	Low embedding capacity has a significant negative influence on video quality.
Inter-frame prediction	There is little impact on computational complexity and video quality.	The ability to embed is constrained.
Motion vectors	The difficulty of the calculation and the embedding payload is modest.	The effect on video quality is significant.
Transform coefficients	Obtain both a low computational complexity and a large embedding payload.	The influence on the video quality is high
Entropy coding	Obtain both a low computational complexity and a large embedding payload.	The steganogram's quality is substantially altered.

There are various compressed domain-based video steganography techniques. The benefits and drawbacks of these techniques are outlined in Table III. J. Yang et L. [24] suggested the most modern method of video steganography employing very effective video coding (HEVC). For the HEVC procedure, this method uses motion vector space encoding. A technique for concealing and retrieving data in high-resolution videos compressed with the HEVC standard was given by D. Rodríguez et al. [25]. The method is based on altering certain blocks' luminance. Information is randomly inserted; the receiver must be aware of the locations to retrieve the information. Results indicate that after embedding the message, it is feasible to extract all the information while preserving the video's quality. S. Liu and D. Xu [26] demonstrated a reliable HEVC-based secret sharing-based video steganography technique. A 4 by 4 luminance DST block contained the secret message that had been encoded through threshold secret sharing. T. Rabie et al. [27] introduced a new video steganography method based on the idea of a pixogram for high-payload steganography. By examining the temporal changes that occur at the pixel level between frames of a video clip, the pixogram offers a fresh viewpoint. Simply put, a pixogram can maximize the redundant area suitable for hiding in the transform domain by converting highly uncorrelated spatial areas of individual frames of a video scene into highly correlated temporal segments by utilizing the temporal correlation between the frames of the same scene in a given video segment. R. Sangeetha et al. [28] offered a revolutionary video steganography that converts the pixel value to the frequency domain using the Fast Fourier Transform and is based on a non-dynamic section from the secret frame (FFT). The random Least

Received 15/January/2023; Accepted 21/February/2023

DOI: https://doi.org/10.33103/uot.ijccce.23.3.12

Significant Bit (LSB) of the FFT component is employed as a carrier object for high-quality video and concealed data-carrying capacity.

TABLE III. ADVANTAGES AND DISADVANTAGES TECHNIQUES IN THE COMPRESSED DOMAIN

Ref.	Year	Technique used	Secret message	Advantages	Disadvantages
Ref.[24]	2018	Motion vector	Text	- Under comparable motion vectors, embedding capacity is greater than LSB, but under identical carriers, embedding capacity is lower than LSB. -The PSNR is varying from 30 to 41.50 db.	- By choosing carrier objects with good security, PSNR value, and high robustness may be improved.
Ref.[25]	2018	- HEVC	Text	–HM-16.2 and x265 encoding software both retain the quality of Full HD and 4K videos.	- Although the insertion blocks are picked at random, numerous tests need to be run to determine the robustness of the method against steg-analysis assaults.
Ref.[26]	2020	-DST - Secret sharing scheme	Text	- Based on H.265/HEVC codec. -The average Bit Error Rate (BER) is between 20.41% and 22.59%, with the PSNR value fluctuating between 34.4 and 46.38 dB. -It shows robustness.	-This approach can stop the intra-frame distortion drift. However, there is a need to take into account the inter-frame distortion drift caused by video steganography.
Ref.[27]	2019	-DCT Pixogram concept	Video	- Strong robustness. - High embedding capacity. - High imperceptibility. - Acceptable performance against temporal-based attacks.	- The proposed method having trouble fending off compression attacks.
Ref.[28]	2022	-FFT -LSB	Image	- High embedding capacity. - High imperceptibility. - Based on H.264 codec. -Good robustness.	- FFT is a complex transform - It is necessary to improve PSNR and robustness by choosing well-secured carrier objects.

B. Video Steganography in Uncompressed Domain

Contrary to compressed video, raw video steganographic techniques work with the video as a series of identically formatted frames. In order to hide the secret information, the digital video must first be transformed into frames that may be utilized as still photos. All of the frames are combined to create the stego video after the embedding procedure. Raw video steganographic techniques consist of spatial and transform/temporal/frequency domains [29] as seen in *Fig. 3*. Table IV shows advantages and disadvantages for each domain.

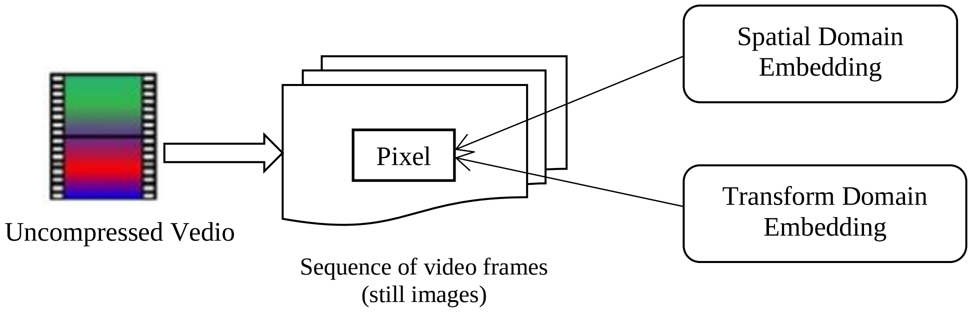
Spatial Domain Embedding
Pixel
Transform Domain Embedding
Uncompressed Vedio
Sequence of video frames (still images)

FIG. 3. VIDEO STEGANOGRAPHY IN UNCOMPRESSED (ROW) DOMAIN[19].

Received 15/January/2023; Accepted 21/February/2023

DOI: https://doi.org/10.33103/uot.ijccce.23.3.12

TABLE IV. ADVANTAGES AND DISADVANTAGES OF SPATIAL AND FREQUENCY DOMAIN [20]

Domain	Advantages	Disadvantages
Spatial	-No need for pre-processing Less computation time	- Highly affected by noise factor
Frequency	- Frequency with high capacity - Less sensitive to noise more reliable	-Pre-processing is necessary. - It’s complex, and it has less capacity than spatial domain approaches.

