I. J. Computer Network and Information Security, **2021, 2, 53-65**
Published Online April 2021 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2021.02.05

A Novel Secure Data Hiding Technique into Video Sequences Using RVIHS

Vinay D. R.
Malnad College of Engineering, Hassan – 573202, India
E-mail: vinu.ise@gmail.com

Ananda Babu J.
Malnad College of engineering, Department of Information science and engineering, Hassan-573202, India
E-mail: babu.tiptur@gmail.com

Received: 03 December 2020; Revised: 10 January 2021; Accepted: 25 February 2021; Published: 08 April 2021

Abstract: Most of the present hiding techniques on video are considered over plaintext domain and plain video sequences are used to embed information bits. The work presented here reveals the novelty for information embedding in a video sequence over the ciphered domain. The carrier video signal is encrypted using chaos technique which uses multiple chaotic maps for encryption. The proposed reversible video information hiding scheme (RVIHS) exhibits an innovative property that, at the decoding side we can perfectly extract the information along with carrier video without any distortion. The public key modulation is a mechanism used to achieve data embedding, whereas in secret key encryption is not required. The proposed approach is used to differentiate encoded and non-encoded picture patches at decoder end by implementing 2 class Support Vector Machine grouping. This helps for us to retrieve the original visual sequence with embedded message and to scale up embedding capacity. The experiment is conducted using real time videos for embedding the information. The outcome of proposed work brings about best embedding capacity, compared to existing techniques.

Index Terms: RVIH, SVM, MSE, 2D-Logistic Map, 3D Lorenz map, chaotic map.

1. Introduction

Most of the present hiding techniques on video are considered over plaintext domain and plain video sequences are used to embed information bits. The existing approaches mainly focused on lossless compression technique to compress definite image structures to get space for data embedding. This method gives us moderately limited embedding capacity and suffered on watermarked visual distortion. Traditional work reveals embedding the information in static images. However, data embedding in images limits the embedding capacity. To overcome this problem, the proposed work reveals the novelty for information embedding in a video sequence over the ciphered domain. This increases the embedding capacity as well as reduces the bit error.

The research objectives mainly include, a) Establishing data hiding technique using advanced steganographic algorithms in video sequences, b) Establishing data encryption technique using advanced cryptographic algorithms in video sequences, c) Increasing the embedding capacity, d) Reducing the bit error rate. The work introduced here is to propose an encrypted domain RIHV approach by precisely having above strategy preferences. The novel technique used to hide data over public key inflection technique and accomplishes information detach by developing the arithmetic differentiability of encoded and non-encoded image chunks. As actual image and decoded data bits are combined together, the given method comes under non-separable RIHV results. The approach helps us to accomplish faultless reformation of original visual frame with embedded data bits and achieves more embedding capacity.

2. Related Work

The CABAC bin-string substitution [1] is proposed for partially encrypted AVC streams and it's emerged as an improvised level of hiding technique. To improve the structural deterioration significantly, work is carried out to perform Luma prediction encryption with motion vector and residual encryption. The information submerge is achieved in encoded state and approach is used towards video confidentiality. The outcome of the investigation viewed applied scheme can accomplish high inserted capacity and better scrambling performance than the method in [2]. The high-quality videos facing a real time problem due to transmission delay. The proposed method gives equal importance for videos which are poor illumination to high quality and data hiding. The technique [3] used to improve the video quality in streaming by performing contrast enhancement. The novel approach is to perform visual contrast enhancement to strictly preserve visual file size. The result shows the better video quality to become useful in real-world scenarios. The author [4] proposed the novel hiding strategy to an AVI video for the embed a hidden picture. Inside 1 among the structure in a video. When contrasted with current methodologies, in this procedure does a two-level encoded technique that utilizes 2 bit position in the specific structure video. Because the setting of the secret image in four unique quadrants, the size of the video or the nature of the secret image stays same when encryption along these lines giving curiosity. Information as the video, which has the size is perfect to the length of bearer video can likewise be encrypted. The recommendation extensively expands nature of the hidden information that a program convey safely. That was additionally reached out by changing situating of hidden bits, altogether build unsystematic. The author [5] work infer that the data got encrypted to cipher by following SPN type of block cipher. The embedding can be done to cipher text by applying sudoku puzzle as a key. The block cipher resembles a robust and new encryption model by comparing with AES (Advanced Encryption Standard) gives an improved level of security interns of attack. The SPN architecture looks quite different than AES architecture in round key mixing method. The authors have used steganography and cryptographic method as well sudoku game for improvise the freedom in high level. The Author [6] proposed steganography technique dependent on Video Sparse Representation (V-SR). In deed appropriate word reference, KSVD calculation was apply for the DCT measure of Y part identified with cover video frames. The OMP technique is used to calculate both sparse representation and video frames. The proposed algorithm performance was evaluated in terms of PSNR (Peak Signal to Noise Ratio), Hiding Ratio, Bit Error Rate and then secret message Similarity. The outcomes exhibit good invisibility and outperformed by comparing existing algorithms [7-10]. [11] Proposed a motion-vector based steganography for MPEG-2 compression method. In homogenous regions, motion vectors are altered to embed the secret bit. For embedding purpose and to improve statistical un-detectability will use higher motion vectors. We can extend this research further for 3D video steganography. The blind attack can go for investigate steganographic embedding without any clue on embedding algorithm [12] is a more generic behavior and it’s generally hard. [13] The paper focuses on hiding secret information to LZW codes present in cover media. It covers encoding method such as altered transport to front (MTF) technique for secret data follows LZW of coding approach to get LZW codes. The scheme helps us to improvise hiding capacity for the scale of gray and text information by 28.1-381 % and 109.6-203.6% respectively comparing to state of art techniques. [14] The author taken H.264/AVC videos for to achieve reversible data hiding technique. The embedded blocks are selected based on macroblocks with 4*4-dimension intra frame prediction modes. The pairing can be done with last zero QDCT coefficients in completely 4*4 blocks. The outcome gives us low distortion and high embedding capacity compared to LSB method. The experiment results give better video quality when we keep common embedding payloads. [15] Author implements shifting free (Reversible Data Hiding) RDH by using multiple-bit embedding technique. The data hiding approach is simplified by avoiding multiple layers hiding and difference histogram computation. Stego-image quality got improved due to no-shifting. The proposed method leads to superior performance and evidenced with paired t-test by carrying broad simulations. RDH technique permits decoder to not only for extracting embedded information, sooner helps to reconstruct carrier image with less distortion [16, 17]. [18] The novel approach is encryption at two level that is to data decipher, means way the original decomposing of secret image and embedding can be done at which frame acknowledged. The embedded quality of hidden picture and video dimensions is not modified even initial & behind secret data encryption. Any type of multimedia information to be stored in secret image and further it can be predictable and obtained. In [19] author proposed matrix array symmetric key (MASK) for key generation and chaos-based image encryption for image cryptography. In [20] author uses the concept of video Steganography, where the data is hidden behind the frames of videos. They provide two level of security to the data i.e. Steganography and cryptography.in [21] a new data hiding algorithm based on pixel pairs using chaotic map is proposed. Data hiding scheme is created by applying modulo function to pixel pairs. In [22] author proposed a new RGB shuffling method proposed. The concept of encryption using RGB Shuffling is shuffling all of RGB element to distort the image. RGB Shuffling method will shuffle the RGB each pixel of image depends on the input password from user. The basic step of RGB shuffling is adding RGB element with ASCII password, invers and shuffle it. In [23] author proposed Image Steganography with watermarking using LSB and interpolation Techniques. They have designed a system that will allow a user to securely transfer text messages by hiding them in a digital image file using the local characteristics within an image. A combination of image Steganography and interpolation with watermarking provides a strong backbone for its security. In [24] author proposed the particle swarm optimization. The particle swarm optimization algorithm is applied to the spatial domain technique. The improved algorithm called the accelerated particle swarm optimization converges faster than the usual particle swarm optimization and improves the performance. In [25] In author have proposed the hybrid representation for the embedding of the data, which utilizes the random pattern embedding along with the cryptography for the higher steganography security levels.

