[1]Bilal A. Ozturk

[2] Heba Emad Namiq

[3]Fitian shafeeq

[4]Anas atef Shamaileh

[5]Hayder Mohammedqasim

[6]Milind Eknath Rane

Independent Video Steganalysis Framework Perspective of Secure Video Processing

Abstract: We have designed an algorithm of cross-domain feature set extraction for cross-domain video steganalysis of video steganography in multiple domains. For video steganography, we implemented the recently proposed steganography methods such as PMs, MVs, and IPMs. The outcomes of these techniques have fed as input to the proposed Steganalysis approach. We have designed a cross-domain technique for Steganalysis in which the global feature set is extracted according to common statistical properties. After the extraction of global features, the domain-specific features have been extracted in the local features set. Both global and local features are set to form the cross-domain steganalysis technique. The classification has been performed by using the conventional machine learning classifiers such as Support Vector Machine (SVM) and Artificial Neural Network (ANN).

Keywords: Support Vector Machine, Artificial Neural Network, steganography methods, algorithm of cross-domain feature.

I. INTRODUCTION *(HEADING 1)*

Video Steganography is a method that conceals data into a constructing video file. Video steganography is more appropriate than multimedia files, because of its dimension and memory conditions. In video steganography, a digital video contains a set of frames that are cooperating back at convinced frame rates depending on the video standards. Video steganography conceals the information in some individual frames. After covering, it is very hard to inspect in which frame the records or information is hidden. Steganography is the video method that is separated into two important processes. The first one is embedding the data in raw video. The next one is trying to embed data straight in a trodden video stream. In video steganography, various plans are employed. The best method is to conceal the covert information without reducing the aspects of the cover video so that it failed to find out through naked eyes. The embedded video is recognized as the “stego” video which is dispatched to the customer region by the dispatcher. Recently, steganography techniques have revealed extensive success in image processing for hiding the secret message and making it complicated for attackers to find the occurrence of messages. But, the lack of embedded payload using reversible method remains a demanding task to maintain robustness on code streams in low prediction-error environments. The reversible methods produce the code streams with low capacity secret data leading to higher prediction errors.

After the video steganography, the perceptive who has the option to eavesdrop and examine the carrier article and who is additionally attempting to identify the presence of the mysterious message is called steganalyzer and this cycle is called steganalysis. The objective of the steganalysis cycle is to recognize stego from cover. In digital steganography, the message carrier article can be of any digital medium like picture, sound, video,

[1] *Corresponding author: Faculty of Engineering, Software Engineering Department, Istanbul Aydin University. Istanbul. Turkey

[2] College of Science for Women, University of Baghdad

[3]University of information technology and communications

[4] Applied Science Private University, Amman JORDAN

[5]Faculty of Engineering, Istanbul Aydin University, Istanbul, Turkey

[6]Vishwakarma Institute of Technology, Pune

electronic archives, and so on Each digital medium has its benefits. At the point when the information size and the assortment of approaches to implant messages are thought of, video has benefits over others. Notwithstanding these benefits of video, until of late, most of the steganalysis explores have zeroed in on pictures as a result of their prominence, simplicity of execution, and simplicity of sharing them on the Internet. Nonetheless, by an acceleration of the number of Internet clients and headways in systems administration frameworks, the quantity of videos shared online has expanded practically 800% throughout the most recent couple of years. This hazardous development of online video makes it an engaging channel for secretive correspondence utilizing steganography. Subsequently, this reality has attracted more scientists to the space of video steganalysis.

Video steganography can be performed by different types of methods recently across the various domains. The video steganography techniques have been classified according to the approach of hiding secrete messages into the compression pipeline of input cover video. On the receiver side, various video steganalysis techniques have been recently proposed according to embedding domains [12]. The video steganography can be performed effectively using any embedding techniques; however, it is challenging to discover the type of message embedding technique at the receiver end for steganalysis methods [13]. In short, the majority of steganalysis techniques heavily relied on pre-domain information about the steganography method. But this is not a practical solution, the steganalysis should be cross-domain and independent for different kinds of real-time investigations. In this research, we attempt to propose novel steganalysis methods for video steganography of different domains [14]. The steganalysis techniques should be cross-domain and applicable to each type of video steganography mechanism.

