A Robust Reversible Data Hiding Framework for Video Steganography Applications

Manjunath Kamath K[1]
Assistant Professor
Dept. of Computer Science and Engineering
Canara Engineering College
Benjanapadavu, India

Dr. R. Sanjeev Kunte[2]
Professor
Dept. of Information Science and Engineering
J.N.N College of Engineering
Shivamogga, India

***Abstract*—Reversible Data Hiding (RDH) is a special form of data hiding approach for data integrity and confidentiality protection where the secret image bits (SI) are embedded into Cover Media (CM) by altering its intrinsic pixel attributes. However, in RDH the CM along with the secret message is recovered at the end of computing phase. However, despite of its potential use-cases for enhancing the embedding performance, when it comes to security for various network standards, the traditional RDH mechanisms cannot fully comply with the standards for different set of attacks during the bit-stream transmission scenarios. Therefore, the proposed study contributes towards a computational framework of a robust RDH framework for Video Steganography (VS) which is modeled and simulated under various attack effects and the observation outcome are produced in before and after attack situations to justify the improvement over Embedding Capacity (EC) and Peak Signal-to-Noise Ratio (PSNR) performance for both CM and secret message unlike traditional difference expansion-based methods (DE). The outcome of the study shows that the formulated RDH method not only achieves better reversibility at lower cost of computing but also ensures effective PSNR and imperceptibility outcome for both CM and secret image.**

Keywords*—Reversible data hiding; data integrity; embedding capacity; video steganography

I. INTRODUCTION

The underlying principle of Data Hiding (DH) has been extensively explored and the scope of evolution in research advancement for practical solutions still being nurtured. The prime agenda of this area is to provide better level of security solutions in communication scenarios for various network applications [1][2]. This area has got wide range of applications starting from civil, military to critical healthcare domains. However, DH has come as a substitution for the traditional data security mechanisms of crypto-graphic solutions where the prime challenge persists in dealing with bit-stream pattern vulnerability for textual and image data in transit [3]-[8]. In conventional approaches of DH, the secret message is embedded into a Cover Media (CM) as a hidden data so that the privacy of the data can be protected while in wireless transmission and this approach has been found as a promising security measure as the bit stream patterns are not easily noticeable by the malicious users. Exposing the data requires a high technical and tactical computing process which is not a trivial task to be carried out by the malicious user during network transmission [9] [10]. However, in some cases of DH such as steganography and watermarking the secret message while embedded into CM alters its intrinsic properties which result in distortion during the data embedding operations and the restoration of CM in acceptable form while extracting the message is highly required in some sensitive cases. Thereby distortion of CM is strictly forbidden in some critical scenarios [11][12][13]. The reversible data hiding (RDH) has gained attention from researchers for solving this problem to a greater extent in the field of DH and also ensures protection of the content ownership and authenticity of data. Unlike digital watermarking the prime concern of RDH is to conceal the data into cover medium in such a way so that the embedded data remains unnoticeable which refers to imperceptibility [14]-[17].

However, traditional RDH techniques lacks efficiency while restoring the CM in the original form as the process of secret image bits extraction often affects the signal quality of both the message and the CM. In many cases most of the RDH techniques are also found shrouded with computing complexity problems and do not ensure robustness against different forms of network attacks in video steganography [18][19][20]. This study explores various attack scenarios and their impact on the concealed data and introduces a simplistic and robust RDH framework for uncompressed video formats. This model intends to design the framework in such a way where it measures the performance of EC in terms of marked image quality and the capacity of payload metric considering the optimized execution flow of H.264/AVC encoding standard. The framework enables two model executions such as DWT and DWPT in conditional bases prior performing the embedding process for the uncompressed CM. However, it also creates a test environment to observe the outcome of EC and PSNR without attacks and even if the marked image undergoes through any of the most popular attacks such as a) Speckle noise, b) Gaussian noise, c) Histogram Equalization etc. in transit, then how the attacks affect the CM and secret image quality in the reconstruction phase. Also, the study observes the outcome with respect to EC in the measure of Normalized Correlation (NC) and assesses visual perception metric from the extraction of secret image quality before and after the attack is performed. The numerical assessment produces the promising outcome correspond to PSNR for both CM and secret image in the presence of attacks and without performing attacks which are comparable to the

existing approach of DE. This also shows that the proposed RDH attains good reversibility with enhancement in the EC aspects with the measure of imperceptibility for Normalized Correlation (NC) metric as NC(Ow/Rw). Here Ow refers to original video frame and Rw refers to reconstructed video frame index. The prime novelty of this formulated approach is as follows:

- It addresses the overflow/underflow problem of intrinsic pixel attributes for secret image during the numerical computing which maintains the range of pixel values for frames with upper bound of 255 and lower bound of 0.
- Another contributory aspect of the proposed method of RDH is it addresses the design limitations of existing Difference Expansion (DE) approach in RDH, where the difference value between pixel pairs is computed and this computed difference values are used to embed the secret data. The traditional DE based approaches ensure better hiding capacity of secret message but do not ensure better reconstruction of signals for CM and secret image in or without the presence of attack effects. This indicates that the distortion effects remain present in the restored signal too.
- The system model of RDH here not only balances the EC and PSNR performance but also ensures robustness against different types of popular attacks.
- It also exhibits that in the presence of attacks also the system attains considerable optimized reversibility with good PSNR performance.
- It also ensures higher imperceptibility while maintaining better computing performance for embedding scenario considering H.264/AVC.
- The simplistic design format for the H.264/AVC based embedding solutions also optimizes the time complexity for operations which is not much addressed in the existing systems.

Owing to the above stated contributory points of novelty, the proposed system of RDH evolves up with a solution to address impending problems towards data hiding scheme that was not solved before. The paper is further organized as follows: here Section II analyses the related studies correspond to RDH and its implications on the futuristic research prospects of video steganography. Section III further implies exhibiting the problem formulation for the study where the scope of improvement of the RDH method is also discussed followed by research method explanation in Section IV. Further Section V discusses the core numerical design modeling for the proposed RDH framework and in Section VI discusses the proposed algorithm modeling followed by in Section VII the produced comparable outcomes for performance assessment are observed to show the improvement in the aspects of EC, security, and reconstructed signal quality. And finally, Section VIII remarks conclude the overall research.