3. Methodology

3.1. Video Encryption/Hiding Scheme

In this method each video frame is subjected to encryption followed by data hiding in ciphered domain.

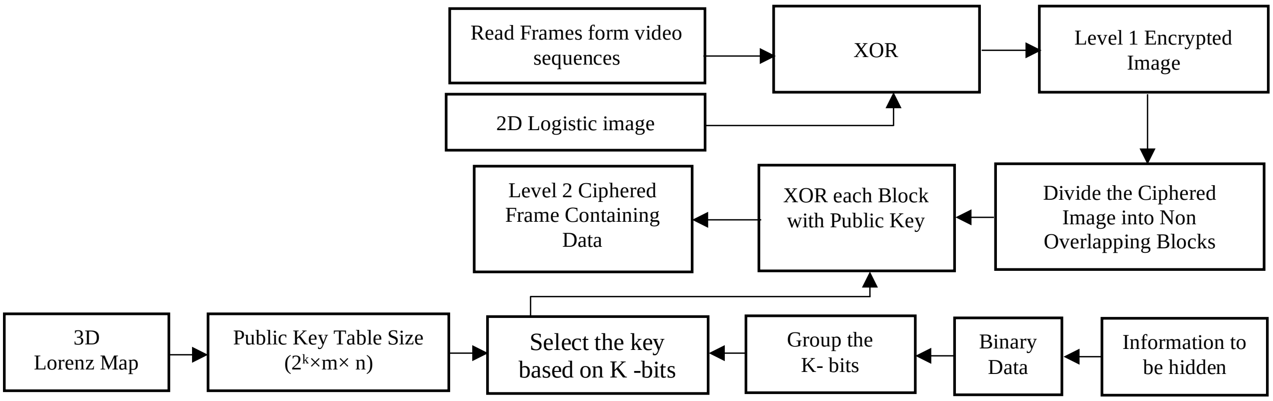

Read Frames form video sequences
XOR
Level 1 Encrypted Image
2D Logistic image
Level 2 Ciphered Frame Containing Data
XOR each Block with Public Key
Divide the Ciphered Image into Non Overlapping Blocks
3D Lorenz Map
Public Key Table Size (2ᵏ×m× n)
Select the key based on K -bits
Group the K- bits
Binary Data
Information to be hidden

Fig.1. The Proposed Data Hiding technique

Data Hiding

1. Determine the type of the input image frame.
2. Generate a set of random sequences using 2D Logistic map.
3. Perform XOR operation with video frame and random matrix.
4. Generate the information to be hidden.
5. Convert the generated information into binary stream using threshold value and group the stream into K bits.
6. Generate the chaotic sequence using 3D Lorenz Map.
7. Create a Public key matrix table of size $2^k \times M \times N$ using the chaotic sequence. (Where $M \times N$ is the total number of blocks).
8. Select the key from the public key table based on the K number of bits.
9. Divide the level 1 ciphered frame into non overlapping blocks.
10. XOR each block with selected public key to obtain final level 2 ciphered frame containing data.

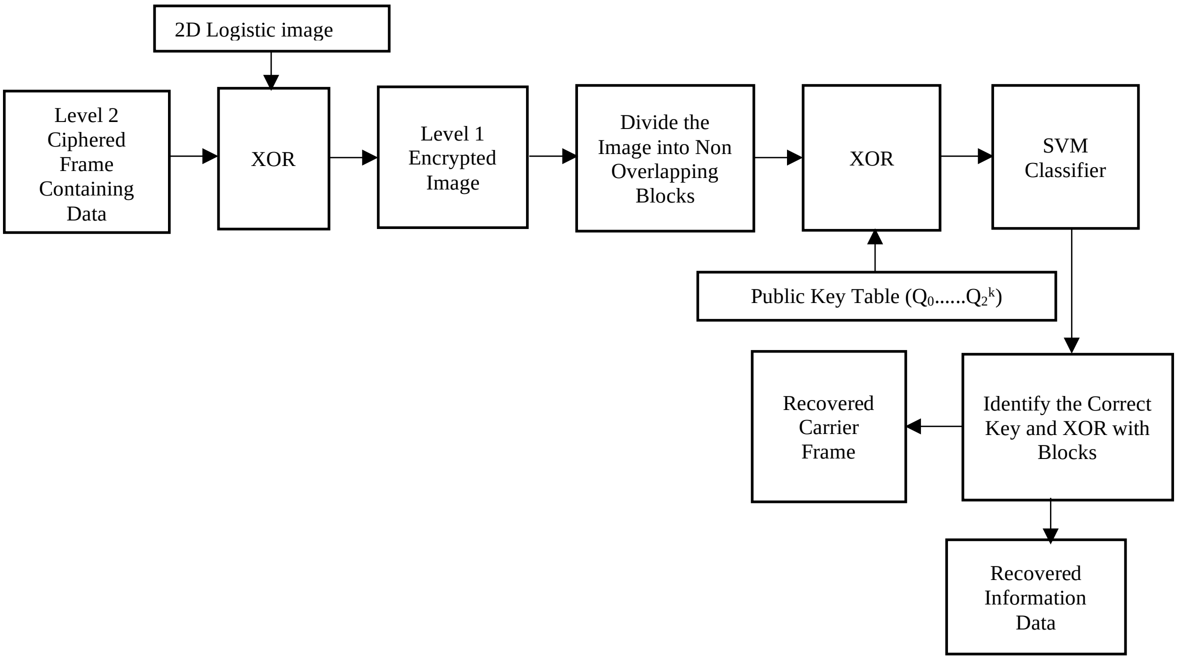

2D Logistic image
Level 2 Ciphered Frame Containing Data
XOR
Level 1 Encrypted Image
Divide the Image into Non Overlapping Blocks
XOR
SVM Classifier
Public Key Table (Q₀......Q₂ᵏ)
Recovered Carrier Frame
Identify the Correct Key and XOR with Blocks
Recovered Information Data

Fig.2. The Proposed Data Retrieving technique

Data Extraction

1. Read the Level2 Ciphered Frame.
2. Perform XOR operation between the Level2 Ciphered Frame and 2D Logistic map to obtain second level decrypted image.
3. Divide the resultant image into non overlapping blocks of size X/block size x Y/block size where X and Y size of the image.
4. Perform XOR operation for each block with key present in the public table.
5. The resultant block is identified as encrypted or non-encrypted by extracting the features like entropy, variance, histogram, directional features, correlation and standard deviation for classifying the obtained features using Support Vector Machine classifier (SVM).
6. The SVM result provides information data for which the selected block decoded properly.