II. RELATED WORK

In [1], authors have proposed all inclusive list of capabilities which is fit for distinguishing the video steganography in different spaces. Two famous installing spaces, i.e., partition mode (PM) area and motion vector (MV) area, are considered for steganalysis. The system relies upon the perception that the MVs of the sub-blocks in the equivalent macroblock are generally unique in relation to one another, and they will in general be predictable in qualities after the MV changes or PM alterations.

In [2], authors have proposed a rich model-based MV steganalysis profiting from both worldly and spatial connections of MVs. Their steganalysis technique had significantly unrivaled discovery exactness than the past strategies, even the designated ones.

In [3], steganography was applied by presenting the accompanying commitments. First authors have proposed nover way to deal with track down the most imperceptible inserted MV. Additionally, an original alteration cost work concerning the MVs' intraframe and between outline measurable contrasts previously, then after the fact implanting had proposed for the condition lattice coder. Besides, a pseudo-arbitrary generator had presented for adjusting the game plan of motion vectors which were utilized by the condition lattice coder to work on its proficiency.

In [4], authors have proposed strategy for recognition of H.264 steganographic calculations that balance quantized change coefficients (QTCs) for information stowing away. The in-circle deblocking channel determined in the H.264 standard had utilized for constricting the discontinuities at coded block limits. They performed steganalysis by considering the impact of QTC alteration on separating choices and sifting activities.

In [5], MV-based video steganographic strategy had proposed. For implanting the mysterious piece stream, the installing MVs were chosen for the homogeneous locales of the reference outline. Since homogeneous or smooth areas contain large scale blocks with comparable forecast blunder blocks, it assists with decreasing the shot at discovery by veiling the inserting clamor with comparative expectation mistake among adjoining full scale blocks.

In [6], authors have proposed information stowing away and extraction for Audio Video Interleave videos, which inserts the picture in Bitmap Image File, which has the restricted intel in a casing of the video by dividing the bytes of the mysterious picture and setting them in the video outline giving a more elevated level of encryption.

In [7], authors have proposed a coverless video steganography calculation dependent on semantic division. In particular, to build up the planning connection between restricted intel and video records adequately, they proposed the profound learning dependent on semantic division organization to ascertain the measurable histogram of semantic data.

In [8], authors have proposed general system for building video quantitative steganalyzers that can distinguish the installing of MVs dependent on highlights learned by profound convolutional neural organizations (CNN). They zeroed in on the development of info information lattice for profound CNN and the vigor of the recognition network against various bitrates.

In [9], authors have proposed an original technique to ensure the nearby optimality of changed MVs. To adjust a MV, first and foremost assign a hunt region which comprises of applicant MVs. Second, assess the neighborhood optimality of every MV in the pursuit region to find all nearby ideal ones, from which at long last select the one contributing least to video pressure effectiveness corruption as the changed MV.

In [10], novel secure video steganography dependent on a novel installing procedure had proposed. Video steganography had joined with video encoding. First and foremost, the edge was encoded by a unique encoder and all the significant data was saved. The up-and-comer block was found by the applicable data and planning rules. Then, at that point, each certified square was examined, and a the slightest bit message was implanted during intra-expectation encoding. Finally, if the Intra-Prediction Mode (IPM) of this square had changed, the upsides of the remaining were altered to keep the optimality of the adjusted IPM.