II. Review of Literature

In the past two decades RDH advances with its widespread methodical approaches. This aspect of RDH has been studied and reflected in more and more publications to strengthen the research scope from futuristic perspectives. This section critically reviews the related literatures from the recent publications and its primary concern lies in finding the current state-of-the-art approaches, their strength factors, and design limitations. Moreover, it also extracts the gap that persists in RDH research, clarifying the possible research needed in this domain. The implications of futuristic communication systems over 4G and 5G although provides idea for seamless way of data streaming but the security loopholes remain open research problems for various concern. However, the traditional RDH approaches also encounters a challenge while increasing the EC as it affects the visual perception of CM, once the signal is recovered during secret message extraction process. This condition also remains as vulnerability for the present communication systems and provides intruder the opportunity to target the secret information. A set of studies have explored the trade-off for RDH that remains between Visual Perception (VP) and Embedding Capacity (EC). The relationship that exists between VP and EC that can be expressed with a maximization problem, and realized as follows:

$$EC \propto \frac{1}{VP} \quad (1)$$

This Equation (1) indicates that a major concern of the current research trend is to maximize the EC in RDH without sacrificing the considerable of VP at the receiver end as reconstruction of CM and embedded message is also required in acceptable forms in some of the critical cases. Thereby, the prime motive of the current research evolves towards balancing this trade-off. The study of Cao et al. [21] has suggested that no matter in which domain of RDH procedure is concerned either 1) Plaintext Domain or 2) Encrypted Domain, but in both the domains proper restoration of CM and secret image bits has to be carried out irrespective of EC and its dependency on the size of the secret image [21]. It also explores that reason behind the justifications for the type of SM which has be embedded inside the CM. So here lies a question that what kind of form of SM is to be embedded inside CM so that maximum level of security can be retained throughout the transmission. Here security refers to protection of data confidentiality and integrity. However, the challenge in imposing the security arises as it also has to maintain the minimum threshold of human visual perception for acceptable form of reconstructed media. The study suggests from its crucial findings that optimization can be a better approach to deal with this aspect of RDH which can be of two different types such as i) Single objective optimization problem and ii) Multi-objective optimization problem. The study of Qi et al. [22], Wang et al. [23] and Ou et al. [24] considers single-objective based optimization considering the technique Multiple Histogram Modifications (MHM) where the bin selection approach has been referred extensively to attain better EC performance. However, the study of Ke et al. [25] studies the encrypted domain of RDH and introduces a fully Homomorphic encryption and Difference Expansion (DE)

based RDH based on single objective optimization solution. The study also attempts to minimize the Rate Distortion (RD) effects on the CM while also attain better EC for data hiding and also claims that the outcome produced show effective security outcome.

However, it is observed that the above studies have not extensively discussed about different types of attack scenarios and the also the conventional HS based approaches do not ensure better utilization of CM during the embedding scenario. And also, often exploits the texture characteristics of image for correlation purpose which could degrade the quality of the CM.

The multi-level optimization based solutions also have been referred in various studies; the study of Yin et al. [26] introduced a multi-objective optimization based theory to develop a solution approach for RDH. However, one limitation of the approach is that it can only operate in JPEG images for combination of non-overlapping parts. However, this approach also attempts to attain a proper balance between EC and RD. The study in this research specific context does not talk about the inclusion of videos as CM for video steganography applications. On the other hand the study of Mohammadi et al. [27] also emphasizes on multi-objective problem formulation for local difference predictor. The labeling during the prediction scenario also helps in effective extraction of the embedded data. The study not only ensures better performance for signal quality aspects of the reconstructed cover video but also attain high EC from the point of view of data hiding and security. The limitation of the study lies within the fact that it doesn't considers video object as a cover media. There exist other related studies such as Roy et al. [28], Peng et al. [29] and Wang et al. [30] which have also incorporated the multi-objective optimization based solutions and also talk about its scope in the futuristic methods of RDH. The study of Li et al. [31] also talked about the problem context of variation in statistical features of shifting histograms and introduced an improved version of difference histogram shifting based algorithms. However, another improved version of DE based approach was seen in the study of Kim et al. [32] which also utilizes the features of location map and Laplace distribution. The DE based approaches also observed for lossless compression which can be observed in the studies of [33-37].

The study by Liu et al. [38] provides a solution approach of combination of art image generation and data hiding for image security aspect. The outcome assessed from this approach shows that, the algorithm's computational complexity is quite higher and data hiding performance is also not considerable for different images. There are studies by Wang et al. [39], Yao et al. [40], and Ke et al. [41], where the prime concern was laid on digital data security considering RDH techniques. However, most of studies consider RDH on encrypted domain however most of the techniques are not assessed for color images and computational complexity aspects are also not much explored. The study of Rahman et al. [42] also introduces a RDH technique for the authentication of source for biological signals. Similar problem context for RDH is also explored in, Wu et al. [43] and Xie et al. [44]. Here one critical observation exhibits the matter of fact that majority of the techniques are majorly concerned about enhancing the EC of the image signal. The study of Weng et al. [45] addresses the problem of higher embedding distortion considering the approach of invariability and adjustment in the pixel attributes. However, this approach of RDH is found not suitable for the high dimensional image matrix. The study of Wang et al. [46] explores various DE based RDH mechanisms and presented their design models for VQ-based data hiding. The study also refers another significant research, the study basically introduces a novel DE based embedding solutions to enhance the EC without compromising with the distortion aspect. Apart from this, various recent work towards RDH has been carried out by Zhou et al. [47], Dragoi et al. [48], Li et al. [49], and Sheidani et al. [50]. Although, these techniques are quite robust from security perspective, but a computationally extensive process has been implemented towards data hiding that increases complexity on the long run. The next section outlines the identified research problems in this perspective.

III. Research Problem

The prime motive behind the design solutions for RDH is to enhance the quality of data security so that the contribution in this domain could make this research track more worthy for different purposeful use cases. Another primary concern of RDH is to overcome the constraints of privacy protection offered by the traditional cryptographic and DH methods. From the previous segment of the study, a set of observations are outlined which helps in generalizing the problem statement of this research specific context. It should be noted that the advancement of embedded and computing systems has brought so many changes in the existing communication scenarios and also network protocol integrations for artificial intelligence (AI) based systems aims to serve more and more consumers for streaming services. However, RDH since many years have extensively applied on digital images whereas later various communication standards from the business and security perspectives of data protection have enabled the seamless video transmission over wireless channels and with this a consistent evolution on standard frame formats is also witnessed. Hence, various video frame formats of CIF, QCIF, WVGA and HD have been explored for different streaming applications. The study mostly focuses on video steganography-based applications where data security from the point of view of privacy protection plays a crucial role. However, the study realizes that those traditional RDH systems are evolving but still lacks improvement in many areas. Prime objective of this section is to illustrate those key findings which cover the areas where RDH requires improvement. The following are the key aspects for research problem:

- Most of the critical vision-based systems require effective and secure transmission of secret message embedded in a video and henceforth require robustness in security implementations.
- It is also observed that the traditional approaches of HS/MHM and DE in RDH mostly focuses on images for transmission but do not talk much about the videos as CM. This has become a core motivating factor for this research.

- Most of the existing popular approaches of DE attains better EC along with adequate data hiding but lacks computing efficiency along with high distortion problem of images. However, RDH on encryption domain even though achieve higher EC factor but also do not ensure better reversibility and not evaluated for color videos or other forms of images. It can also be seen the reconstruction of CM and secret message do not ensure better PSNR range for uncompressed videos when entropy encoding is concerned.
- Very lesser studies have actually revealed the potential factors of H.264/AVC towards performing embedding of secret image in an uncompressed video which opens up more VS based applications deployment opportunities for security concern.
- The existing MHM and DE based approaches do not ensure robustness against different security attacks rather JPEG compression. This restricts their deployment in futuristic critical use-cases where proper reconstruction of CM and message is required.
- It is also observed that not much emphasize has been given on the assessment of computational complexity for the traditional RDH solutions for videos. Videos are formed through a sequence of frames which creates a larger form of complex data and needs efficient processing, storage indexing and transmission schema to meet the requirements of effective embedding operations of RDH.