3.2. Reversible Video Information Hiding Scheme (RVIHS)

In spite of having keen encryption method personalized to situation of encryption-based data hiding, here we concentrated towards the predictable stream cipher useful in regular format. It means, will perform bitwise XORing of key stream with plaintext to generate cipher text. If it's not mentioned, will go for assume using stream cipher AES in CTR mode.

The resultant information hiding standard on encrypted domain gives practically an added advantage for two reasons.

1) One of the most standard and trustworthy encryption tools is stream cipher with regular format, because of demonstrable security and implemented hardware/software efficiency at its best. It is infeasible to convince end users to accept novel encryption methods which are not properly examined.
2) The encryption is already performed to huge quantity of data by flow cipher in regular path. During engaged flow of a cipher, the encrypted picture was obtained by

$$[[\mathbf{I}]] = \mathrm{Enc}(\mathbf{I}, R\ ) = \mathbf{I} \oplus \mathbf{R} \tag{1}$$

Where **I** and [[**I**]] represents the original and the ciphered video frame. Here, **R** stand for the key flow obtained by the hidden encoded key *K*. The present job assumes all images are of 8 bits without losing its generality. All the way through this task, we use [[**u**]] to indicate the ciphered form of **u**. undoubtedly, the original visual arrangement can get by implementing the beneath decryption function:

$$\mathbf{I} = \mathrm{Dec}([[\mathbf{I}]], R\ ) = [[\mathbf{I}]] \oplus \mathbf{R} \tag{2}$$

As stated before, the ciphered single frame [[**I**]] now assists as the concealment to provide space for hidden data. We first split [[**I**]] into a sequence of non-overlapping chunks $[[\mathbf{I}]]_i$'s of dimension $m \times n$, where i was index block. Every block was intending transport k bits of data. Allowing total block numbers inside frame be B and total number Video frames be V, the hiding capability of our recommended approach becomes $k \cdot V \cdot B$ bits.

To authorize better embedding, we suggest $Z = 2^k$ binary *public* keys $\mathbf{E}_0$, $\mathbf{E}_1$…… $\mathbf{E}_{Z-1}$, each of its $l = m \times n \times 8$ bits. All $\mathbf{E}_j$'s, for $0 \le j \le Z - 1$, this was publicly reachable, even hacker also knew it.Public keys are selected initially to the information embedding, confirming to the initial conditions used for Lorentz chaotic map given in equation 3.

To allow proficient hiding, we offer to use $Z = 2^n$ binary *public* keys $\mathbf{E}_0$, $\mathbf{E}_1$…… $\mathbf{E}_{Z-1}$, each of l =m×n×8 bits. Totally $\mathbf{E}_j$'s, for $0 \le j \le Z - 1$, are made to reachable for everyone, that infers the hacker identifies them. These keys were selected initially preceding to the data hiding, as stated in the initial conditions used for Lorentz chaotic map given in equation 3.

$$\begin{aligned} \frac{dX}{dt} &= s(x-y) \\ \frac{dY}{dt} &= y(r-z)-y \\ \frac{dZ}{dt} &= x*Y-b*z \end{aligned} \tag{3}$$

The System exhibits chaotic behaviour when the parameters are having values $s\ is\ equal\ to\ 10, r\ is\ equal\ to\ 28$ and $b = \frac{8}{3}$

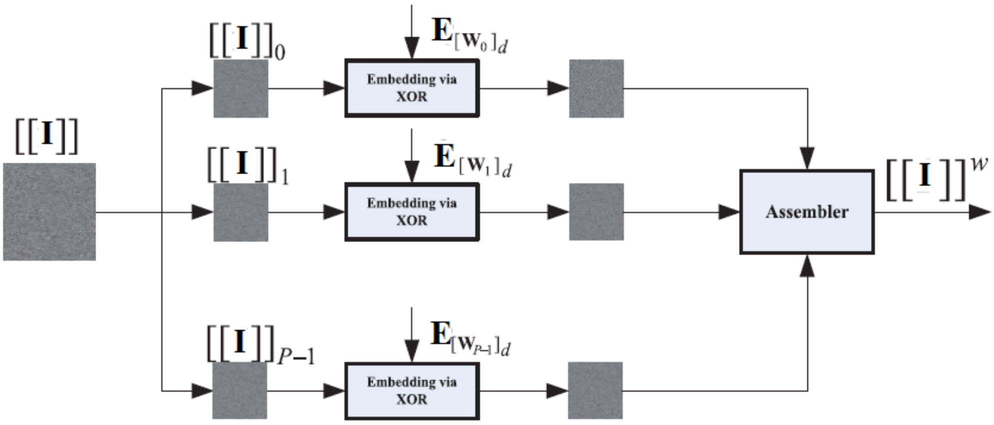


Fig.3. Schematic of information hiding in the single frame over encoded domain.

The planned figure is to introduce information hiding method over encoded domain was revealed in Fig. 3. The proposed approach is not considering the situation of hiding numerous water which marks to the 1 of the blocks, means all block was handled only one time utmost. In a straightforwardness, we consider number of information bits to be inserted in *k a*, in this $a \le b$ and *b* was count of block in the picture. footsteps in carrying out data hiding were précised follow.

1st step: load block index $i = 1$.
2nd step: *Select k* bits of information to hide, refered by $\mathbf{W}_{i.}$
3rd step: Find public key $\mathbf{E}_{[\mathbf{W}i]\,d}$ linked by $\mathbf{W}_i$, in this the index $[\mathbf{W}_i\ ]_d$ is the decimal

Form of $\mathbf{W}_i$.
Let's take an example, when $k = 3$ and $\mathbf{W}_i = 010$, the correlate public key was $\mathbf{E}_{2.}$

4th Step: Hide length-*k information* bits *Wi* into the *i* th block over

$$[[\mathbf{I}]]_i^w\ = [[\mathbf{I}]]_i \oplus \mathbf{E}_{[\mathbf{W}i\ ]d} \tag{4}$$

5th Step: Increase $i = i + 1$ and rewind the Step 2 to 4 unless all information bits are embedded.

In spite of going forward with data decoding and decryption approaches, primarily will go for feature investigation to categorize ciphered and non-ciphered image chunks. We designed classifier based on features exposing important is the given link information decoding and picture recovery method.