III. Research Motivation

Steganalysis aims to correctly detect the hidden messages into the input stegno video. As per the recent studies, the steganalysis techniques can be classified into two categories such as domain-specific and cross-domain. The domain-specific steganalysis has prior information about the steganographic domain and hence it becomes easier to detect secrete messages. The cross-domain steganalysis technique detects the secrete message without prior knowledge of the steganographic domain. In short, cross-domain techniques perform regardless of the domain of video steganography. The image-based steganography and steganalysis methods comparatively simple and effective compared to video applications. Due to the complexity of video processing, it received very little attention regardless of its growing demand. The video steganography has been performed under different domains such as Partition Modes (PMs), Motion Vector (MVs), Intra Prediction Modes (IPMs), Quantization Parameters (QPs), and DCT coefficients. These different domain steganography methods had associated steganalysis techniques. As all these methods are at a preliminary stage, more generalized solutions for secure video processing has expected. The use of steganography domains for secrete message embedding belongs to individuals, but generalized video steganalysis regardless of the video steganography method is a key requirement of real-time applications. Thus, the cross-domain steganalysis is main motivation of this research study that includes the key focus on multiple domain video steganography, single steganalysis technique to detect the secret messages, deep learning for classification, and computational efficiency for steganalysis.

IV. Problem Statement

Due to the significant demand for digital video processing since from last decade, security becomes a crucial issue. The video steganography has received significant attention since from researchers. However, video steganography suffers from a wide range of challenges starting from the selection of appropriate video steganography method, embedding capacity, computational efficiency, and steganalysis. The recent video steganography solutions show promising results, but detecting accurate and robust secrete messages in stegno video is a more challenging research problem than stegno images. Although the existing steganalysis features can produce high efficiency in the targeted embedding domain, they cannot be adapted to identify the video steganography in other embedding domains. By considering the real-time applications of video processing, steganalysis should be generalized and can be applied to multiple domain embedding techniques. The common steganalysis for multi-domain video steganography is a challenging research problem as the statistical properties of steganography methods differ from each other. Thus, the first problem statement of this research is to design the cross-domain video steganalysis technique that accurately detects the universal steganalysis features regardless of the video steganography domain. For cross-domain steganalysis features, statistical stability enhancement becomes an important problem. This can b performed by applying the classification model by dividing the entire video dataset into training and testing. As the existing techniques used machine learning techniques that are suffering from the problems like misclassification errors and vanishing gradients. Thus, the second problem statement of this research is related to design the automatic and efficient classification model in the video steganalysis domain.

V. Research Objective

As per the research motivations and problem statements, the main goal of this research is to design novel video steganalysis techniques for cross-domain video steganography methods. The main objectives of this research are:

- To design and implement video steganography techniques across the different domains.
- To propose cross-domain steganalysis by estimating the global features set for multi-domain video steganography methods.
- To design the cross-domain steganalysis using deep learning classifiers for performance improvement.
- To design, model, and evaluate the performance of proposed steganalysis methods with state-of-art techniques using different datasets.
-

1. Research Contributions

As per the research objectives, we plan the design of this research in two contributions. In the first contribution, we aim to satisfy the first two objectives such as the design of different video steganography methods across the different domains and a single cross-domain steganalysis method to correctly detect the hidden messages. The second contribution belongs to optimizing the first contribution by introducing the features vector computation strategy by using artificial intelligence and deep learning classifiers for classification. The first contribution is called Independent Video Steganalysis (IVS), and the second contribution is called Deep Learning-based IVS (IVS). A brief idea about both contributions presented below:

- **IVS**: In this contribution, we design the algorithm of cross-domain feature set extraction for cross-domain video steganalysis of video steganography in multiple domains. We will consider three recently introduced video steganography domains such as PMs, MVs, and IPMs. The global feature set will be extracted according to the common statistical properties of all three steganography methods. After the extraction of global features, the domain-specific features are extracted in the local features set. Both global and local features are set to form the cross-domain steganalysis technique. This contribution satisfies objectives 1, 2, and 4. The classification can be performed by using the conventional machine learning classifiers such as Support Vector Machine (SVM) and Artificial Neural Network (ANN).

- **DL-IVS**: This contribution satisfies the third objective along with the first and fourth. The goal of this contribution is to further optimize the steganalysis performance by intelligently selecting the cross-domain features set using AI. The AI brings the best features extraction using fuzzy logic or optimization techniques. It may little increase the processing time but will enhance the extraction accuracy for video steganalysis. For classification, we will apply the deep learning classifiers such as Convolutional Neural Network, Long Short Term Memory (LSTM), and Recurrent Neural Network (RNN).