Thereby the study formulates its problem statement as "To design and develop a secure and robust RDH framework for uncompressed videos which should comply with the futuristic network constraints while maintaining better embedding performance in the measure of imperceptibility while maintaining efficient reversibility of the reconstructed CM and the secret image".

IV. Research Method

The study adopts analytical research modeling for the design of H.264/AVC based embedding solution to comply with the requirements of formulated RDH framework. The core functional block-based execution shows that initially the framework enables model selection of customized blocks under the conditional cases of discrete wavelet transform (DWT) and discrete Wavelet Packet Transform (DWPT) to make the uncompressed video (C_m) suitable for embedding operation. The mode of DWT exploits the high correlation between the adjacent temporal frames and also deals with high frame rate video constraints. This helps in efficient computing of C_m from both storage and processing point of view. The incorporation of DWT while performing the embedding operation also maximizes the capacity of ownership protection. The DWT model here also helps in decomposing the Y components for YUV color-space during the embedding operation for H.264/AVC. During the embedding process the workflow for the DWT model also insert the secret image into the resulting sub-bands using extracted low level coefficient values. The DWT decomposition here also makes the video suitable for the embedding operations considering a customized function of principal component analysis (PCA) and also enhances the security of the algorithm. Finally, the embedding operation considering UC-Video Cover and secret data generates the H.264/AVC based encrypted video. The Fig. 1 shows the overall design of the system model for proposed solution of RDH.

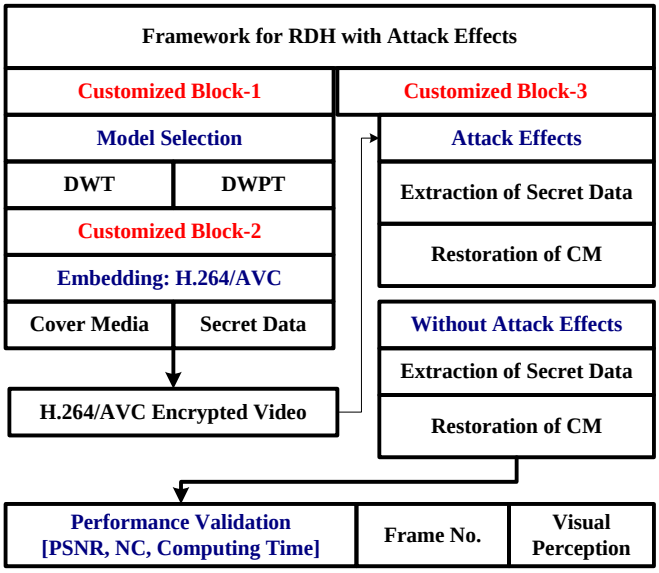


Fig. 1. Framework for RDH.

The system further also assesses the performance outcome in the measure of visual perception for the original frame index, reconstructed frame index of both CM and secret image message for two different types of scenarios. Here one scenario indicates extraction of secret data after performing a set of attacks such as – i) Speckle noise, ii) Gaussian noise, iii) Histogram equalization, iv) Salt and pepper noise, v) Poisson noise, vi) Frame averaging, v) JPEG compression, vi) Gamma correction and vii) Median Filtering. On the other hand, another scenario considers assessment of the model without attack effects. In both the scenarios the visual perception for the reconstructed CM and secret image bits are computationally assessed with the metrics of PSNR. Here the NC refers to the performance index to justify the metric for embedding capacity and shows how the formulated approach attains better data hiding as compared to the traditional RDH mechanisms. The study further also assessed the computing time for embedding and to generate the encrypted video sequence of H.264/AVC for $\boldsymbol{C_m}$ which is also referred as embedded video. The next section further shows the numerical modeling for the execution operations of the proposed RDH framework.

V. Numerical Design Implementation

The numerical design and modeling of the proposed system has been implemented over a computing environment and subjected to cover most of the executable operations for RDH and H.264/AVC based embedding. The study impels the design requirements to make the RDH numerical framework model robust and considers a set of hypothetical assumptions to make it more realistic for the futuristic video steganography-based applications.

A. Assumption for System Design

The study considers a set of hypothetical assumptions during the design and research modeling of the formulated approach. The prime reason behind taking these assumptions is to develop a sophisticated numerical model for the research specific purposes. The primary assumption considers that both S_{msg} to be embedded and the video file in the form of C_m are not distorted and restore its original form after a set of computation. The video file $v_i \rightarrow C_m$ is considered to be uncompressed in the initial phase of the system modeling and further subjected to embedding process. The secondary assumption of the research is that the formulated RDH approach offers better embedding capacity along with robustness, perceptibility and security measures which is needed to be validated under different conditions of parametric numerical evaluation. The tertiary assumption in the context of the formulated study considers that the embedded secret information msg in C_m to be transmitted over a wireless medium to a specified terminal under different operating conditions.

B. Model Selection and Embedding Process

1) Uncompressed video: C_m processing: The system initially considers two different mode of selection that is either DWT or DWPT in the form of analytical model and further enables the proposed effective embedding operations with respect to potential form of computing aspect. Further customizes a function to read and process the cover media that is- $f(x)$: $f \leftarrow C_m$. This function considers uncompressed video file (v_i) in the form of cover medium $v_i \rightarrow C_m$. To process the uncompressed v_i for i number of frame sequence, the system initially locates the file v_i with two distinct attributes, the expression to denote the C_m with these two attributes can be expressed in Equation (2) as:

$$C_m \leftarrow [f_n(v_i), floc(v_i)] \quad (2)$$

Here the first attribute in the vector $f_n(v_i)$ indicates the particular file naming string, whereas the second attribute $floc(v_i)$ denotes the locator of the v_i within the disk drive file system structure. Finally, the system process both the attributes $fn, floc \in v_i$ to generate an object Obj(v) as follows:

$$V_{obj}(i) \leftarrow [floc \parallel f_n] \in v_i \quad (3)$$

The Equation (3) shows a concatenation operation of these string attributes in order to generate an object file of $V_{obj}(i)$. The method further converts the yuv4mpeg media object form of $V_{obj}(i)$ into numerically compatible movie format M. The system here also applies another custom functional module $f(x)$: $f \leftarrow V_{obj}(i)$, to generate the numerically compatible format M and associative fields after as set of computing procedure. The numerical conversion of the yuv4mpeg (C_m) is shown with the following flowchart as shown in Fig. 2.