3.3. Reversible Video Information Extraction Scheme (RVIES)

The extractor of information center which recovery R key then tries to recuperate the hidden data with actual picture concurrently from $[[I]]^w$, which was expected to be collect effortlessly with no disturbances. The majority of present RIDH schemes will follow same expectation. Because of XOR swappable operation property, the extractor primarily XOR_s $[[I]]^w$ using ciphered key stream R and generates

$$\mathbf{I}^w = [[\mathbf{I}]]^w \oplus \mathbf{R}. \tag{5}$$

The resultant $\mathbf{I}^w$ is then subdivided into a sequence of non-over lapping chunks $\mathbf{I}_i^w$'s of dimension $m \times n$, related to the process accompanied in hiding steps. From (6), consider

$$\mathbf{I}_i^w = \mathbf{I}_i \oplus \mathbf{E}_{[\mathbf{W}i]\,d} \tag{6}$$

The link information extracting, and video frame decrypting are blind signal division problem with **W***i* and **I***i* are don't know. We planning to solve the problem which was on observation: **I***i*, as the real picture block, it exhibits very littel picture form, and tell semantic messages. This **E** [**W***i] d* is compared to $E = \{\mathbf{E}0, \mathbf{E}1\ldots\ldots\ \mathbf{E}_{\mathbf{Z}\text{-}\mathbf{1}}\}$. Then, XOR $\mathbf{I}_i^w$ this **E***j's*, then outcome is **I***i*, that demonstrate form of data. It was shortly, the other outcomes correlate for uncertainly arranged blocks that is differentiated from real form **I***i*.

Most importantly, initially create *S* decoding candidates using XORing $\mathbf{I}_i^w$ with every *Z* publically accessible keys.

$$\mathbf{E}_0, \mathbf{E}_1 \ldots\ldots\ldots \mathbf{E}_{Z-1}.$$

$$\mathbf{I}_i^{(0)} = \mathbf{I}_i^w \oplus \mathbf{E}_0 = \mathbf{I}_i \oplus \mathbf{E}_{[\mathbf{W}_i]_d} \oplus \mathbf{E}_0$$

$$\mathbf{I}_i^{(1)} = \mathbf{I}_i^w \oplus \mathbf{E}_1 = \mathbf{I}_i \oplus \mathbf{E}_{[\mathbf{W}_i]_d} \oplus \mathbf{E}_1$$

$$\mathbf{I}_i^{(S-1)} = \mathbf{I}_i^w \oplus \mathbf{E}_{Z-1} = \mathbf{I}_i \oplus \mathbf{E}_{[\mathbf{W}_i]_d} \oplus \mathbf{E}_{Z-1} \tag{7}$$

As informed initially, above Z candidates will have $\mathbf{I}i$, then others in form of

$$\mathbf{I}_i^{(t)} = \mathbf{I}_i \oplus \mathbf{E}_{[\mathbf{W}_i]_d} \oplus \mathbf{E}_t \tag{8}$$

Where $t \neq [\mathbf{W}i]\ d$.

The outcome $\mathbf{I}_i^{(t)} = \mathbf{Enc}(\mathbf{I}_i \oplus \mathbf{E}_{[\mathbf{W}_i]_d} \oplus \mathbf{E}_{t)}$ refers for encoded version of $\mathbf{I}i$ with equal key flow being $\mathbf{E}_{[\mathbf{W}_i]_d} \oplus \mathbf{E}_{t.}$ Note publically accessible keys $\mathbf{E}_j$ for $0 \leq j \leq Z - 1$, which structured to form high randomness. Hence $\mathbf{I}_i^{(t)}$ implies loss of an picture structural data, forming it unorderingly.

Pinpoint candidate correlate to $\mathbf{I}i$, we integrate the designed two-class SVM classifier to these Z candidates. Let $\mathbf{r} = (r0, r1 \ldots rS{-}1)$ be the vector recording the classification outcomes, where $r\,j = 0$ and $r\,j = 1$ correlate the real and unarranged blocks, accordingly. If specific j that $r\,j = 0$, then we decrypt the embedded data bits as

$$\mathbf{W}_i = [\,j\,]_2 \tag{9}$$

Here $[j]_2$ was length-n binary of j and $k = \log_2 Z$. Let's take an example, if $k = 3$ and $j = 7$, it results $[j]_2 = 111$. $\mathbf{W}_i$ was the real picture block that was easily recollected by

$$\mathbf{I}_i = \mathbf{I}_i^w \oplus \mathbf{E}_{[\mathbf{W}_i]_d}. \tag{10}$$

3.4. Feature extraction for Differentiating Ciphered and Non-ciphered Image Blocks

To distinguish ciphered and unciphered pictures chunks, will propose a characteristic vector $\boldsymbol{\rho} = (H, \sigma, \mathbf{V})$ that take part features in various viewpoints. Where, H was designer entropy indicator, σ was Standard Deviation of chunk, then $\mathbf{V}$ indicates directional local difficulties in 4 ways. Upper characteristics section construction is shown in below discussion.

Related to real unciphered block, ciphered block pixel incline to take a more unvarying dispensation. That inspires our present native entropy in feature vector to have distinguishing features. Though, we want to be careful when computing the entropy standards since the samples count in chunk will be moderately restricted, ensuing in evaluation bias, particularly chunk dimension was less. For illustration of situation $M = N = 8$, we have 64-pixel models, while choice of every model was starting from 0 to 255. To lessen adverse result in inadequate values in trials comparative to huge variety models, then we suggest calculating entropy mass according to quantized models Here the quantization stage area was designed by considering chunks dimension. Precisely, will apply unvarying scalar quantization to every block pixel.

$$\hat{I} = \frac{MN * I}{256} \tag{11}$$

Where I and $\hat{I}$ indicate the original and the quantized pixel value correspondingly. Positively, $\hat{I}$ drops into the range of array size $[0,\ MN - 1]$.Entropy H depends on quantized trials set by

$$H = -\sum_{j=0}^{MN-1} p(j) \log\, p(j) \tag{12}$$

In single 1st order entropy capacity is not enough to cover every essential feature in a chunk, we advise to expand the feature vector by presenting additional component,

$$\sigma = \sqrt{\frac{1}{MN} \sum_j (I(j) - \mu)^2} \tag{13}$$

Here $\mathbf{I}\ (\mathbf{j})$ was jth pixel of chunk and $\mu = \frac{1}{MN} \sum_j I(j)$ was sample mean in every model of the chunk. Together with characteristic component, it increases the categorization performance in information scatterings and tightness is well mirrored.