Figure 1 shows the functionality of the IVS model. As shown in figure 1, we have designed an algorithm of cross-domain feature set extraction for cross-domain video steganalysis of video steganography in multiple domains. For video steganography, we implemented the recently proposed steganography methods such as PMs, MVs, and IPMs. The outcomes of these techniques have fed as input to the proposed Steganalysis approach. We have designed a cross-domain technique for Steganalysis in which the global feature set is extracted according to common statistical properties. After the extraction of global features, the domain-specific features have been extracted in the local features set. Both global and local features are set to form the cross-domain steganalysis technique. The classification has been performed by using the conventional machine learning classifiers such as Support Vector Machine (SVM) and Artificial Neural Network (ANN).

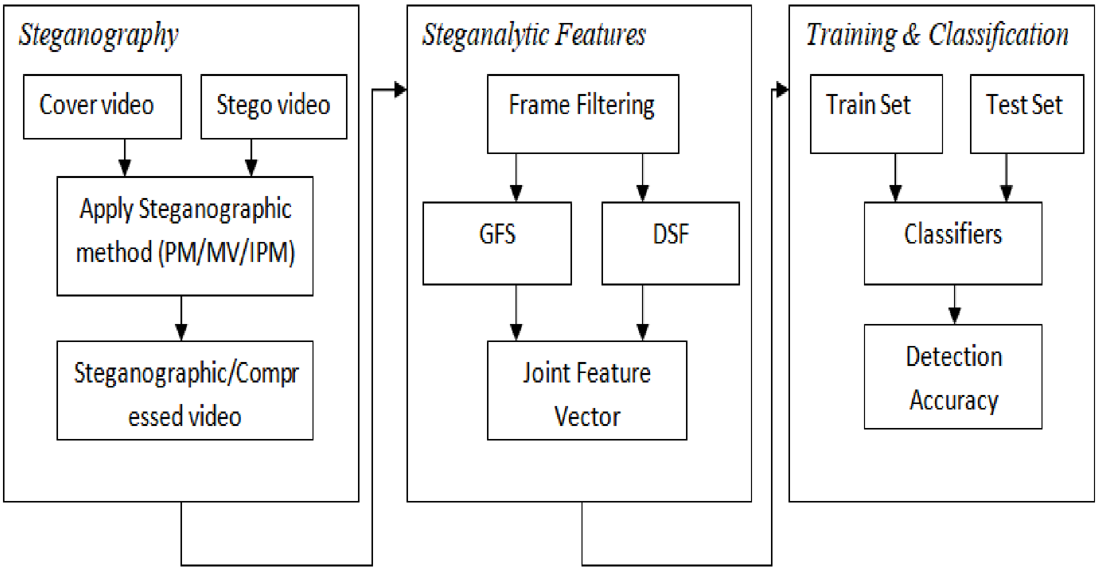

Figure 1. Proposed video steganalysis system

Below are the steps of proposed model:

1. Brose the input pair of cover and stego video sequences from the dataset
2. Perform the stganography using either PM-domain or MV-domain, or IPM-domain techniques.
3. Fed the outcome of steganogrpahic techniques as compressed video to cross-domain features extraction.
4. Perform the filtering on each frame.
5. Extract the domain-independent features called Global Features Set (GFS) from the compressed video sequence.
6. Extract the domain-dependent features called Domain Specific Features (DSF) from the compressed video sequence.
7. Build the joint cross-domain feature vector for steganalysis.

2. Classification & Training: To work on the measurable dependability of steganalytic highlights, the successive casings in every video arrangement are first isolated into non-covered gatherings with equivalent length (an encounter worth of 6), and afterward an element vector is removed from each edge bunch independently. The cover and stego sets of the video arrangements in a data set are haphazardly parted into equal parts, one half for preparing (70%) and the other half for testing (30 %). The classification and training performed by using two conventional classifiers ANN and SVM.

- The training set comprises a randomly-selected 70% of the cover-stego pairs, and is used to build a steganalyzer based on a given steganalytic feature set.
- The test set contains the remaining 30% of the cover-stego pairs, and is used for classification.

VI EXPEREMETALS DETAILS

1. System Requirements

Softwares: MATLAB 2020a, Windows OS.