The process flow in the Fig. 2 shows that in this procedure initially the system enables the function to load the object form of video sequence $V_{obj}(i)$. In the further stage the system computes the structure of data and its corresponding color map [d, C_m] from the $V_{obj}(i)$ which is in the form of YUV structure of data. The system further computes the file size on the disk in bytes and process the file in the read only mode followed by computation of the headers (h) and last position of headers $e(h)$. Finally, the process computes the headers and start computing the frame length (f_l) for each frame i. The computation of the f_l takes place with the following mathematical Equation (4).

$$f_l(i) = f_h(i) \times f_w(i) \quad (4)$$

Here in the Equation (4) the system computes frame length for each frame $i \in V_{obj}(i)$. Further, the process flow enables conditional statement to check the color space from the fields, if color space is found to be 'C420' then the system computes the frame length as shown in Equation (5):

$$f_l(i)C420 = (f_l(i) \times \lambda)/\rho \quad (5)$$

However, in another case if the color space in the fields match with 'C422' then the system computes the frame length as below:

$$f_l(i)C422 = (f_l(i) \times \lambda) \quad (6)$$

In the case of color space 'C444' the frame length is computed as shown in Equation (7).

$$f_l(i)_{C444} = (f_l(i) \times \rho) \quad (7)$$

Further the process flow execution computes the frame count (f_c) before proceeding to the reading of YUV-frame sequence. The Equation (8) shows the numerical expression for frame count.

$$f_c = (f_b - e(h))/\sum (\alpha + f_l(i)) \quad (8)$$

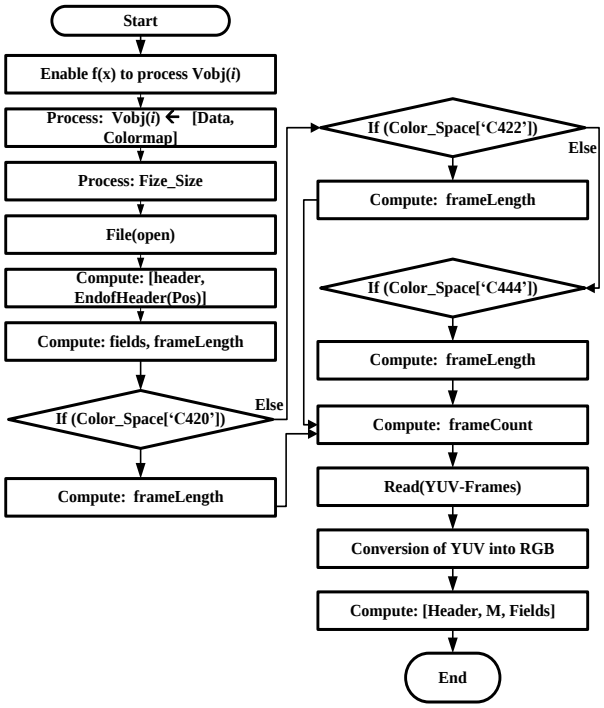


Fig. 2. Process-flow of the Conversion Operation of [$V_{obj}(i) \rightarrow M$].

Here f_b refers to the file size in bytes and α is a system constant. After computing the frame length, the system further read the YUV-frame sequence from the video object and converts it into final sequence of RGB which is in the numerically compatible format. Finally the system generates the computed header, M and fields for the consecutive part of the process execution.

C. Uncompressed: Smsg Processing

Further the system process in this phase of modeling also considers S_{msg} in the form of secret image bits ($S_{msg} \rightarrow w$) and digitize it in the compatible numerical form. For this process the system initially locates the specific w with two distinct attributes wLoc and wN. The secret message is further generated with the following numerical expression Equation (9).

$$S_{msg}(i) \leftarrow [wLoc \parallel wN] \in w \quad (9)$$

Further the system computes the numerical form of S_{msg} by performing digitization of the matrix and generates secret image bits type-1 (w1) followed by computation of secret image bits type-2 (w2) in binary form based on thresholding.

D. Formulated H.264/AVC based Embedding Procedure

The system further extends its workflow on the formulated embedding procedure of the secret message msg in the form of secret image bits w2. The system designs the embedding procedure with two stages of execution with invoking custom function. Initially it considers nf , M for $f_{i,}$. The system furthers also constructs a cell structure of M{ $f_{i,}$}. The system performs numerical vectorization of the msg→w2 with the following mathematical expression.

$$R1, C1 \leftarrow Rf(msg \rightarrow w2)$$

$$w2 \leftarrow Rf(w2t)R1xC1 \quad (10)$$

In the above equation (10), the system here computes the resizing operations with respect to a transpose operation for the dimension of R1, C1 correspond to w2 matrix. Further the computation, converts the RGB component of M{ $f_{i,}$} into YCbCr color space as YCbCr[i] ← M{ $f_{i,}$}. It also computes the individual frame matrix for YUV such as y← y(r,c,1) , u←u(r,c,2) and v←v(r,c,3) from the converted YCbCr[i]. The computation further applies N-level wavelet decomposition procedure on the y←y(r,c,1) component with "haar" wavelet transformation. The wavelet decomposition here takes place with the following mathematical Equation (11).

$$C1,C2 \leftarrow Wd(\ Matrix[\ y(r,c,1)]N) \quad (11)$$

The wavelet decomposition is carried out on the matrix form of $y(r,c,1)]_N$ at level-N. The outcome produced by the function generates two distinct coefficients of C1 and C2 which are further subjected to approximation stage of two-dimensional signal vector. The function LL←Acoeff(C1,C2) performs basically approximation of the coefficients and generates sub-band of LL. The final coefficient approximation stage further extensive analysis the C1, C2, N and generates other sub-band components of LH, HL, HH components. These two stages of execution modeling can be expressed as shown in Equation (12).

$$LL \leftarrow Acoeff(C1,C2)$$

$$LH,HL,HH \leftarrow Ecoeff(C1,C2,N) \quad (12)$$

The system further performs wavelet decomposition for respective channel (*ch*) of bands which can be formed as [LL→ 1, LH→2,HL→3,HH→4].

$$Cb1,Cb2 \leftarrow Wd(\ Matrix[ch]N)$$

$$LLd \leftarrow Acoeff(Cb1,Cb2)$$

$$LHd,HLd,HHd \leftarrow Ecoeff(Cb1,Cb2,N) \quad (13)$$

In the above Equation (13), the system computes the coefficient extraction process for different bands with conditional execution of *ch* which ranges between 1→4. The system further computes sub-blocks correspond to the matrix form of LLd for each row and col vectors as sub(i,j,n) ← LLd((i,r),(j,c)). The model here also exploits the standard principle of H.264/AVC encoding operations to complement the embedding operation and further the computed sub-blocks are then further processed under a custom function of PCA(x) which generates the final data (Fdata) from the covariance matrix (CovM). This final data is referred to the H.264/AVC encrypted data.

E. Formulated RDH with Extraction Procedure

The extraction procedure in the context of RDH for the formulated approach also constructs a custom function of *f*: $f_{ex}(x) \leftarrow Sub*w, R_f\ (RGB) \quad C_m$. The custom function in this case considers encrypted video object with H.264/AVC coding standard with Sub*w, R_f (RGB) and also considers nf, wavelet name, the dimension factor of R(i), C(i). The system reconstructs the video sequence here for Tm: [*m*1/*m*2]. In the initial phase of computation, the system constructs the cover from the Sub*w, R_f (RGB) for different f_i which is represented as shown in Equation (14):

$$ReCov(i) \leftarrow Sub*w{:}Rf\ (RGB)x,y,z,I \quad (14)$$

The reconstructed cover for particular f_i further undergoes thorugh secret image extraction procedure for two different modes of operations. Here the system initially again converts the R_f (RGB) → YCbCr[i] with the numerically compatible format of YUV. And further computes the frame indexes for y← y(r,c,1) , u←u(r,c,2) and v←v(r,c,3). The system further again performs wavelet decomposition and computes the coefficient attributes for this extraction operation of *w* as shown in Equation (15),

$$Cexb1,Cexb2 \leftarrow Wd(\ Matrix[y]N)$$

$$LL \leftarrow ExAcoeff(Cexb1,Cexb2,N)$$

$$LH,HL,HH \leftarrow Excoeff(Cexb1,Cexb2\ ,N) \quad (15)$$

Further the system performs a sub-blocking operation with H.264 to generates sub-blocks sub(i, j, n). Finally, the PCA(x) algorithm generates the reconstructed *w*2 after set of operations.