Addition to upper characteristic mechanisms, we comprise directional complications indicators that encrypt native geometric statistics. At the last, need describe a four-tuple vector $\mathbf{V} = (v1, v2, v3, v4)$ _, where

$$v1 = \sum_j |I(j) - I(j_{ne})|$$
$$v2 = \sum_j |I(j) - I(j_e)|$$
$$v3 = \sum_j |I(j) - I(j_{se})|$$
$$v4 = \sum_j |I(j) - I(j_s)| \quad (14)$$

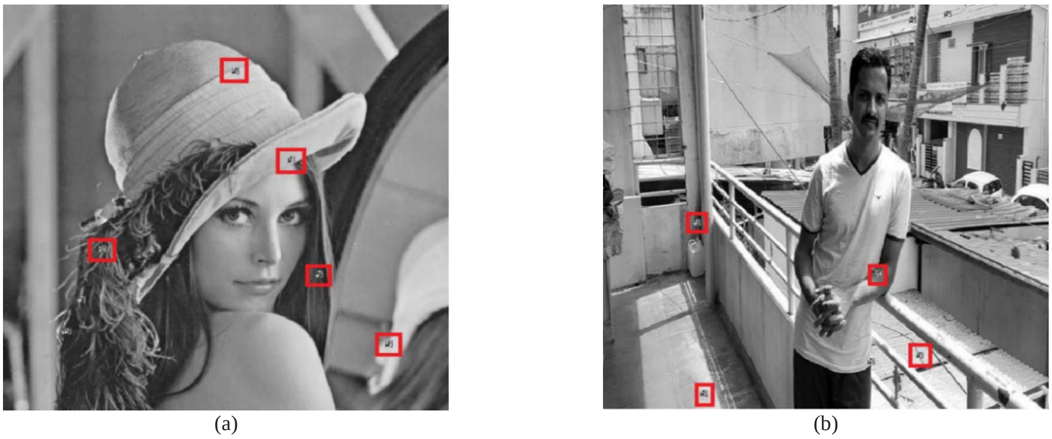
Where$f(j_{ne})$, $f(j_e)$, $f(j_{se})$ and $f(j_s)$ signify the neighbors on 0° (east), 45° (northeast), −90° (south) and −45° (southeast) directions, comparative to $\mathbf{f}(j)$.

Problem Definition from Previous Work

In the earlier work, although the classifier is sensibly designed, it is quite challenging to differentiate those extremely surfaced original blocks from the ciphered ones. While decrypting the blocks, there exists two cases, first, the few blocks cannot be decoded for any arrangement of the keys. Second, there a circumstance where few ciphered blocks are incorrectly classified as the original unciphered block. If any of case happens, it was designating to decrypting errors as shown in Fig.4(a) and Fg.4(b). To properly examine inaccuracies, propose an efficient mistake alteration method, we describe 2 kinds of classification errors.

1) Type I Error: $\mathbf{f}_i^{(j)} = \mathbf{f}_i$, while $r_j = 1$.
2) Type II Error: $\mathbf{f}_i^{(j)} \neq \mathbf{f}_i$, while $r_j = 0$.

In first one generally happens when the original chunk $\mathbf{f}_i$ is complex, e.g., extremely surfaced sections, acting like same as a ciphered block. Second one is typically rises when chunk dimension was quite little, building a ciphered block wrongly be classified as an original unciphered one.


(a)

(b)

Fig.4. Error blocks generated after decryption for (a). Lena image and (b). Real time image.

Solution

At the point of classification of mistakes was recognized in a specific chunk, we want procedure to address them. However, sorting was reasonably planned, and it was little crucial to separate the very finished unique chunks from an encoded one, in case chunk area was little. To calculate difficult issue, prescribe utilize self-closeness property essential in original image. Even in large textured pictures was seen that related chunks can are discovered in nonlocal window.

According to this criterion, the anticipated error correction technique relies upon the resulting key perception: if a block is decoded accurately, at that point with extremely high possibility and sure alike to patches found it. In this case the feature of nonlocal picture likeness inspires us to rank every probable candidate chunks as per little accurate distance with point in nonlocal search window. In the last, we firstly state a to-be-corrected set C by

$$C = \begin{cases} \{\boldsymbol{I}_{\boldsymbol{i}}^{(j)} | \mathbf{0} \leq \boldsymbol{j} \leq \boldsymbol{Z} - \mathbf{1} \\ \{\boldsymbol{I}_{\boldsymbol{i}}^{(j)} | \boldsymbol{r}_{\boldsymbol{j}} = 0 \end{cases} \quad (15)$$

In any candidate chunk Ii (j) in C, compute the distance from a wide range of various chunks in explore window D\ {Ii (j)}, here D has a similar middle as Ii (j) and area was tentatively decided as 5M × 5N.

After calculating these least patch paths within search window

$$d_i^{(j)} = \min|I_i^{(j)} - D|^2 \tag{16}$$

Here **D** was the subjective block with the area M × N inside D\ {$\mathbf{I}_i^{(j)}$}.Where, we utilize straightforward MSE basis In ranking candidate chunks. By involving texture handling, measure into above minimal structure, in this we can additionally increase error alteration execution, however we find extra increase in somewhat restricted and incurred complication is enormous. Candidate $\mathbf{I}_i^{(j)}$ he give less $d_i^{(j}$ then chosen as decrypted block. After deciding list *j* of the utilized public key, embedded information bits, original picture block can straight forwardly recollect as in (9) and (10) which is pictorially shown in Fig.5.

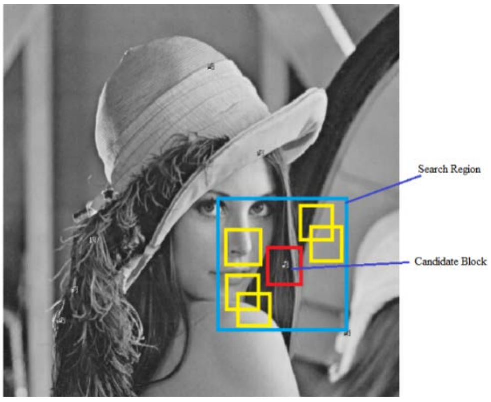


Fig.5. Creating a local search region to eliminate the error block.

4. Results and Discussions

In this part, we tentatively assess the embedding execution in the proposed encoded-providences RVIHS.

We calculate embedding capacity and data removal precision r of the process in the various situations in the chunk area. Where, r was characterized as

$$r = \frac{\text{\# of accurately recovered bits}}{\text{\# of hidden bits}} \tag{17}$$

The number, which were given as average of all the chunks in 100 test pictures. In addition, we fix k = 3 in the technique, that is every chunk occupies 3 pieces.