1. Spatial Domain Techniques

The secret message is instantaneously hidden utilizing pixel intensities in the spatial domain approach. Numerous steganographic methods have been used in the spatial realm. such as histogram manipulation, spread spectrum, area of interest (ROI), LSB replacement, pixel value differencing (PVD), most significant bit (MSB), and quantization index modulation (QIM)[23], matrix encoding with bit-plane complexity segmentation (BPCS) [30]. The lowest bit in a string of binary numbers is known as the LSB, or least significant bit, and it is located to the string's extreme right. The LSB technique is used to replace a few LSBs of pixels from the cover video with the secret message bits, making the changes invisible to the human eye.[31]. PVD uses the difference value between two adjacent pixels in a block to determine how many secret bits should be embedded. MSB also known as the high-order bit is the highest value in a binary number. Here, data is concealed using MSB. The hidden message is disseminated via the spread spectrum technique throughout the sound file's frequency spectrum, which is separate from the actual file[23]. These techniques have been used by several researchers to achieve spatial video steganography on various images. Additionally, their experimental findings demonstrate the effectiveness of video steganography as determined by many qualitative parameters[30]. There are several specified related works of spatial video steganography techniques and Table V. lists the advantages and disadvantages of each of them.

To increase the effectiveness of the embedding process with minimal distortion, M. Rani et al. [32] developed a novel video steganographic approach based on the Mid-point circle algorithm with the LSB methodology. According to M. Hashemzadeh [33], a video steganography technique that works should be built on the dynamic and conspicuous areas of a cover video. Based on motion clues from the feature points, his method locates the dynamic regions, from which the regions of interest are derived. He hid the secret data in the appropriate places using the LSB replacement approach. K. Rajalakshmi et al. [34] suggested a novel approach for video steganography called Zero Level Binary Mapping (ZLBM). The cover video is first converted into frames in their suggested procedure. The FAMF method is then used to remove the impulse noise from the frames. Then, it groups the pixels inside the improved frames using the block-wise pixel grouping technique. Finally, it encrypts the secret data using the patch-wise code generation approach and embeds it using the ZLBM method. S. Abed et al. [35] proposed a method of video steganography to increase the security of sensitive information without compromising the reliability and capacity of the videos. The AES algorithm is used to encrypt the secret data on the first level, which renders the data unreadable. A field-programmable gate array (FPGA) hardware is used in the second level, to make the data invisible. The LSB scheme is utilized to preserve noticeably high frame imperceptibility. The randomization system used in this work chooses the video frames used as cover files at random. The data is dispersed among the video frames as a result of the randomization process, making it difficult to retrieve the data in its original sequence without the right key. A novel method for video steganography based on the corner point concept and the LSBs algorithm was proposed by R. Mstafa et al. [36] . The Shi-Tomasi method is first used to find areas with corner points inside the cover video frames. Then, it employs the 4-LSBs method to conceal private information inside the noted corner spots. Additionally, to increase security, the suggested approach encrypts sensitive data using Arnold's cat

Received 15/January/2023; Accepted 21/February/2023

DOI: https://doi.org/10.33103/uot.ijccce.23.3.12

map prior to embedding. By combining a number of techniques, S. Dhawan et al. [37] developed a technique for picture steganography that employs image encryption based on binary bit-plane decomposition (BBPD) to increase the security of the secret data. The Salp Swarm Optimization Algorithm (SSOA)-based adaptive embedding technique is then recommended in order to increase the payload capacity by modifying the parameters of the steganographic embedding function for edge and smooth blocks. The SSOA approach is successfully used in this instance to identify the edge and smooth blocks. Then, a hybrid fuzzy neural network with a backpropagation learning method is employed to enhance the quality of the stego images. These Stego images are then sent to the target utilizing an extremely secure IoT protocol. M. Khari et al. [2] developed a data security method based on the elliptic Galois cryptography (EGC) protocol to ward against data eavesdropping while being sent over an IoT network. Utilizing encryption technology, confidential data collected from multiple medical sources is encrypted. After that, the encrypted data is Matrix XOR encoded and integrated into a low-complexity image (a transformed frame for the H.264/AVC movie). The suggested method additionally employs Adaptive Firefly, an optimization technique, to optimize the selection of cover blocks within the image. A system was suggested by R. Sangeetha et al. [37] to provide a reliable, effective way to protect data from hackers and send it securely to the intended location. The data is considerably guarded by hiding images and text inside video and audio files, merging them into a stego file at the sender's end, and then using facial authentication at the receiver's end to cross-check the security parameter by approving the recipient. The movie successfully preserves the secret text information and analyses the audio file with an emphasis on secret text extraction.

TABLE V. ADVANTAGE AND DISADVANTAGES ANALYSIS OF DIFFERENT TECHNIQUES IN THE SPATIAL DOMAIN

Ref.	Year	Technique used	Secret message	Advantages	Disadvantages
Ref.[32]	2018	-Mid-point circle LSB	Text	-Highest PSNR value is 82.0468. -High embedding capacity. -Preserve video quality.	-
Ref.[33]	2018	-LSB	Text	- High embedding capacity. - High imperceptibility.	- Cover video without moving objects or areas cannot be utilized with this strategy. The high-motion and extremely dynamic videos were far more beneficial for the suggested method, the data indicated.
Ref.[34]	2018	- ZLBM - Fuzzy Adaptive Median Filtering	Text	- Provide high security. - Lessen the difficulty of embedding videos.	- Difficulty in guaranteeing a good trade-off between imperceptibility and robustness.
Ref.[35]	2019	-LSB	Text	-High imperceptibility -High PSNR and SNR, and low MSE.	- To increase processing speed, the randomization mechanism might be shifted from the software module to the hardware module. - For improved performance, the FPGA implementation may be expanded to incorporate other LSB techniques.
Ref.[2]	2019	-CNN -XOR	Text	- Perform better in terms of embedding effectiveness, carrier capacity, PSNR, MSE, and time complexity.	- Complex and difficult to implement. - Increase the size of the encrypted message.
Ref.[36]	2020	-Shi-Tomasi algorithm -4-LSBs	Image	- Acceptable embedding capacity. - High resistance against a variety of assaults. - High imperceptibility.	- By utilizing one of the public keys available in cryptography, the level of security may be increased instead of using Arnold's cat map method.
Ref.[37]	2021	-LSB	Text Image	- Offers a reliable, effective solution for protecting data.	- The color components of pixels may be significantly changed by the LSB Insertion.