VI. Algorithm Design

The algorithm design for the formulated embedding operations for two different mode of embedding operations is shown as follows:

Numerical Algorithm-I: Formulated Embedding Process in RDH technique

Input: M, f_i, nf, $w2$

Output: Reconstructed cover media [Re(V_i)]

Start

1. Init → M, f_i, nf, $w2$, n$f \in$ M for f_i
2. Enable Tm: [$m1$/$m2$]
3. Construct→cell structure of M{ f_i}
4. Enable : f_{en1}(x). pass in: M{ f_i}, msg→$w2$
5. R1 ,C1← R_f(msg→$w2$)
6. $w2$← $R_f(w2^t)_{R1xC1}$
7. C1,C2 ← Wd(Matrix[y(r,c,1)]$_N$)
8. LL←Acoeff(C1,C2)
9. LH,HL,HH ← Ecoeff(C1,C2,N)
10. Cb1,Cb2 ← Wd(Matrix[ch]$_N$)
11. LLd←Acoeff(Cb1,Cb2)
12. LHd,HLd,HHd ← Ecoeff(Cb1,Cb2,N)
13. Select ch: 1→4
14. n←1
15. Compute sub-blocks correspond to LLd
    - For i← 1 to r
      - For j← 1 to c
        1. sub(i,j,n)← LLd((i,r),(j,c))
        2. n←n+1
      - End
    - End
16. Enable custom function of PCA(x) : pass in sub(i,j,n)
17. PCA(x): pass out Fdata ← Eign(CovM)^T* Adjst // here Adata← sub_{double}-sub_{mean}
18. R_f(Sub*w)
19. Reconstruct Odata ← Sub*w(i)
20. Apply Filp-array up → down on Odata
21. construct
22. new_y(r,c,1)← IDWT2(LLd,LHd,HLd,HHd)
23. new_y(r,c,1)← IDWT2(new_y(r,c,1),LH,HL,HH)
24. y(r,c,1), u(r,c,2), v(r,c,3)
25. compute numerical form of y
26. Perform reconstruction from YCbCr → R_f (RGB)

End

The computation of the formulated embedding approach for mode type-1 in DWT model whole perform the PCA analysis for component of sub(i,j,n) further generates Final data attributes considering the following Equation (16).

$$\text{Fdata} \leftarrow \text{Eign(CovM)T* Adjst} \quad (16)$$

Further it reconstructs the Sub*w with resizing factor and generates the original form of data Odata. It also enhances the embedding efficiency by performing flip-array up-down approach. Further the system constructs the new_y(r,c,1) followed by reconstruction of R_f (RGB). The extensive analysis of the formulated approach shows that the embedding efficiency has significantly increased owing to the involvement of PCA. The numerical outcome is further shown in the result and analysis section.

The algorithm for extraction procedure is shown as follows:

Numerical Algorithm-II: The w Extraction Procedure

Input: Sub*w, R_f (RGB) C_m

Output: ReCov(i)

Start

1. Init → Sub*w, R_f (RGB), nf, Dim ←(R,C)
2. Tm: [$m1$/$m2$], f_{ex}(x)
   - a. For each frame f_i
     - i. Enable : ReCov(i) ← Sub*w:R_f $(RGB)_{x,y,z,i}$
     - ii. Convert: (RGB) → YCbCr[i]
   - b. End
3. Cexb1,Cexb2 ← Wd(Matrix[y]$_N$)
4. LL←ExAcoeff(Cexb1,Cexb2,N)
5. LH,HL,HH ← Excoeff(Cexb1,Cexb2 ,N)
6. Perform Sub-block operation with H.264/AVC
7. sub(i,j,n)
8. R_f ($w2$)←PCA(x)

End

The secret image bits extraction procedure has been verified for before attack and under the attack's scenario with the simplified computing steps. Here the system basically considers 9 different set of attacks in the form forms of AS = {AS1, AS2, AS3, AS4, AS5, AS6, AS7, AS8, AS9}. The performance of imperceptibility along with the signal quality evaluation is further done in the numerical outcome section. The performance estimation of signal quality considers PSNR as a metric to justify the outcome.

VII. Result and Analysis

The study outcome to justify the performance of the formulated embedding approach in RDH process is shown and discussed in this section. The study in this section not only estimates the PSNR, NC outcome but also assess the time complexity for above two algorithms of embedding and extraction with respect to CPU time. The analysis clearly shows that the experiments are conducted for a cover media named Akiyo.CIF of type Y4M, where the frame size is considered to be CIF (288 x 352). The size on the disk for the CM found to be approximately 43.5 MB (44,552 KB). The message media is considered as a single image file of TIF and its size on the disk is approximately 5KB. The numerical experiments are further realized in a computing environment of MATLAB R2015a environment on a PC with CPU Intel(R) Core (TM) i5-3470 @ 3.2 GHZ with 4-GB of RAM. The numerical computing is carried out considering a set of explicit custom functions invoked during the simulation of the above-mentioned numerical modeling of i) Uncompressed cover media and secret image processing, ii) Formulated approach of embedding and iii) Extraction process in RDH. The simulation outcome from the numerical modeling takes a set of observation of each frame and its visual perception measures correspond to the input CM and the embedded secret data in the form of image. To justify the reversibility and proper data hiding performance the system model considers two different scenarios. Here in one scenarios secret image is simply extracted considering Algorithm-II from the embedded

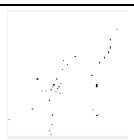
CM and the visual perception with respect to frame number is obtained for both CM and *w*. In another scenario the study considers *w* extraction after performing a set of attacks on the embedded CM. The similar sort of observations are carried during the reconstruction process of the original CM frame along with the reconstructed frame after embedding and also the visual perception of frame after performing a set of attacks conditionally.

The visual perception score for the original image (Table I(A)) and the extracted image on shows higher similarity score in the absence of attacks which shows that the proposed RDH model attains good reversibility while fulfilling the requirements of PSNR for the reconstruction scenario. However, the experiments for VP are further also extended to generalize the robustness of the system in the presence of nine different types of attacks AS ={AS1, AS2, AS3, AS4, AS5, AS6, AS7, AS8, AS9}. The visualization to show the attack effect on the extracted secret image bits is provided in Table I(B). It considers embedding process and a specific type of attack at a time performed on the embedded CM.