Programming Language: MATLAB

Hardware: RAM-4GB, HDD-80 GB

2. Dataset Information

For the performance analysis we will use two of uncompressed video sequences. Every video sequence is progressively scanned and stored as a raw video file in the 4:2:0 chroma sampling format (YUV420p).

DB1: 100 uncompressed video sequences at CIF resolution with an average of 220 frames per sequence.

DB2: 100 uncompressed video sequences at 1080p resolution with each of which contains 912 average frames.

These datasets can be downloaded from below link

https://pan.baidu.com/s/1KLDQGRJ1-3hPiccvggl9Cw#list/path=%2Fyuv_seqs

3. State of Art Methods

The method from references [1]-[4] acts the main related works for comparative study. We will use all these methods for comparative analysis with proposed steganography methods.

4. Key Performance Metrics

The commonly used performance metric to evaluate the performance of Steganalysis methods is Detection Accuracy. It is computed as:

$$Accuracy = 1 - \frac{1}{2}\left(P^{FA} + P^{MD}\right) \tag{1}$$

Where P^{FA} is probability of false alarm and P^{MD} is probability of missed detection.

5. Modulation structure for QPSK: As shown in figure 2. , the parallel data stream is part of the in-stage and quadrature-stage segments. These are then separately balanced onto two even premise limits. In this utilization, two sinusoids are utilized. A short time later, the two sign is superimposed, and the following sign is the QPSK signal. Note the utilization of polar non-come back to-zero encoding [11, 12]. These encoders can be set before for parallel data source [13], however, have been set after to illustrate the applied distinction among digital and simple sign engaged with digital modulation [14.15].

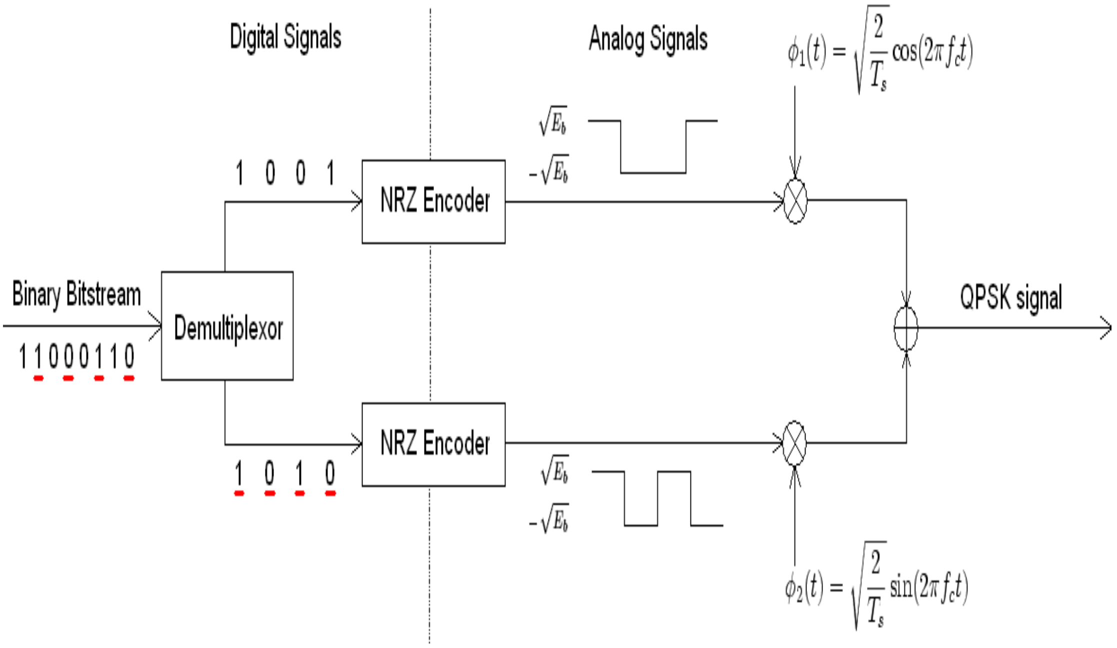

Figure 1. QPSK modulation.