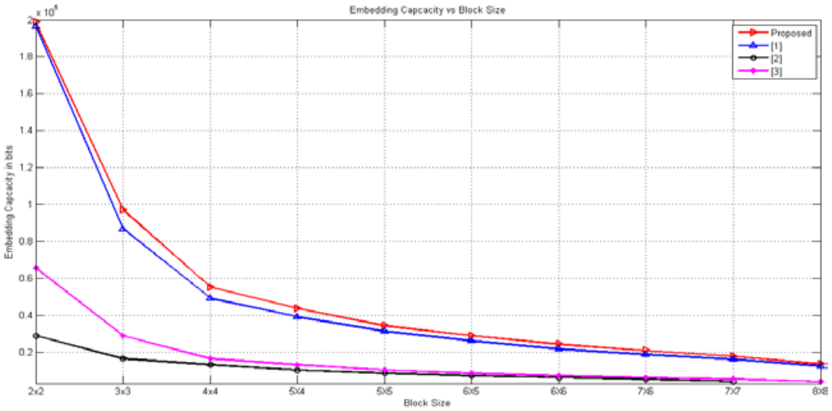


Fig.6. Graph showing embedding capacity with respect to block size

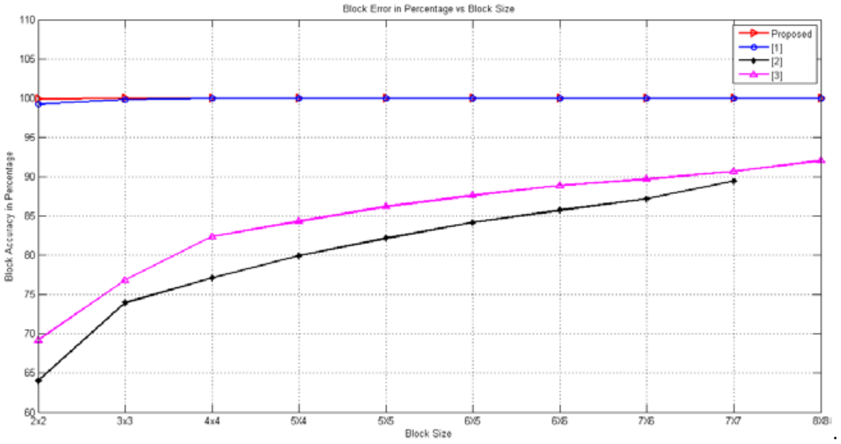


Fig.7. Error Accuracy percentage with respect to block size

Table 1 is representing the comparative results on our proposed technique for the existing work. The results clearly indicate the proposed technique gives better performance by comparing the certain parameters such as block size, capacity and accuracy. As and when the block size reduces, the capacity and accuracy decrease as in [15], [16] and [17]. In our proposed technique, Even the minimum block size gives the better embedding capacity and accuracy is shown in Fig. 6.

As shown in Fig. 7, for pictures with an enormous bit of textural region degraded outcomes particularly when chunk area was little. Let us take an example; the removal precision was 99.9913%, for the frame of chunk of area was 4 × 4. Interestingly, process offers vastly improved removal precision for every setting of chunk area.

Table 1. Comparative results showing performance of proposed work over previous works.

Block Size	**Proposed**		**[15]**		**[16]**		**[17]**	
	Capacity	**Accuracy**	**Capacity**	**Accuracy**	**Capacity**	**Accuracy**	**Capacity**	**Accuracy**
8x8	13448	100%	12288	100%	4096	89.4468%	4096	92.0461%
7x7	17672	100%	15987	100%	5329	87.2088%	5329	90.655%
7x6	20808	100%	18615	100%	6205	85.7437%	6205	89.6938%
6x6	24200	100%	21675	100%	7225	84.1943%	7225	88.8833%
6x5	28800	100%	26010	99.9973%	8670	82.1644%	8670	87.6347%
5x5	34320	100%	31212	99.9930%	10404	79.9319%	10404	86.1932%
5x4	43808	100%	39168	99.9903%	13056	77.1022%	13056	84.3227%
4x4	55231	99.9913%	49152	99.9761%	16384	73.9654%	16384	82.3897%
3x3	96992	99.9806%	86700	99.8224%	28900	64.0132%	28900	76.8219%
2x2	198562	99.8923%	196608	99.2356%	NA	NA	65536	69.1936%

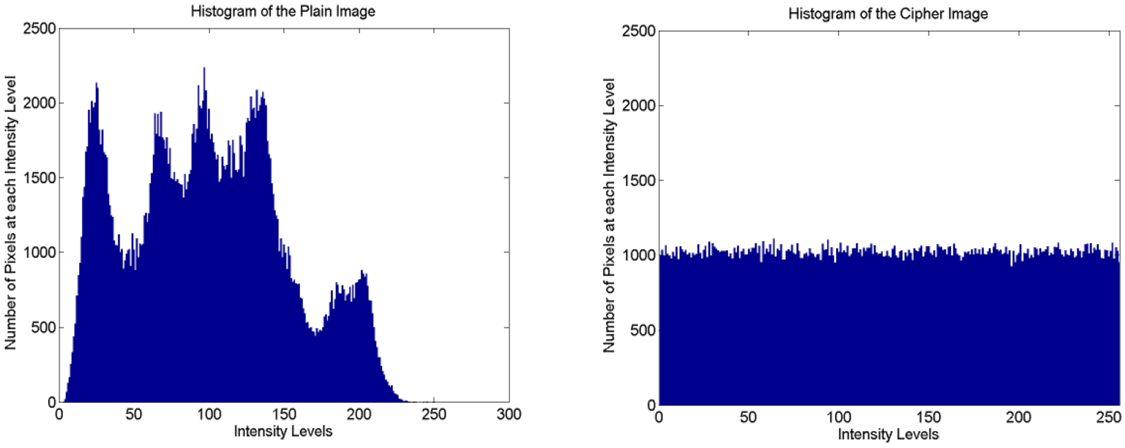
Cryptographic Statistical Analysis

Information Entropy

Entropy is a measure of information and also the magnitude of randomness. The entropy for a plain gray scale video frame is theoretically less than 8. When all the gray scale pixels of different intensity levels are equally distributed (i.e. with equal probability), the entropy will be equal to 8. The entropy for the cipher video frame using the proposed encryption algorithm is calculated and recorded Table 2. The results reveal that the entropy is close to 8. Hence the cipher video frame is random, and the chances of prediction are very less and the proposed algorithm is more secure.