TABLE I. (A): VISUALIZATION OF ORIGINAL SECRET IMAGE, EXTRACTED SECRET IMAGE FROM BITSTREAM (BEFORE ATTACK)

Original Secret Image (*w*2)	**Extracted Secret Image (*w*2) from the Bitstream (Before Attack)**
	

(B): VISUALIZATION OF ORIGINAL SECRET IMAGE, EXTRACTED SECRET IMAGE FROM BITSTREAM (AFTER ATTACK EFFECTS)

Types of attacks performed on *w*2	**Visualization of the extracted *w*2 (After Performing Attack)**
1.Speckle noise	
2. Gaussian noise	
3. Histogram Equalization	
4. Salt and pepper noise	
5. Poisson noise	
6. Frame averaging	
7. JPEG compression	
8. Gamma correction	
9. Median Filtering	

The interpretation of the visual outcome here shows that how the extracted secret image looks like while the embedded CM of Akiyo.CIF undergoes through a set of attacks conditionally. The outcome obtained clearly shows that in all the cases of attacks the system attains considerable outcome of visual perception for secret image bits. However, the effects of Gamma correction are found more on the extracted secret image. The system further also performs analysis on the visual perception and the parameters for embedding efficiency for data hiding aspects for the CM which is further shown in the following Table II.

TABLE II. NUMERICAL OBTAINED FOR PSNR, NC FOR CM= AKIYO.CIF AFTER EMBEDDING AND EXTRACTION PROCESS

Original frame from C_m	**Frame after Embedding Process**	**Frame After Attack**
AS-1: PSNR(Ov/Rv) =47.0357	AS-1: NC(Ow/Rw) =0.72456	AS-1 NC(Ow/Rw)=0.767
AS-2: PSNR(Ov/Rv) =48.77	AS-2: NC(Ow/Rw) =0.55514	AS-2 NC(Ow/Rw)=0.57004
AS-3: PSNR(Ov/Rv) = 50.4078	AS-3: NC(Ow/Rw) =0.36798	AS-3 NC(Ow/Rw)=0.574
AS-4: PSNR(Ov/Rv) = 44.4851	AS-4: NC(Ow/Rw) =0.6484	AS-4 NC(Ow/Rw)=0.68499
AS-5: PSNR(Ov/Rv) =50.77	AS-5: NC(Ow/Rw) =0.545	AS-5 NC(Ow/Rw)=0.5654
AS-6: PSNR(Ov/Rv) = 48.7379	AS-6: NC(Ow/Rw) =0.44532	AS-6 NC(Ow/Rw)=0.67
AS-7: PSNR(Ov/Rv) = 43.13	AS-7: NC(Ow/Rw) =0.5364	AS-7: NC(Ow/Rw)=0.39645
AS-8: PSNR(Ov/Rv) = 50.41	AS-8: NC(Ow/Rw) =0.476	AS-8: NC(Ow/Rw)=0.697
AS-9: PSNR(Ov/Rv) = 52.41	AS-9: NC(Ow/Rw) =0.486	AS-9: NC(Ow/Rw)=0.687

The study incorporates numerous performance metrics to validate the system such as PSNR and NC. Here the PSNR performance is obtained considering the following standard form of mathematical Equation (17) as below.

$$\text{PSNR} = 10 \times \log\left(\frac{\text{MAX}^2}{\text{MSE}}\right) \quad (17)$$

Here MSE refers to mean square error computation for the original frame and the embedded frame of CM. And also, MAX refers to the maximum possible pixel range of each frame. The system also considers another performance metric of NC which is attributed as a measure to assess the embedding efficiency and the robustness of the proposed H.264/AVC based embedding operations against different forms of attacks. It measures the similarity index between the frame after embedding and the frame after attack. It is also applicable to the original secret image and extracted secret image similarity measures. The standard form of numerical model to evaluate this NC is given as below.

$$\text{NC} = \frac{\sum\sum[\text{Ow}(i,j)\times\text{Rw}(i,j)]^2}{\left(\left(\sqrt{\sum\sum\text{Ow}(i,j)^2}\right)\times\left(\sqrt{\text{Rw}(i,j)^2}\right)\right)} \quad (18)$$

The performance metric of NC here evaluates the robustness and embedding efficiency accomplished by the proposed algorithm (P-RDH). The analysis of imperceptibility from the PSNR outcome for the original frame of $\mathbf{C_m}$ and the embedded frame shows that the system accomplishes considerable PSNR during the reconstruction of original CM of Akiyo. CIF even though in the presence of different types of attacks. The average PSNR (dB) outcome for CIF (288 x 352) is obtained as 52.7379dB which is comparable to the conventional baselines of RDH (C-RDH). The visual outcome of the PSNR is also shown with the following Fig. 3. The system outcome is further assessed for NC to justify the efficiency of encoding process in terms of embedding efficiency and robustness for different conditions. The NC computation here also justifies the robustness of the system modeling during the attack scenario.

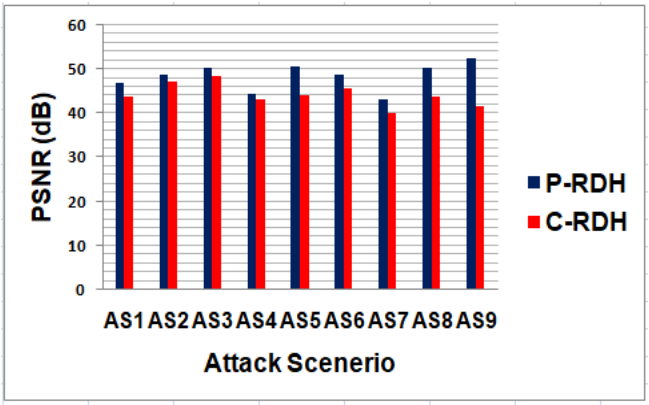


Fig. 3. Analysis of PSNR Outcome for CM Reconstruction.

The analysis of the outcome of NC shows that with the variation of embedding strength the system achieves better normalized correlation not only in the case of secret image of Lena but also in the case of reconstructed frames of CM. This indicates that the proposed approach P-RDH outperforms C-RDH to a greater extent under different operational conditions and also ensures higher reconstructed signal quality. The system performance in this chapter also shows that the P-RDH attains superior performance from the viewpoint of computing too. It attains CPU execution time of overall 143.166324 seconds during the computing process of embedding whereas in the existing system it is quite higher. The reconstruction process accomplishes the CPU time of 30.7447secs for each frame which is also found significant as compared to the existing baselines.

The prime reason behind this is the proposed encoding applies PCA based component analysis is to generate significant coefficient attributes from both the secret image bits and cover-media which in extraction process helps. Thereby to a greater extent the system outperforms the C-RDH by means of PSNR and CPU computing for embedding. It also enhances the embedding capacity irrespective of the message size.