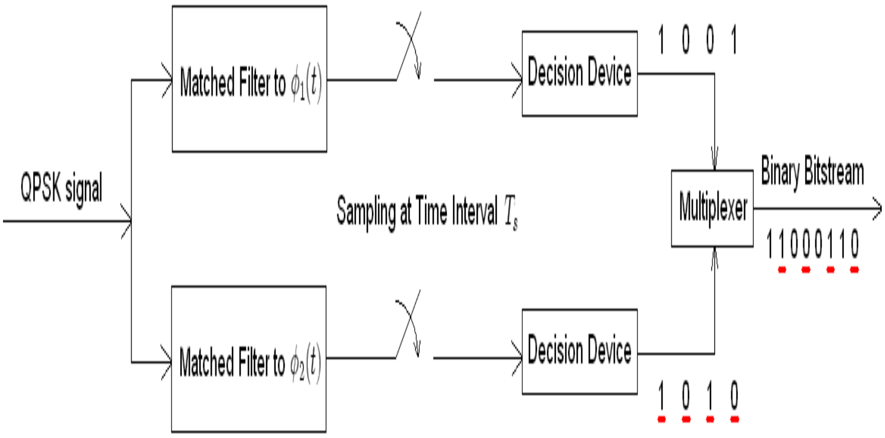

Figure 2. QPSK demodulation.

Demodulation structure for QPSK: As shown in figure 5.4 the coordinated channels can be supplanted with correlators. Every discovery gadget utilizes a reference limit, an incentive to decide if a 1 or 0 is identified.

5.1 QAM

The Quadrature Amplitude Modulation (QAM) is extensively used in various computerized information radio correspondences and information exchange applications. A variety of sorts of QAM is open, and a part of the more commonplace structures incorporate 16 QAM, 32 QAM, 64 QAM, 128 QAM, and 256 QAM,[16-18]. Here the figures 5.6 to 5.8 allude to the number of focuses on the star grouping, for example, the number of individual states that can exist.

VII RESULT AND DISCUSSION

By knowing the initial chaotic values, the decryption of the matrix is done by the values which have been set done initially is given by

$$\overset{\wedge}{\alpha} = \begin{bmatrix} a_i \\ b_i \end{bmatrix}^{-1} \qquad (2)$$

Then the random matrix, which was obtained by the condition of the regression principle can be predicted by

$$\overset{\wedge}{\varpi} = \underset{\tau,\upsilon}{Min} = \frac{1}{N}\sum_{i=1}^{N} f(P_{ij}, C_{ij}, \tau, \upsilon) \quad \text{Subjected to} \quad \|\upsilon\| < t \qquad (3)$$

Thus by predicting the random matrix by the regression principle, decrypting the chaotic values and the proper estimation of noise, the original image obtained in the reconstruction phase is given by relating the equation 2, 3, and 4 is

$$I_m = \frac{\overset{\wedge}{c_i}}{\overset{\wedge}{\varpi}\,\overset{\wedge}{\alpha}} \qquad (4)$$

Where I_m is the original image reconstructed by the proposed Corvus Corone Module. The pseudo code for the reconstruction phase of the proposed module is showing in figure 3.