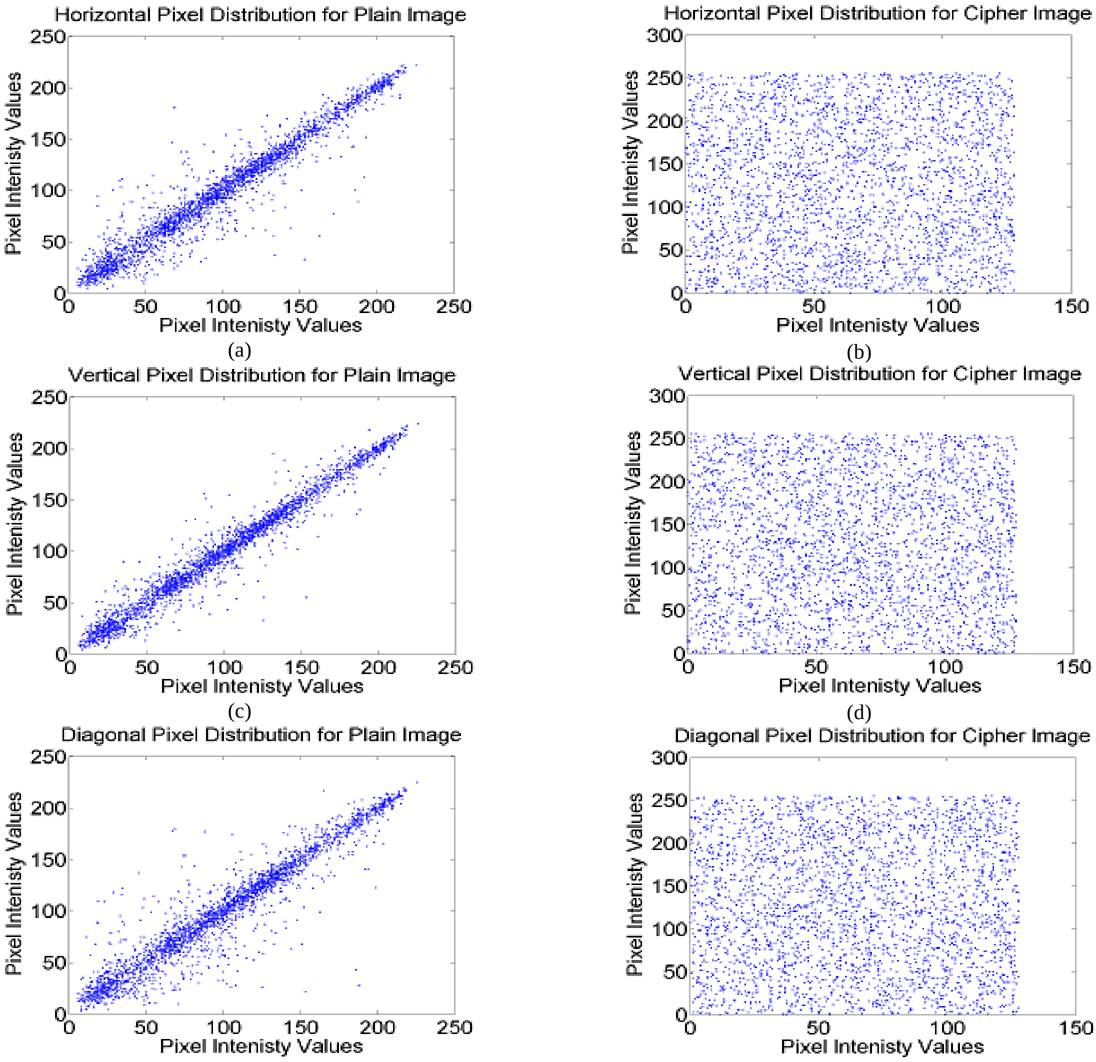
Mean Square Error (MSE) and Peak Signal to Noise Error (PSNR)

The plain video frame has a visual perception to the human eyes and is considered as the original plain video frame. But when it is encrypted, it yields a cipher video frame which is not perceptual to human eyes and hence it is considered as noise. The degree of noise produced by the proposed algorithm is determined by calculating the MSE, the Mean Square Error and PSNR, the Peak Signal to Noise Ratio. The MSE and PSNR are calculated using the proposed encryption algorithm for the different document image and are tabulated in the Table 2. A very large value of PSNR represents both plain and cipher video frames appearing almost the same. The results of MSE and PSNR in Table 2 reveals that, the proposed encryption algorithm is resistant enough to withstand the statistical attacks.



(a) (b)

Fig.8. Histogram of (a) Plain video frame (b) Ciphered video frame



(a) (b)

(c) (d)

(e) (f)

Fig.9. Results of Correlation for a video frame: (a) Horizontal Correlation (d) Horizontal Correlation of Cipher video frame, (b) Vertical Correlation of Plain video frame, (e) Vertical Correlation of Cipher video frame, (c) Diagonal Correlation of Plain video frame and (f) Diagonal Correlation of Cipher video frame

Histogram

The histogram is the graphical representation of how pixels of various intensity levels are distributed. It is the number of pixels versus various pixel intensity levels. The spikes in the histogram for the plain image represents the statistical relationship among its pixels. The flat histogram in the cipher video frames represents no statistical relation among pixels and thereby it is not easy for the cryptanalyst to judge or predict the plain video frame. The histogram for a single video frame is shown in Figure 4. The Figure 8(a) represents the histogram of a video frame image and has spikes in it. This shows that there is statistical relationship between the grayscale pixel levels. From the Figure 8(b), it is seen that the histogram of the cipher video frame is perfectly flat. There is no statistical relation among the pixels since pixels with different intensity levels are appeared with the same magnitude. Hence prediction of any plain video frame is impossible. Also, the flat histogram does not provide any clue about the plain video frame. Therefore, the proposed algorithm is resistant to statistical attacks.

Correlation

The correlation is a measure of similarity or relativity. Since the pixels are correlated in the plain video frame, the information is perceptual to human eye. For a cipher video frame, the pixels of different intensity levels are randomly distributed and hence no correlation among the neighboring pixels. The correlation among the adjacent pixels can be determined by calculating the correlation coefficient for a set of 3000 pixels along horizontal, vertical and diagonal directions for both plain and cipher images. The correlation coefficient using the proposed encryption algorithm is calculated for a video frame along the Horizontal, Vertical and Diagonal directions and recorded in Table 2. From the Figure 6, it is seen that the gray level pixels are distributed uniformly and randomly in all directions. Hence the plain and cipher video frames are purely dissimilar and cipher video frame is not perceptual to human visual system.

Table 2. Cryptographic results.

Parameters	Experimental Values
MSE	1.814×10^{4}
PSNR	5.543
Horizontal Correlation	-0.0292
Vertical Correlation	-1.0060×10^{-4}
Diagonal Correlation	0.0132
Entropy	7.9993

5. Conclusion

The proposed method of data hiding scheme uses a hiding technique in the ciphered domain, which combines multi-dimensional chaotic maps and Support Vector Machine (SVM) image classifier. The Video Frames Encrypted by modifying the pixels with a random matrix generated using the 2-D Logistic map. The ciphered frame divided into non-overlapping blocks, and each block XORed with blocks of the public key table made by the 3D Lorenz map. The public key blocks are selected based on the R binary Information bits stream. The machine learning approach for data extraction is used. Using public key table information bit streams are reversibly embedded in ciphered domain during hiding hence chances of cracking the cipher video frame even if the interceptor knows private and public keys are very less. Hence the cryptanalyst finds it very difficult to crack the algorithm. Data extraction is carried out by performing XORing with non-overlapping blocks and the public key table. The SVM classifier extracts the information data based on the decoded block for both cryptographic and steganography analysis performed on the ciphered frames for security analysis.

References

[1] Dawen Xu, Rangding Wang, Yani Zhu, “Tunable data hiding in partially encrypted H.264/AVC videos”, Journal of Visual Communication and Image Representation, Vol. 45, pp.34-45,2017. DOI: 10.1016/j.jvcir.2017.02.008.