VIII. Result and Discussion

The outcome obtained from the current study showcase that proposed scheme is highly resilient to different forms of attacks which the existing schemes didn't have reported for [21]-[25]. A simplified assessment towards the optimal data hiding scheme presented in [22] has claimed about higher reversibility degree, however it fails to identify the threat on dynamic scenarios. The system of proposed RDH is found to offer higher robustness towards attack of various forms (i.e., Speckle noise, Gaussian noise, Histogram equalization, salt and pepper, Poisson noise, jpeg compression and frame averaging, Gamma correction and median filtering), hence attain efficient imperceptibility from data security viewpoint and this critical aspect has not much explored in the existing studies [30]-[36]. Further, it is also noted that the outcome of this RDH in this research aspect is also found comparable with the existing baseline solution for PSNR, NC and computing time. From the perspective of the computational efficiency, the study outcome is also found to support the claim that it balances the trade-off between EC and the visual perception while accomplishing faster CPU execution with PCA based solution for H.264/AVC. Similarly, the attack analysis has been carried out for the CM too where it shows higher PSNR efficiency in post embedding phase of reconstruction of the signal whereas in the after-attack scenario the signal quality in the measure of PSNR got slightly affected in case-8. Such case was not evident in the recent work too [44]-[50]. However, in the other cases the system found higher PSNR outcome with good reversibility of both secret message and the CM. Therefore, from the overall perspective of study outcome, it shows that proposed system offers better performance in data hiding compared to majority of the related existing models.

IX. Conclusion

This research study introduces a novel computing framework of RDH mechanism which ensures better embedding capacity under both attack and un-attack scenarios. The simplistic design approach of the embedding ensures better flow of execution and also retains higher PSNR with imperceptivity for extraction process of both secret image and cover media. The outcome also shows that in 1-2 cases of

attack scenario the PSNR performance got affected for the reconstructed signals but still higher imperceptibility is achieved. The system is not only robust against different form of attacks as on an average the NC score is obtained towards 1 but also it can be seen that it balances the trade-off between EC and CPU computing time while maintaining acceptable PSNR range for the reconstructed frames of CM. This indicates the performance efficiency of the H.264/AVC based system. It also further ensures that the good reversibility is happening for both Akiyo.CIF and Lena.TIF. The system performance of embedding still has a scope to be improvised despite its robustness against different form of attacks for that reason the study in the future work of this research targets to enhance the optimization procedure to strengthen the embedding procedure of RDH so that it can ensure better EC, PSNR and execution time trade-off for different range of cover media types and secret image. Apart from this, the prime significance of the proposed study is that it offers an efficient computational model towards framing up RDH, which can be applied over any form of video steganography application owing to its robustness. Without losing potential quality of the video, the proposed system is capable of leveraging better embedding capacity without using any iterative scheme or sophisticated operation involved in it. Hence, the scope of adopting the proposed RDH model is quite higher in multimedia application to a large extent.

REFERENCES

[1] Barton JM, inventor; Barton, James M., assignee. Method and apparatus for embedding authentication information within digital data. United States patent US 5,646,997. 1997 Jul 8.

[2] J. Fridrich, Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge, U.K.: Cambridge Univ. Press, 2009.

[3] Y. Q. Shi, Z. Ni, D. Zou, C. Liang, and G. Xuan, ``Lossless data hiding: Fundamentals, algorithms and applications," in Proc. IEEE Int. Symp. Circuits Syst., vol. 2. May 2004, pp. 3336.

[4] Y. Q. Shi, ``Reversible data hiding," in Proc. Int. Workshop Digit. Watermarking, 2004, pp. 112.

[5] R. Caldelli, F. Filippini, and R. Becarelli, ``Reversible watermarking techniques: An overview and a classication," EURASIP J. Inf. Secur., vol. 2010, 2010, Art. no. 134546.

[6] J. M. Barton, ``Method and apparatus for embedding authentication information within digital data," U.S. Patent 5 646 997, Jul. 8, 1997.

[7] C. W. Honsinger, P. W. Jones, M. Rabbani, and J. C. Stoffel, ``Lossless recovery of an original image containing embedded data," U.S. Patent 6 278 791, Aug. 21, 2001.

[8] F. Bao, R.-H. Deng, B.-C. Ooi, and Y. Yang, ``Tailored reversible watermarking schemes for authentication of electronic clinical atlas," IEEE Trans. Inf. Technol. Biomed., vol. 9, no. 4, pp. 554563, Dec. 2005.

[9] G. Coatrieux, C. Le Guillou, J.-M. Cauvin, and C. Roux, ``Reversible watermarking for knowledge digest embedding and reliability control in medical images," IEEE Trans. Inf. Technol. Biomed., vol. 13, no. 2, pp. 158165, Mar. 2009.

[10] K. L. Chung, Y. H. Huang, P. C. Chang, and H. Y. M. Liao, ``Reversible data hiding-based approach for intra-frame error concealment in H.264/AVC," IEEE Trans. Circuits Syst. Video Technol., vol. 20, no. 11, pp. 16431647, Nov. 2010.

[11] D. Coltuc and I. Caciula, ``Stereo embedding by reversible watermarking: Further results," in Proc. Int. Symp. Signals, Circuits Syst., Jul. 2009,pp. 14.

[12] X. Tong et al., ``Stereo image coding with histogram-pair based reversible data hiding," in Proc. Int. Workshop Digital-Forensics Watermarking, 2014, pp. 201214.

[13] X. Wang, C. Shao, X. Xu, and X. Niu, ``Reversible data-hiding scheme for 2-D vector maps based on difference expansion," IEEE Trans. Inf. Forensics Security, vol. 2, no. 3, pp. 311320, Sep. 2007.

[14] F. Peng, Y.-Z. Lei, M. Long, and X.-M. Sun, ``A reversible watermarking scheme for two-dimensional CAD engineering graphics based on improved difference expansion," Comput.-Aided Design, vol. 43, no. 8, pp. 10181024, 2011.

[15] K. Hwang and D. Li, ``Trusted cloud computing with secure resources and data coloring," IEEE Internet Comput., vol. 14, no. 5, pp. 1422, Sep. 2010.

[16] J. Fridrich, M. Goljan, and R. Du, ``Invertible authentication," Proc. SPIE, vol. 4314, pp. 197208, Aug. 2001.

[17] M. Goljan, J. J. Fridrich, and R. Du, ``Distortion-free data embedding for images," in Proc. 4th Inf. Hiding Workshop, 2001, pp. 2741.

[18] J. Fridrich, M. Goljan, and R. Du, ``Lossless data embeddingNew paradigm in digital watermarking," EURASIP J. Adv. Signal Process., vol. 2002, no. 2, pp. 185196, 2002.

[19] G. Xuan, J. Zhu, J. Chen, Y. Q. Shi, Z. Ni, and W. Su, ``Distortionless data hiding based on integer wavelet transform," Electron. Lett., vol. 38, no. 25, pp. 16461648, Dec. 2002.

[20] G. Xuan, J. Chen, J. Zhu, Y. Q. Shi, Z. Ni, and W. Su, ``Lossless datahiding based on integer wavelet transform," in Proc. IEEE Int. Workshop Multimedia Signal Process., Dec. 2002, pp. 312315.

[21] X. Cao, Y. Zhou and J. -M. Guo, "Guest Editorial Introduction to Special Section on Modern Reversible Data Hiding and Watermarking," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 30, no. 8, pp. 2297-2299, Aug. 2020. doi: 10.1109/TCSVT.2020.3002109.