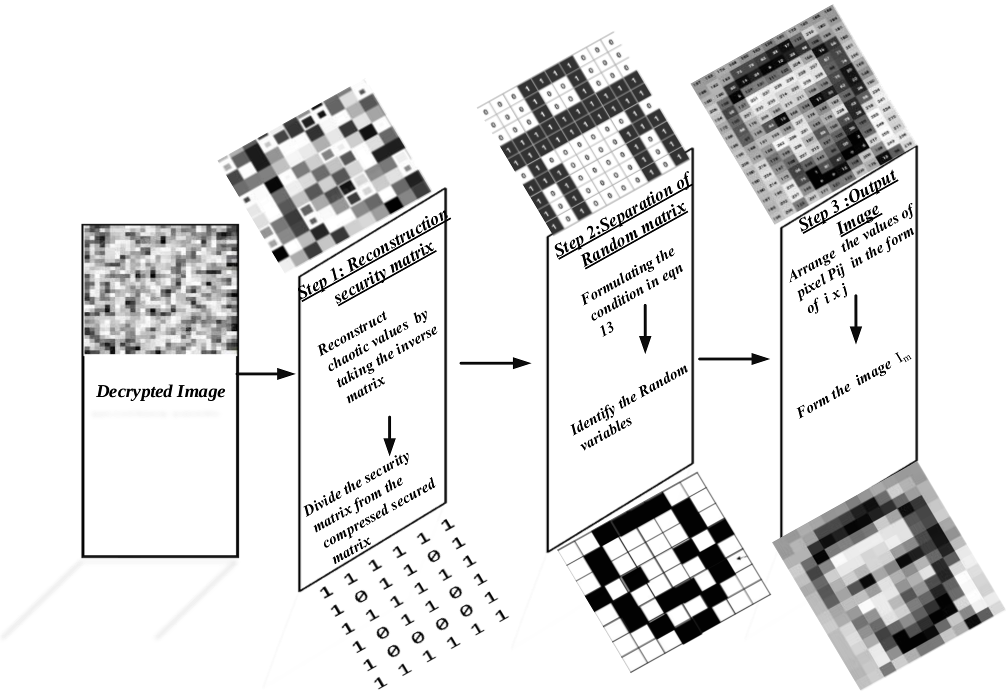
Decrypted Image
Step 1: Reconstruction security matrix
Reconstruct chaotic values by taking the inverse matrix
Divide the security matrix from the compressed secured matrix
Step 2:Separation of Random matrix
Formulating the condition in eqn 13
Identify the Random variables
Step 3 :Output Image
Arrange the values of pixel Pij in the form of i x j
Form the image I_m

Figure 3. Reconstruction of the original image.

Table 1. Comparison of BER with the existing techniques.

Methods	**Lena**	**Barbara**	**Man**
Singh et al. [159]	0.02	0	0.01
Hybrid water marking [160]	0.01	0	0.005
JSCC	0.015	0.0145	0.1
ES	0.0.056	0.075	0.078
DP	0.056	0.0075	00.075
DP and BB	0.0781	0	0.089
SSIM [bilal]	0.0003032	0.0003089	0.0003054
Our paper proposal	0.0003022	0.0003094	0.0003047

From table 1. , the proposed methodology compared with the other existing methodology of Singh et al., hybrid watermarking, JSCC, ES, DP, and DP with BB in terms of their BER

VII Conclussion

Introduced in this contribution of this research in which the two-way secure cooperative communication model designed using the CorvusCorone module. The extensive results using the different quality parameters and efficiency parameters presented for this contribution. From the simulation results of all the contributions, the proposed methods overcome the challenges of existing techniques related to energy efficiency, image quality, security, etc.

ACKNOWLEDGMENT

I would like to thank Department of Software department of, Istanbul Aydin University.