Received 15/January/2023; Accepted 21/February/2023

DOI: https://doi.org/10.33103/uot.ijccce.23.3.12

In general, the majority of LSB techniques did not rely on picture content or pixel correlation. As a result, it may be located via RS analysis. Therefore, several safety measures are required to improve the security of LSB-based steganography algorithms. The LSB-based steganography technique contains an edge detection step to address this problem. The secret photographs should also be encrypted before being included in the cover image to further security. The degree of security of numerous modern systems has been reduced since encryption methods weren't there before the embedding phase.

2. Transform Domain Techniques

The transform domain-based video steganography approach involves converting still pictures from one spatial domain into another using the correct transform coefficients, for instance, discrete sine transform (DST), discrete cosine transform (DCT), discrete Fourier transform (DFT), discrete wavelet transform (DWT), and discrete curvelet transforms (CvT). The transform coefficients' low, medium, or high frequencies are employed to obfuscate the private information. Despite the high complexity level of the approaches utilized in the changed area, they provide resilience against numerous threats, increasing security. The private data is translated into the frequency domain using transform coefficients before being embedded. After the embedding procedure is finished, the modified coefficients are once again changed using an inverse transformation to produce a stego video[19]. Following is a discussion of the last studies on video steganography utilizing transformed coefficients in an uncompressed domain and Table VI lists the advantages and disadvantages of each of them:

S. Kumar et al. [38] proposed an algorithm for concealing the secret text beneath the cover multimedia video file. Additionally, find out the all operation parameter methods such as capacity, bitrate (BR), PSNR, correlation (CR), MSE, and histogram. Additionally, they employed different-2 cover video files or image files, as well as studies, to get the best results according to capacity and execution matrix. M. Suresh et al. [39] introduced a novel method for video steganography based on DCT-based random integer generation. The recommended approach finds the carrier frames by using scene change detection. The scene change is recognized by the DCT coefficients' inter-frame variation. Once the carrier frame has been located, it is divided into sub-images. The threshold value is utilized in place of the eight least significant DCT coefficients for computing the sub-images DCT coefficients. Depending on the sensitive information that has to be hidden, the threshold number might be either 0 or 1. Where the private data will be put is determined by the generated random number. To boost security, the private data is mixed up using a randomly generated integer. M. Ramalingama et al. [40] suggested a video steganography method based on an integer wavelet transform (IWT) To hide the secret data. The technique demonstrated fewer channel bit errors and used affine modifications for steganography. The hidden information is stored in the video frames' IWT coefficients. The pixels are spread via an affine modification during embedding. The suggested approach has been tried on a variety of input data, and both quantitative and qualitative evaluations have been made of its performance. M. Dalal et al. [41] introduced a technique for video steganography that uses DWT for embedding and multiple-moving object identification. The DWT program was used to transform the moving objects using a biorthogonal wavelet filter. SIT (Secure IoT), a simple technique for hidden picture encoding and decoding, was used. The middle-frequency sub-bands Y (luminous) component included the encrypted secret image. Before embedding, the secret data is also divided into four sub-bands using DWT. The proposed approach is tested on several video sequences by comparing subjective and objective measurements.

Received 15/January/2023; Accepted 21/February/2023

DOI: https://doi.org/10.33103/uot.ijccce.23.3.12

TABLE VI. ADVANTAGE AND DISADVANTAGES O OF DIFFERENT TECHNIQUES IN THE TRANSFORM DOMAIN

Ref.	Year	Technique used	Advantages	Disadvantages
Ref.[38]	2018	DWT	- High quality. - High PSNR and low MSE. - High hiding information payload.	- The security should be improved because it is not resisting all security attacks.
Ref.[39]	2018	DCT	- Ensure more security. -Low BER and high PSNR of more than 36db. - Good video quality and can withstand attacks.	-To secure communication, the video characteristics should be developed
Ref.[40]	2020	Affine transformation	- Compared to existing approaches, assure undetectable aberrations with little computing expense.	- With little computational cost in terms of the PSNR factor, the improved capacity may guarantee imperceptible distortions.
Ref.[41]	2021	DWT	- Improves great robustness, security, and imperceptibility.	- The most recent frequency domain methods may be used with other techniques and fields, such as computer vision, to create greater resilience and security.

VI. JOINT CRYPTO-STEGO SCHEMES

Utilizing the steganography method alone is "less secure" in comparison to the combined approach since including cryptography improves the security of the data. Because the hidden data is vulnerable to hacking and manipulation once the steganographic pattern is disclosed to the unintended user. To safeguard the data produced by *IoT* devices, several methods and strategies have been developed. We have shown a variety of modern security methods and strategies that combine cryptography with steganography in the section below. *Fig. 4* illustrates a scheme for combining the two methods and Table VII lists the advantages and disadvantages of each of them. Y. Yao et al. [43] developed an approach that successfully masks H.264/AVC video bit stream data. Video encryption, data embedding in the encrypted video, data extraction, and video recovery are the three elements of the technique. In order to protect the privacy of the video content, the intra-prediction mode code words, motion vector variation, and partial coefficients were encrypted during the encryption stage without reducing the video's bit rate. The specified video bit stream was completely recovered once the receiver decoded the encrypted video bit stream and deleted the hidden data. A combined security strategy based on encryption, steganography, and watermarking methods was developed by Abdur et al. [44], It broke down into three phases. The proposed approach included three steps. XOR to the right rotates pixel bits were used for the initial step of encryption. The second stage of steganography then included replacing bits of the encrypted image with LSBs from the cover image. The third step concluded with time and frequency domain watermarking. To embed information into the gray scale image, J. Bhadra et al. [45] devised and used a computation that makes use of the elliptic bent encryption method to encode the data.