[22] W. Qi, X. Li, T. Zhang and Z. Guo, "Optimal Reversible Data Hiding Scheme Based on Multiple Histograms Modification," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 30, no. 8, pp. 2300-2312, Aug. 2020, doi: 10.1109/TCSVT.2019.2942489.

[23] J. Wang, X. Chen, J. Ni, N. Mao and Y. Shi, "Multiple Histograms-Based Reversible Data Hiding: Framework and Realization," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 30, no. 8, pp. 2313-2328, Aug. 2020, doi: 10.1109/TCSVT.2019.2915584.

[24] B. Ou and Y. Zhao, "High Capacity Reversible Data Hiding Based on Multiple Histograms Modification," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 30, no. 8, pp. 2329-2342, Aug. 2020, doi: 10.1109/TCSVT.2019.2921812.

[25] Y. Ke, M. -Q. Zhang, J. Liu, T. -T. Su and X. -Y. Yang, "Fully Homomorphic Encryption Encapsulated Difference Expansion for Reversible Data Hiding in Encrypted Domain," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 30, no. 8, pp. 2353-2365, Aug. 2020, doi: 10.1109/TCSVT.2019.2963393.

[26] Z. Yin, Y. Ji and B. Luo, "Reversible Data Hiding in JPEG Images With Multi-Objective Optimization," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 30, no. 8, pp. 2343-2352, Aug. 2020, doi: 10.1109/TCSVT.2020.2969463.

[27] Mohammadi, Ammar, Mansor Nakhkash, and Mohammad Ali Akhaee. "A high-capacity reversible data hiding in encrypted images employing local difference predictor." IEEE Transactions on Circuits and Systems for Video Technology 30.8 (2020): 2366-2376.

[28] A. Roy and R. S. Chakraborty, "Toward Optimal Prediction Error Expansion-Based Reversible Image Watermarking," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 30, no. 8, pp. 2377-2390, Aug. 2020, doi: 10.1109/TCSVT.2019.2911042.

[29] Peng, Fei, et al. "Separable robust reversible watermarking in encrypted 2D vector graphics." IEEE Transactions on Circuits and Systems for Video Technology 30.8 (2020): 2391-2405.

[30] Wang, Xiang, Xiaolong Li, and Qingqi Pei. "Independent embedding domain based two-stage robust reversible watermarking." IEEE Transactions on Circuits and Systems for Video Technology 30.8 (2019): 2406-2417.

[31] J. Tian, “Reversible data embedding using a difference expansion,” IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.

[32] L. Kamstra and H. J. A. M. Heijmans, “Reversible data embedding into images using wavelet techniques and sorting,” IEEE Trans. Image Process., vol. 14, no. 12, pp. 2082–2090, Dec. 2005.

[33] W. L. Tai, C. M. Yeh, and C. C. Chang, "Reversible data hiding based on histogram modification of pixel differences", iEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 6, pp. 906-910, Jun. 2009.

[34] J. Tian, "Reversible data embedding using a difference expansion", iEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890-896, Aug. 2003.

[35] A. M. Alattar, "Reversible watermark using the difference expansion of a generalized integer transform", iEEE Trans. image Process., vol.13, no. 8, pp. 1147-1156, Aug. 2004.

[36] L. Kamstra and H. 1. A. M. Heijmans, "Reversible data embedding into images using wavelet techniques and sorting", iEEE Trans. Image Process., vol. 14, no. 12, pp. 2082-2090, Dec. 2005.

[37] H. J. Kim, V. Sachnev, Y. Q. Shi, J. Nam and H. Choo, "A Novel Difference Expansion Transform for Reversible Data Embedding," in IEEE Transactions on Information Forensics and Security, vol. 3, no. 3, pp. 456-465, Sept. 2008.

[38] S. Liu and W. Tsai, "Line-Based Cubism-Like Image—A New Type of Art Image and its Application to Lossless Data Hiding," in IEEE Transactions on Information Forensics and Security, vol. 7, no. 5, pp. 1448-1458, Oct. 2012.

[39] Wang, H. Lin, X. Gao, W. Cheng and Y. Chen, "Reversible AMBTC-Based Data Hiding With Security Improvement by Chaotic Encryption," in IEEE Access, vol. 7, pp. 38337-38347, 2019.

[40] H. Yao, X. Liu, Z. Tang, Y. Hu and C. Qin, "An Improved Image Camouflage Technique Using Color Difference Channel Transformation and Optimal Prediction-Error Expansion," in IEEE Access, vol. 6, pp. 40569-40584, 2018.

[41] Y. Ke, J. Liu, M. Zhang, T. Su and X. Yang, "Steganography Security: Principle and Practice," in IEEE Access, vol. 6, pp. 73009-73022, 2018.

[42] M. S. Rahman, I. Khalil and X. Yi, "Reversible Biosignal Steganography Approach for Authenticating Biosignals Using Extended Binary Golay Code," in IEEE Journal of Biomedical and Health Informatics, vol. 25, no. 1, pp. 35-46, Jan. 2021.

[43] Wu, J. Dugelay and Y. Shi, "Reversible Image Data Hiding with Contrast Enhancement," in IEEE Signal Processing Letters, vol. 22, no. 1, pp. 81-85, Jan. 2015.

[44] X. Xie, C. Chang and K. Chen, "A High-Embedding Efficiency RDH in Encrypted Image Combining MSB Prediction and Matrix Encoding for Non-Volatile Memory-Based Cloud Service," in IEEE Access, vol. 8, pp. 52028-52040, 2020.

[45] S. Weng, Y. Zhao, J. Pan and R. Ni, "Reversible Watermarking Based on Invariability and Adjustment on Pixel Pairs," in IEEE Signal Processing Letters, vol. 15, pp. 721-724, 2008.

[46] W. Wang, C. Huang and S. Wang, "VQ Applications in Steganographic Data Hiding Upon Multimedia Images," in IEEE Systems Journal, vol. 5, no. 4, pp. 528-537, Dec. 2011.

[47] N. Zhou, M. Zhang, H. Wang, Y. Ke and F. Di, "Separable Reversible Data Hiding Scheme in Homomorphic Encrypted Domain Based on NTRU," in IEEE Access, vol. 8, pp. 81412-81424, 2020. doi: 10.1109/ACCESS.2020.2990903.

[48] I. C. Dragoi and D. Coltuc, "On the Security of Reversible Data Hiding in Encrypted Images by MSB Prediction," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 187-189, 2021. doi: 10.1109/TIFS.2020.3006382.

[49] S. Li, L. Hu, C. Sun, L. Chi, T. Li and H. Li, "A Reversible Data Hiding Algorithm Based on Prediction Error With Large Amounts of Data Hiding in Spatial Domain," in IEEE Access, vol. 8, pp. 214732-214741, 2020. doi: 10.1109/ACCESS.2020.3040048.

[50] S. Sheidani, A. Mahmoudi-Aznaveh and Z. Eslami, "CPA-Secure Privacy-Preserving Reversible Data Hiding for JPEG Images," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 3647-3661, 2021. doi: 10.1109/TIFS.2021.3080497.