[2] D.W. Xu, R.D. Wang, “Context adaptive binary arithmetic coding-based data hiding in partially encrypted H.264/AVC videos”, Journal of Electronic Imaging, Vol.24, No.3, pp. ,2015. DOI: 10.1117/1.JEI.24.3.03

[3] Lakshmi M, Arjun K P, Sreenarayanan N M, Arya K A, “Reversible Data Hiding in Videos for Better Visibility and Minimal Transfer”, Procedia Technology”, Vol.25, pp.256-263, 2016. DOI: 10.1016/j.protcy.2016.08.105.

[4] S. Manisha, T. Sree Sharmila, “A two-level secure data hiding algorithm for video steganography”, “*Multidimensional Systems and Signal Processing*”, Vol.30,pp. 529–542,2018.DOI: 10.1007/s11045-018-0568-2.

[5] Sunanda Jana, Arnab Kumar Maji, Rajat Kumar Pal, ”A novel SPN-based video steganographic scheme using Sudoku puzzle for secured data hiding”, *Innovations in Systems and Software Engineering*, Vol.15, pp.65–73,2019, 10.1007/s11334-019-00324-8.

[6] Arash Jalali, Hassan Farsi,"A new steganography algorithm based on video sparse representation", Multimedia Tools and Applications, Vol.79, No.6,2020,DOI: 10.1007/s11042-019-08233-5.

[7] Hassan Farsi, "Improvement of minimum tracking in Minimum Statistics noise estimation method", Signal Processing: An International Journal (SPIJ), Vol.4, No.1, pp.17-22,2010.

[8] Mstafa RJ, Elleithy KM, "A novel video steganography algorithm in DCT domain based on hamming and BCH codes", IEEE, pp.208–213,2016. DOI: 10.1109/SARNOF.2016.7846757.

[9] Rajesh GR, Nargunam AS, "Steganography algorithm based on discrete cosine transform for data embedding into raw video streams", IET Chennai Fourth International Conference on Sustainable Energy and Intelligent Systems (SEISCON), Chennai, pp 554–558,2013.

[10] Yadav P, Mishra N, Sharma S, "A secure video steganography with encryption based on LSB technique", IEEE International Conference on Computational Intelligence and Computing Research, pp.1–5,2013. DOI: 10.1109/ICCIC.2013.6724212.

[11] Shuvendu Rana, Rohit Kamra, Arijit Sur, "Motion vector based video steganography using homogeneous block selection",Multimedia Tools and Applications,Vol.79,No.3,pp.1-16,2020. DOI:10.1007/s11042-019-08525.

[12] Alharthi N, Gutub A, "Data visualization to explore improving decision- making within hajj services",Scientific Modelling and Research, Vol.2,No.1,pp.9–18,2017. DOI: 10.20448/808.2.1.9.18

[13] Rajeev Kumar, Satish Chand, Samayveer Singh, "An optimal high capacity reversible data hiding scheme using move to front coding for LZW codes", Multimedia Tools and Applications, Vol.78, No.10,2019. DOI: 10.1007/s11042-019-7640-2

[14] Yi Chen, Hongxia Wang, Hanzhou Wu, Yong Liu, "Reversible video data hiding using zero QDCT coefficient-pairs", Vol.78, pp.23097–23115,2019. DOI: 10.1007/s11042-019-7635-z

[15] Weiqing Wang, "An efficient multiple-bit reversible data hiding scheme without shifting",*Multimedia Tools and Applications*, Vol.79, pp.555–579,2020. DOI: 10.1007/s11042-019-08065-3

[16] Jafar IF et al, "An efficient reversible data hiding algorithm using two steganographic images", Signal Processing, Vol.128, p.98-109,2016. DOI: 10.1016/j.sigpro.2016.03.023

[17] Chang JC, Lu YZ, Wu HL (2017) "A separable reversible data hiding scheme for encrypted JPEG bit streams", Signal Processing, Vol.133, pp.135–143,2017. DOI:10.1016/j.sigpro.2016.11.003

[18] S. Manisha, T. Sree Sharmila, "A two-level secure data hiding algorithm for video steganography",Multidimensional Systems and Signal Processing,Vol.30,No.1,2019.DOI: 10.1007/s11045-018-0568-2.

[19] Tarun Kumar, Shikha Chauhan, "Image Cryptography with Matrix Array Symmetric Key using Chaos based Approach", International Journal of Computer Network and Information Security, 2018.

[20] Gat Pooja Rajkumar, Dr V. S. Malemath, "Video Steganography: Secure Data Hiding Technique", International Journal of Computer Network and Information Security, 2017.

[21] Sengul Dogan, "A New Approach for Data Hiding based on Pixel Pairs and Chaotic Map", International Journal of Computer Network and Information Security, 2018.

[22] Rosalina, Nur Hadisukmana, "An Approach of Securing Data using Combined Cryptography and Steganography", International Journal of Mathematical Sciences and Computing, Vol.6, No.1, pp. 1-9, 2020.

[23] Sonia Bajaj, Manshi Shukla, "Performance Evaluation of an approach for Secret data transfer using interpolation and LSB substitution with Watermarking, "International Journal of Computer Science and Information Technologies, Vol.5, pp.6213-6217,2014.

[24] E Divya,P Raj Kumar, "Steganographic Data Hiding using Modified APSO", International Journal of Intelligent systems and Applications,Vol.8,No.7,pp.37-55,2016.

[25] Ravpreet Kaur, Manish Mahajan, "Random Pattern based sequential bit RaP-SeB) Steganography with Cryptography for Video Embedding", International Journal of Modern Education and Computer Science, Vol.8, No.9, pp.51-59,2016.

Authors' Profiles

Vinay D. R. worked as an Assistant Professor in the Department Computer Science Engineering, Channabasaveshwara Institute of Technology, Gubbi. He obtained his BE Degree Computer Science Engineering from Visvesvaraya Technological University, Belgaum His specialization Master of Technology in Computer Science and Engineering at Channabasaveshwara Institute of Technology, Gubbi.VTU, Belgaum.

He is pursuing PhD in Computer Science Engineering, Malnad College of engineering, Hassan. His area of interest is in the field of Digital Image Processing, steganography, machine learning and neural network. He is professional membership in ISTE, New Delhi.

Dr. Anand Babu J. is an Associate Professor in the Department of Computer Science Engineering, Malnad college of engineering, Hassan. He obtained his BE Degree Computer Science Engineering from Visvesvaraya Technological University, Belgaum His specialization Master of Technology in Computer Science and Engineering at National Institute of Engineering, Mysore, VTU, Belgaum.

He was awarded PhD in Computer Science & Engineering VTU, Belagavi. He has over 20 research publications in refereed International Journals and Conference Proceedings. His research interests include Image Processing, Computer Networks, Wireless Sensor Networks, and Big Data. He is life member of IETE, ISTE, and IAENG.

How to cite this paper: Vinay D. R., Ananda Babu J., "A Novel Secure Data Hiding Technique into Video Sequences Using RVIHS", International Journal of Computer Network and Information Security(IJCNIS), Vol.13, No.2, pp.53-65, 2021. DOI: 10.5815/ijcnis.2021.02.05