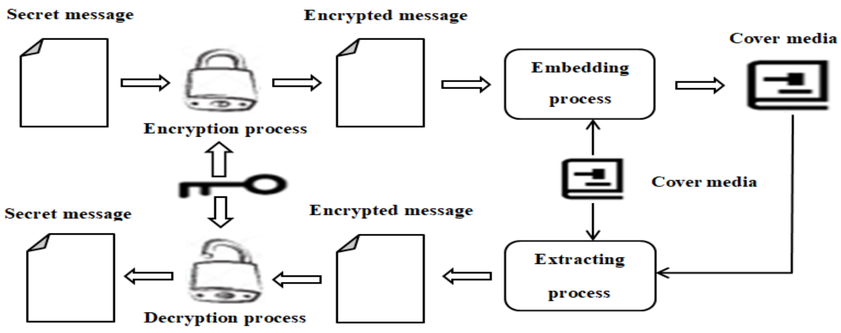

FIG. 4. BASIC DIAGRAM OF JOINT STEGANOGRAPHY AND CRYPTOGRAPHY [42].

Received 15/January/2023; Accepted 21/February/2023

DOI: https://doi.org/10.33103/uot.ijccce.23.3.12

R. Das [46] proposed a security model for securing data between IoT devices and clouds. Data transit between an IoT device and a home server is initially secured then, between the home server and the clouds using a combination method of lightweight cryptography and steganography. S. Manisha [47] proposes a novel data-hiding method that may be used to embed a covert image into one of the frames of an AVI video. Before and after the secret data has been encrypted, neither the quality of the embedded secret image nor the size of the video has changed. Any multimedia data that may be further retrieved and identified may be included in the hidden image. S. Kamil et al. [48] suggested a data-hiding technique that is lightweight and optimized. This technique consists of two phases. First data was encrypted using the lightweight BORON cipher, which only used less RAM than more conventional algorithms like 3DES and AES. Second, to achieve minimum variability, the encrypted data is concealed in either the complemented or un-complemented form. The results showed that the AES algorithm's avalanche effect may be closely matched by the small-footprint BORON cipher. In addition, the PSNR value has significantly improved over the GA optimization process.

Video steganography based on the ROI in human vision combined with a face identification algorithm in the medical imaging system is presented by S. Balu [49]. The selected frame in a video is used to compute the motion attention index value and variation range; the human vision area of interest is picked based on the resulting value. To find moving objects in a video, a face detection method is then used. Other than the foreground items' face region, secret information is concealed in the background object. Y. Liu et al. [50] presented a fresh and reliable method for video steganography using a scheme based on the H.265/High-efficiency video coding. They used three prediction directions to manage the intra-frame deformation drift. Their suggested approach encrypts sensitive data before embedding using the BCH coding technique. The encrypted secret data was then implanted. The selected four-by-four discrete sine transform blocks that fulfill the groups have many coefficients. M. Kaur et al. [51] a solution for video steganography that might provide sufficient security during data transmission from the source to the destination was proposed. The suggested approach involves two steps: coding and decoding. Use the DWT domain to compress a set of randomly chosen frames. Then convert a secret image to binary representation and embedding into video frames. Bit-exoring is used to embed the hidden image within compressed frames. To enhance the ability to embed H.264/AVC video sequences based on quantized discrete cosine transform (QDCT), Nguyen et al. [52] created a novel steganography technique. The QDCT coefficients were split into two different clusters in the proposed scheme: concealing clusters and preventing clusters. Zainab et al. [53] developed an approach to boost security by combining two crucial techniques—steganography and encryption. The secret image was encrypted using the Vernam Cryptography technique before being embedded in the cover image. The pseudorandom key determines how resilient this technique is. Therefore, a nonlinear feedback shift register is used to create the pseudo-random key (Geffe Generator). Z. Younus [54] offered a method based on the LSB and modified Knight Tour (KTA) algorithm for hiding data in a movie. The key components of secret communications are encrypted using this procedure. Then, random pixel selection inside the frame was performed using the knight tour method. Then, using the LSB method, the secret message was encoded and inserted in bits (7 and 8) in the selected pixels. A. Basahel et al. [55] presented an LSB-based method for image steganography. Additionally, a brand-new approach to constructing an encryption key that has been broken down into four parts and may be utilized to build a highly intricate distribution of a hidden message within the cover image has been proposed. Additionally, a mobile application for the suggested approach has been developed and offered by this study so that any user may exchange incredibly sensitive data without worrying about a possible assault. A successful HD and SD video steganography method was proposed by M. Dalal et al. [56]. By using just the luminance (Y) component, this technique makes advantage of DWT to insert the hidden

Received 15/January/2023; Accepted 21/February/2023

DOI: https://doi.org/10.33103/uot.ijccce.23.3.12

message inside the video frames. By pre-encrypting the secret message, the recommended technique is made more secure. The embedding process is carried out after the video frames are split into 16 sub-bands using second-level 2-D DWT. C. Biswas et al. [57] presented the image steganography technique based on LSB. In this technique, a hybrid of cryptography and steganography provides more security. To verify the message's integrity, a hash value is created for it. J. Kuri et al. [58] suggested a cryptography method used to encrypt confidential information obtained from various medical sources. The encrypted information is then hidden in a sometimes complicated image using the Matrix XOR coding Steganography method. The proposed study also makes use of a modification of the Firefly optimization technique to enhance the selection of canopy blocks in the image. To guarantee data integrity and privacy, J. Vivek et al. [59] suggested video stenography for real-time applications based on video compression techniques and a chaotic approach with improved mapping. D. Gurumoorthy et al. [60] offer a recommended image encryption method based on elliptic Galois cryptography (EGC), and the encrypted data is then inserted into a square image using the steganography method Matrix XOR encoding. The suggested technique additionally employs an optimization algorithm to choose the cover blocks most effectively from the image. H. Khalid et al. [61] presented a novel encryption technique for crucial messages transmitted by IoT apps. The suggested approach offers secret communication four degrees of protection. Applying Conformal Mapping to the secret image creates a representation of the first level. The first level's output is encoded to represent the second level, and the cover image is used to conceal the message at the third level. The last degree of protection is stego image compression.