REFERENCES

1. G Zhai, L., Wang, L., & Ren, Y. (2019). Universal Detection of Video Steganography in Multiple Domains Based on the Consistency of Motion Vectors. IEEE Transactions on Information Forensics and Security, 1–1. doi:10.1109/tifs.2019.2949428.
2. Tasdemir, K., Kurugollu, F., & Sezer, S. (2016). Spatio-Temporal Rich Model-Based Video Steganalysis on Cross Sections of Motion Vector Planes. IEEE Transactions on Image Processing, 25(7), 3316–3328. doi:10.1109/tip.2016.2567073.
3. Ghamsarian, N., & Khademi, M. (2020). Undetectable video steganography by considering spatio-temporal steganalytic features in the embedding cost function. Multimedia Tools and Applications, 79(27-28), 18909–18939. doi:10.1007/s11042-020-08617-y.
4. H. Zhang, W. You and X. Zhao, "A Video Steganalytic Approach Against Quantized Transform Coefficient-Based H.264 Steganography by Exploiting In-Loop Deblocking Filtering," in IEEE Access, vol. 8, pp. 186862-186878, 2020, doi: 10.1109/ACCESS.2020.3030685.
5. Rana, S., Kamra, R., & Sur, A. (2019). Motion vector based video steganography using homogeneous block selection. Multimedia Tools and Applications. doi:10.1007/s11042-019-08525-w.
6. Manisha, S., & Sharmila, T. S. (2018). A two-level secure data hiding algorithm for video steganography. Multidimensional Systems and Signal Processing. doi:10.1007/s11045-018-0568-2.
7. Pan, N., Qin, J., Tan, Y., Xiang, X., & Hou, G. (2020). A video coverless information hiding algorithm based on semantic segmentation. EURASIP Journal on Image and Video Processing, 2020(1). doi:10.1186/s13640-020-00512-8.
8. Huang, X., Hu, Y., Wang, Y., Liu, B., & Liu, S. (2020). Deep Learning-based Quantitative Steganalysis to Detect Motion Vector Embedding of HEVC Videos. 2020 IEEE Fifth International Conference on Data Science in Cyberspace (DSC). doi:10.1109/dsc50466.2020.00030.
9. Zhang, H., Cao, Y., & Zhao, X. (2015). Motion vector-based video steganography with preserved local optimality. Multimedia Tools and Appli
10. Amenah D. Abbood, Bara'a A. Attea, Ammar A. Hasan, Richard M. Everson, Clara Pizzuti (2023), Community detection model for dynamic networks based on hidden Markov model and evolutionary algorithm. Artificial Intelligence Review, 56(9), 9665.10.1007/s10462-022-10383-2
11. Ameen M. Hameed,Arkan R. Ridha., Electron Scattering from Stable and Exotic Li Isotopes. (2024). Iraqi Journal of Science, 65(3), 1391-1401.https://doi.org/10.24996/ijs.2024.65.3.18
12. A.A.Abdulmajeed,T.M,Tawfeeq,M.A, Al-jawaherry.Constructing a Software Tool for Detecting Face Mask-wearing by Machine Learning . Baghdad Sci.J [Internet]. 2022 Jun. 1 [cited 2024 Apr. 2];19(3):0642. https://bsj.uobaghdad.edu.iq/index.php/BSJ/article/view/5716
13. E. F. Naser, S. M. Zeki, Using Fuzzy Clustering to Detect the Tumor Area in Stomach Medical Images. Baghdad Sci.J [Internet]. 2021 Dec. 1 [cited 2024 Apr. 2];18(4):1294.https://bsj.uobaghdad.edu.iq/index.php/BSJ/article/view/4727
14. H. M. Abdulhadi.Y. S. Aldeen,M. A. Yousif,M. jaseem,S.Madni Enhancing Smart Cities with IoT and Cloud Computing: A Study on Integrating Wireless Ad Hoc Networks for Efficient Communication. Baghdad Sci.J [Internet]. 2023 Dec. 5 [cited 2024 Apr. 2];20(6(Suppl.):2672.https://bsj.uobaghdad.edu.iq/index.php/BSJ/article/view/9277
15. A.K.Jassim,M.J. Hamzah,A.H. AliwyUsing Graph Mining Method in Analyzing Turkish Loanwords Derived from Arabic Language. Baghdad Sci.J [Internet]. 2022 Dec. 1 [cited 2024 Apr. 4];19(6):1369
16. Ismaeel, N.Q., Mohammed, H.J., Chaloob, I.Z. et al. Application of Healthcare Management Technologies for COVID-19 Pandemic Using Internet of Things and Machine Learning Algorithms. Wireless Pers Commun (2023). https://doi.org/10.1007/s11277-023-10663-2
17. Alhayani, B.A., AlKawak, O.A., Mahajan, H.B. et al. Design of Quantum Communication Protocols in Quantum Cryptography. Wireless Pers Commun (2023). https://doi.org/10.1007/s11277-023-10587-x
18. Omar A. AlKawak, Bilal A. Ozturk, Zinah S. Jabbar, Husam Jasim Mohammed,Quantum optics in visual sensors and adaptive optics by quantum vacillations of laser beams wave propagation apply in data mining,Optik,Vol,273,2023,170396,https://doi.org/10.1016/j.ijleo.2022.170396.