TABLE VII. ADVANTAGE AND DISADVANTAGES OF DIFFERENT CRYPTO-STENO TECHNIQUES

Ref.	Year	Techniques used	Secret message	Cover	Advantages	Disadvantages
Ref.[43]	2016	- Intra-prediction -Motion vectors - QDCT coefficients -Histogram shifting	Text	Video	- High embedding capacity. - High quality. - The highest SSIM is 0.9680 and PSNR is 37.26.	- It has been challenging to identify the optimum QDCT version for reversible video data that offers great visual quality and compression efficiency at an anticipated embedding rate.
Ref.[44]	2017	-Exclusive OR -LSB - Watermarking in time and frequency domain	Image	Image	- Efficient, simpler, and secure; it provides significant security against threats and attacks.	-High processing time
Ref.[45]	2017	-ECC -LSB	Text	Image	- Good embedding capacity and security with a little decrease in PSNR value.	-It holds good if the key size is not very large. -High processing time
Ref.[46]	2017	- DES, XOR -Digest5 (MD5) -Variable LSB Substitution.	Text	Image	- High security - High quality	- High processing time
Ref.[47]	2018	- Adaptive LSB -Randomized Encoding	Image	Video	- PSNR is 60.035 with Low MSE. - High level of security - High correlation.	--

Received 15/January/2023; Accepted 21/February/2023

DOI: https://doi.org/10.33103/uot.ijccce.23.3.12

Ref.[48]	2018	-BORON cipher	Text	Video	- It could have an avalanche effect similar to what the AES algorithm has. - Good PSNR value.	-The examination of SIM and BER reveals that noise has a significant impact on the spatial domain. As a result, could use error-correcting code.
Ref.[49]	2018	- Face Detection algorithm -AES	Text	Video	-Verified confidentiality, integrity, and authenticity. - Good embedding capacity and quality. - High PSNR with low MSE.	- High processing time
Ref.[50]	2018	- BCH code technique	Text	Video	- Greater robustness. - Better visual quality. - High embedding capacity.	-Future research must still take into account the motion vector's inter-distortion drift (the temporal domain).
Ref.[51]	2018	- LSB - DWT	Image	Video	- High PSNR with low MSE - Good embedding capacity, security, and imperceptibility. -High Correlation.	-For some kinds of analysis and measurements, DWT accuracy may not be sufficient.
Ref.[52]	2019	- QDCT coefficients. - Hiding cluster.	Text	Video	- Better embedding performance. - The Stego video's excellent visual quality.	- Restoring the original video sequences is not a function of the QDCT approach.
Ref.[53]	2019	-Vernam cipher algorithm -Hybrid Sobel and Kirch edge detector -LSB	Image	Image	- High PSNR with low MSE. - Better quality. -Better hiding capacity.	- It uses only gray image
Ref.[54]	2019	- KTA -LSB	Text	Video	- High PSNR with low MSE. -High Correlation	- It may use a key, which stands for a collection of arbitrary values, to pick frames and embed audio or video files.
Ref.[55]	2019	-DES -LSB	Text	Image	-Very strong and resistant to attacks. -High correlation. -High PSNR and low MSE	- Low payload - Not resistant to compressing because it depends on the LSB -Cause some insensitive noise.
Ref.[56]	2019	-DWT	Image	Video	- High robustness as a result of the defense against noise assaults. - High PSNR and low MSE.	- Security has to be strengthened since not all security threats are being thwarted.
Ref.[57]	2019	-AES -LSB -Hash	Text	Image	- Provide confidentiality, integrity, and authentication together.	- Long processing times, making it unsuitable for Internet of Things applications.
Ref.[58]	2020	- Proposed EGC - Adaptive firefly	Text	Image	- Good robustness. - Time complexity is very Low. - High PSNR (70) and low MSE (0.02). - Employ H.264/AVC video.	--

DOI: https://doi.org/10.33103/uot.ijccce.23.3.12

Ref.[59]	2021	- HEVC - Chaos technique -LSB	Video	Video	- Fast encoding and less computation time.	- limited number of video sequences as input(8-secret frames)
Ref.[60]	2022	-EGC -XOR - Adaptive firefly	Text	Image	-High levels of data Security. -MSE and time complexity are very low.	- Low payload capacity
Ref.[61]	2022	-RSA - Conformal mapping -LSB	Image	Image	- High level of security - Speed in transferring and receiving the image. - Good PSNR and MSE.	--

VII. COMPUTATIONAL TIME

The use of cryptographic algorithms in steganographic systems increases the security of hidden data. But this security should not make the entropy more visible. The combination of these two technologies will have advantages and disadvantages that can be examined and observed in ROC curves and confusion matrices by steganalysis algorithms. Also, the maximum capacity that can be included in the use and non-use of cryptographic algorithms in steganographic algorithms is another challenge that should be examined considering security vs. capacity. In [63], it was shown that if the cryptographic algorithm changes the size of the original message after encryption operation, its use in steganography algorithms will reduce the capacity of the insert able message. Video steganography has given a higher performance among many factors like imperceptibility, potential, and robustness. A video will be a sequential association of rapid-paced images and audio clips. Thus, it is very hard for attackers to show mystery facts without studying each unmarried body in the video. Analyse the computational complexity of any method, depending on the platform, and CPU. In video steganography the process of message embedding and extraction, the average time consumed per frame is used to evaluate the computational complexity of these three methods. The embedding time and extraction time are calculated by:

$$t_{emb} = T_{emb}/n \tag{1}$$

$$t_{ext} = T_{ext}/n \tag{2}$$

where n is the number of frames in a video, and T_{emb} and T_{ext} refer to the time consumed by message embedding and extraction, respectively. Also, the computational time is related to the video resolution [64].

VIII. ANALYSIS AND UPCOMING WORK

We may draw the following conclusions from the investigation and analysis of the ongoing research in compressed and uncompressed video steganography methods and Joint Crypto-stego Schemes to safeguard the data generated by IoT devices:

- Compressed video steganography uses a format-based methodology. Several methods were developed for a particular video format by leveraging its structure and compression algorithm.

- When utilizing a transform coefficient like DWT to transform the cover object into a frequency domain in uncompressed video steganography, robustness is enhanced. The information pertaining to the alteration of the original value is selected to be hidden by the carrier object to give extra coverage. It does, however, reduce imperceptibility since, when applying an inverse transform, small changes in the converted value have a big impact on the true value. Since it makes noise in the original cover video, hidden information may be found. Additionally, these video steganography approaches still have the hiding capacity. Also, the following suggestions are made, along with some potential future directions for improving video steganography.

Received 15/January/2023; Accepted 21/February/2023

DOI: https://doi.org/10.33103/uot.ijccce.23.3.12

- Develop a method for video steganography that balances robustness, security against different assaults, degree of imperceptibility, and embedding capability for real-time security applications.
- Using the HEVC/H.265 video codec, many video steganography operations may be carried out in a compressed domain. It provides excellent-quality videos that are substantially compressed.
- In video steganography, the ROI, such as object detection and feature detection, may be used to restrict unauthorized access to secret information by employing the whole frame or a specified area of the frame as a carrier object.
- Since transform domain procedures are immune to signal processing and compression, it is possible to shift video steganography from the spatial to the frequency domain using different transform coefficients in a temporal domain.
- The effectiveness of video steganography may be assessed using the steganalysis method.
- The secret message may be hidden by using a variety of regions of interest (ROI) as carrier objects.

IX. CONCLUSIONS

IoT is a new, growing field that has recently caught the attention of scholars. The usage of the internet has also considerably increased during the last several years. The purpose of this review paper is to present a comprehensive review of various video steganography and crypto-stego techniques with their advantages and disadvantages to help the reader understand different video crypto-stego techniques. Some of the existing video steganography approaches still suffer in terms of less security, poor video quality, and complexity. Therefore, it is a necessity to develop efficient video stenographic schemes along with data encryption to improve video imperceptibility, and security with less complexity and should be resistant to different attacks. Steganography and cryptography together enhance each other's weaknesses. Strengthening security and making it more difficult for hackers to access or steal data.

REFERENCES

[1] A. M. Ray, A. Sarkar, A. J. Obaid and S. Pandiaraj, “IoT Security Using Steganography,” *In book: Multidisciplinary Approach to Modern Digital Steganography, Publisher: IGI Gloabl*, Chapter: 9, pp.191-210, June 2021.

[2] J. L. Kuri and M. Rafi, “Securing Data in Internet of Things (IoT) Using Cryptography and Steganography Techniques,” *International Journal for Research in Applied Science & Engineering Technology*, vol. 8, no. 6, July 2020.

[3] A. K. Singh, B. Kumar, S. K. Singh, S. Ghrera and A. Mohan, “Multiple watermarking technique for securing online social network contents using Back Propagation Neural Network,” *Future Generation Computer Systems*, vol. 86, pp. 926–939, Sep. 2018.

[4] A. Jan, S. A. Parah, M. Hussan and B. A. Malik, “Double layer security using crypto-stego techniques: a comprehensive review,” *Health and Technology*, vol. 12, no. 1. pp. 9–31, Oct. 2022.

[5] N. A. Loan, N. N. Hurrah, S. A. Parah, J. W. Lee, J. A. Sheikh et al., “Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption,” *IEEE Access*, vol. 6. pp. 19876–19897, 2018.

[6] R. Biswas, I. Mukherjee and S. K. Bandyopadhyay, “Image feature based high capacity steganographic algorithm,” *Multimed. Tools Appl.*, vol. 78, no. 14, pp. 20019–20036, Jul. 2019.

[7] V. A. Thalor, M. A. Razzaque and M. R. Khandaker, “Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities,” *IEEE Access*, vo.l 9, pp. 28177–28193, January 2021.

[8] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, and S. W. Baik, “Image steganography using uncorrelated color space and its application for security of visual contents in online social networks,” *Futur. Gener. Comput. Syst.*, vol. 86, pp. 951–960, Sep. 2018.

[9] S. Pal and S. K. Bandyopadhyay, “VARIOUS METHODS OF VIDEO STEGANOGRAPHY,” *International Journal of Information Research and Review*, vol. 3, no.6, pp. 2569–2573, 2018.

[10] S. B. Sadkhan and A. O. Salman, “A survey on lightweight-cryptography status and future challenges,” *International Conference on Advances in Sustainable Engineering and Applications, ICASEA 2018 - Proceedings*. pp. 105–108, 2018.

[11] G. Mustafa, M. A. Mirza, A. Jamil, and E. Sciences, “A Review of Data Security and Cryptographic Techniques in IoT based devices,” *Association for Computing Machinery*, vol. 47, pp. 1-9, June 2018.

[12] P. Panahi, C. Bayılmış, U. Çavuşoğlu and S. Kaçar, “Performance Evaluation of Lightweight Encryption Algorithms for IoT‐ Based Applications,” *Arabian Journal for Science and Engineering*, vol. 46, pp. 4015–4037, April 2021.

Received 15/January/2023; Accepted 21/February/2023

DOI: https://doi.org/10.33103/uot.ijccce.23.3.12

[13] J. Patil, G. Bansod, and K. S. Kant, "LiCi: A new ultra-lightweight block cipher," *2017 International Conference on Emerging Trends and Innovation in ICT, ICEI 2017*. pp. 40–45, Jun 2017.

[14] A. Aziz and K. Singh, "Lightweight Security Scheme for Internet of Things," *Wirel. Pers. Commun. An Int. J.*, vol. 104, no. 2, pp. 577–593, Jan. 2019.

[15] K. Wang, C. Chen, W. Fang and T. Wu, Chien-Ming Chen, "On the security of a new ultra-lightweight authentication protocol in IoT environment for RFID tags," *Journal of Supercomputing*, vol.74, no. 8, pp.65-70, 2018.

[16] Z. Liu and H. Seo, "IoT-NUMS: Evaluating NUMS elliptic curve cryptography for IoT platforms," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 3, pp. 720–729, Mar. 2018.

[17] S. Raza and R. M. Magnusson, "TinyIKE: Lightweight IKEv2 for Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 856–866, Feb. 2019.

[18] R. J. Mstafa and K. M. Elleithy, "A video steganography algorithm based on Kanade-Lucas-Tomasi tracking algorithm and error correcting codes," *Multimed. Tools Appl. 2015 7517*, vol. 75, no. 17, pp. 10311–10333, Nov. 2015.

[19] R. Patel, K. Lad, and M. Patel, "Study and investigation of video steganography over uncompressed and compressed domain: a comprehensive review," *Multimedia Systems*, vol. 27, no. 5. pp. 985–1024, 2021.

[20] S. Kamil, M. Ayob, S. Abdullah and Z. Ahmad, "Challenges in Multi Layer Data Security for Video Steganography Revision," *Asia-Pacific Journal of Information Technology and Multimedia*, vol. 7, no. 2-2, pp. 53 – 62, 2018.

[21] "ISTR Internet Security Threat Report ," *Symantec Corporation in United Stated of America*, vol. 24, pp.1-3, 2019.

[22] E. Ronen and A. Shamir, "Extended functionality attacks on IoT devices: The case of smart lights," *Proc. - 2016 IEEE Eur. Symp. Secur. Privacy*, pp. 3–12, May 2016.

[23] A. John and A. Baby, "A Survey on Video Steganography," *International Journal of Science and Research*, vol. 8, no. 4, April 2019.

[24] J. Yang and S. Li, "An efficient information hiding method based on motion vector space encoding for HEVC," *Multimedia Tools and Applications*, vol. 77, no. 10. pp. 11979–12001, 2018.

[25] D. Rodríguez, A. A. Del Barrio, G. Botella and D. Cuesta, "Intra-Steganography: Hiding Data in High-Resolution Videos," *IEEE/ACM 22nd International Symposium on Distributed Simulation and Real-Time Applications*, pp. 1–8, 2018.

[26] S. Liu and D. Xu, "A robust steganography method for HEVC based on secret sharing," *Cognitive Systems Research*, vol. 59. pp. 207–220, 2020.

[27] T. Rabie and M. Baziyad, "The Pixogram: Addressing High Payload Demands for Video Steganography," *IEEE Access*, vol. 7, pp. 21948–21962, 2019.

[28] P. Patel, K. Lad and M. Patel, "FFT-Based Robust Video Steganography over Non-dynamic Region in Compressed Domain," *Part of the Advances in Intelligent Systems and Computing book series (AISC,vol. 1354)*, pp. 93–102, July 2022.

[29] K. Muhammad, M. Sajjad, I. Mehmood and S. Rho, "A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image," Multimedia Tools and Applications, vol. 75, pp. 14867–14893, May 2016.

[30] 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)*,pp. 1-6, 2017.

[31] H. Kaur and J. Rani, "A Survey on different techniques of steganography," *MATEC Web of Conferences*, vol. 57, pp. 1-12, 2016.

[32] M.Rani, S.Lakshmanan and G.Deepalakshmi, "Video Steganography using Mid-Point Circle Algorithm and Spatial Domain Technique," *International Journal of Engineering and Techniques*, vol. 4, no. 1, pp. 98-105, Feb. 2018.

[33] M. Hashemzadeh, "Hiding information in videos using motion clues of feature points," *Computers and Electrical Engineering*, vol. 68. pp. 14–25, 2018.

[34] K. Rajalakshmi and K. Mahesh, "ZLBM: zero level binary mapping technique for video security," *Multimedia Tools and Applications*, vol. 77, no. 11. pp. 13225–13247, 2018.

[35] S. Abed, M. Al-Mutairi, A. Al-Watyan, O. Al-Mutairi, W. Alenizy and A. Al-Noori, "An automated security approach of video steganography-based LSB using FPGA implementation," *Journal of Circuits, Systems and Computers*, vol. 28, no. 5, pp. 1-15, 2019.

[36] R. J. Mstafa, Y. M. Younis, H. I. Hussein and M. Atto, "A New Video Steganography Scheme Based on Shi Tomasi Corner Detector," *IEEE Access*, vo.l 8, pp. 161825–161837, Spt. 2020.

[37] M. P. R. Sangeetha, G.Koteeswari, "Securing Data in IOT using Cryptography & Steganography Techniques." International Journal of Research in Engineering and Science (IJRES), vol. 9, no. 5, pp. 01-05, 2021.

[38] S. K. Yadav and R. K.Bhogal, "An Video Steganography in Spatial, Discrete Wavelet Transform and Integer wavelet domain," *MultimProc-2nd Int. Conf. Intell. Circuits Syst. ICICS 2018*, pp. 265-270, 2018.

[39] M. S. and I. S. Sam, "High Secure Video Steganography Based on Shuffling of Data on Least Significant DCT Coefficients," *International Conference on Intelligent Computing and Control Systems*, pp. 877-882, 2018.

Received 15/January/2023; Accepted 21/February/2023

DOI: https://doi.org/10.33103/uot.ijccce.23.3.12

[40] M. Ramalingama, N. Ashidi, M. Isa, R. Puviarasi, “A secured data hiding using affine transformation in video steganography,” *Procedia Computer Science*, vol. 171, pp.1147-1156, 2020.

[41] M. Dalal and M. Juneja, “A secure and robust video steganography scheme for covert communication in H.264/AVC,” *Multimedia Tools and Applications*, vol. 80, no. 9. pp. 14383–14407, 2021.

[42] M. S. Taha, M. Rahim, S. Lafta, M. M. Hashim and H. M. Alzuabidi, “Combination of Steganography and Cryptography: A short Survey,” International Conference on Sustainable Engineering Techniques, vol. 512, pp. 1-13, 2019.

[43] Y. Yao, W. Zhang and N. Yu, “Inter-frame distortion drift analysis for reversible data hiding in encrypted H. 264/AVC video bitstreams,” Signal Processing, vol. 128, pp. 531-545, Nov. 2016.

[44] M. Abdur, R. Ahmed, M. Adnan, and A. Ahmed, “Digital Image Security: Fusion of Encryption, Steganography and Watermarking,” *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 5. 2017.

[45] J. Bhadra, M. K. Banga, and M. Vinayaka Murthy, “Securing data using elliptic curve cryptography and least significant bit steganography,” *Proceedings of the 2017 International Conference On Smart Technology for Smart Nation, SmartTechCon 2017*. pp. 1460–1466, 2018.

[46] R. Das and P. Chatterjee, “Securing Data Transfer in IoT Employing an Integrated Approach of Cryptography & Steganography,” *Association for Computing Machinery*, pp. 17-22, March 2017.

[47] S. Manisha and T. S. Sharmila, “A two-level secure data hiding algorithm for video steganography,” *Multidimensional Systems and Signal Processing*, vol. 30, pp. 529–542, March 2018.

[48] S. Kamil, M. Ayob, S. N. Sheikh and Z. Ahmad, “Lightweight and Optimized Multi-Layer Data Hiding using Video Steganography,” *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 12, pp. 256-262, 2018.

[49] S. Balu, C. K. Babu and K. Amudha, “Secure and efficient data transmission by video steganography in medical imaging system,” *Cluster Computing*, vol. 22, pp. 4057–4063, 2018.

[50] Y. Liu, H. Zhao, C. Feng and S. Liu, “A Robust and Improved Visual Quality Data Hiding Method for HEVC,” *IEEE Access*, vol. 6, pp. 53984_53996, August 2018.

[51] P. Parmar and D. Sanghani, “Enhancement of data security using video steganography,” *International Journal of Computer Applications*, vol. 181, pp. 34–38, 2018.

[52] D. C. Nguyen, T. S. Nguyen, F. R. Hsu, and H. Y. Hsien, *“A novel steganography scheme for video H.264/AVC without distortion drift,” Multimedia Tools and Applications,* vol. 78, no. 12, pp. 16033–16052, 2019.

[53] Z. F. Yaseen and A. A. Kareem, “Image Steganography Based on Hybrid Edge Detector to Hide Encrypted Image using Vernam Algorithm,” *SCCS 2019 - 2019 2nd Scientific Conference of Computer Sciences*. pp. 75–80, 2019.

[54] Z. S. Younus and G. T. Younus, “Video Steganography Using Knight Tour Algorithm and LSB Method for Encrypted Data,” *Journal of Intelligent Systems*, vol. 29, n0.1, pp. 1216-1225, Feb. 2019.

[55] A. Sen, A. M. Basahe and Mohammad Yamin, “Enhancing Security of Transmitted Data by Improved Steganography Method,” *International Journal of Computer Science and Network Security*, vol.19, no.4, pp. 239-244, 2019.

[56] M. D. and M. Juneja, “A robust and imperceptible steganography technique for SD and HD videos,” *Multimedia Tools and Applications*, vol. 78, no. 5, pp. 5769-5789, 2019.

[57] H. Shah, P. Oza and S. Agrawal, “Data Encryption Approach Using Hybrid Cryptography and Steganography with Combination of Block Ciphers,” *Part of the Communications in Computer and Information Science book series*, vol. 1760, pp 59–69, 2022.

[58] M. Rekha, S. Rajeswari and V. B. Murthy, “Securing Data in Internet of Things (iot) using Cryptography and Steganography Techniques,” *Journal of Engineering Sciences*, vol. 13, no. 8, pp. 1431-1435, 2022.

[59] J. Vivek and B. Gadgay, “Video Steganography Using Chaos Encryption Algorithm with High Efficiency Video Coding for Data Hiding,” *International Journal of Intelligent Engineering and Systems*, vol.14, no.5, pp.15-24, March 2021.

[60] D. Madhu, M. Priyadharshini, B. Rahulchand, S. Nagaphanisri and G. Ranjitkumar, “SECURING DATA IN INTERNET OF THINGS (IOT) USING CRYPTOGRAPHY AND STEGANOGRAPHY TECHNIQUES,” *International Journal of Creative Research Thoughts*, vol. 10, no. 4, pp. 897-902, 2022.

[61] W. A. Alawsi, H. K. Obayes and S. M. Hussain, “A Novel Image Encryption Approach for IoT Applications,” *Webology*, vol. 19, no 1, Jun. 2022.

[62] F. Djebbar, “Securing iot data using steganography: A practical implementation approach,” *Electron*, vol. 10, no. 21, 2021.

[63] A. Hadipour and R. Afifi “Advantages and disadvantages of using cryptography in steganography*”, IEEE Xplore, International ISC Conference on Information Security and Cryptology,* Iran University of Science and Technology, 2020.

[64] P. Fan, H. Zhang and X. Zhao, “Robust video steganography for social media sharing based on principal component analysis”, *EURASIP Journal on Information Security,* vol. 2022, no. 4, pp. 1-19, 2022.

Received 15/January/2023; Accepted 21/February/2023