International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249 – 8958 (Online), Volume-9 Issue-4, April 2020

Integrated Partial Encryption and Watermarking Technique for Digital Video using Chaos and Support Images

Md. Anwar Hussain, Popi Bora

Abstract*: Encryption and Watermarking are image processing tools that are used mostly separately. Encrypting a document completely obscures it and watermarking is applied mostly for copy right protection. For entertainment type videos, partial encryption and watermarking may be integrated such that both objectives are attained. We report in this paper a novel combined partial encryption and watermarking algorithm for digital videos using chaotic system and support image. Watermarks are generated by using iris information of the authentic user or the authentic producer of the digital video. Watermarks of full size and half size are embedded in the luminance frame (s) of the video using simple LSB steganography. A sequence of color frames is watermarked in two phases, and partially encrypted in two layers, the watermarks considered are encrypted before embedding. The luminance frame (s) is (are) preprocessed before embedding with the watermarks to defy stega-analysis. Chaotic logistic map and a gray level support digital image is used for obtaining unique row/column sequences as well as for generating robust random binary sequences. A support color digital image is used in the first layer encryption of the digital video. Modified Rabinovich 4 dimensional hyper-chaotic system is used for second layer encryption. Encryption algorithm is applied in R, G, B frames separately. The technique may also be applied for integrated encryption and watermarking of digital images.

***Keywords*: Digital color video; partial encryption; LSB steganography; Watermarking; Support image**

I. INTRODUCTION

We live in an era of internet where data information exchanges are mostly multimedia images and videos. Interactive exchanges of such multimedia information have become more and more common with the advent and common use of smartphones. Digital images and videos which are patented or whose use is to be controlled among authentic users are mostly distributed through public internet and thus undergo threat of misuse. Modern computer technologies with developments of software for mischievous acts have jeopardized the situation further [1]. Confidentiality, integrity, security and the authenticity of data has become an important issue. An encryption algorithm is considered as a definite and secure way to protect image and video data from unauthorized and illegal eavesdropping. Conventional encryption algorithms such as DES, AES etc. are not suitable for practical image and videos which are bulk data types, because of their high computational cost.

Many alternative encryption algorithms based on chaos are proposed recently which provide better trade-off between cost and efficiency [2]. Chaotic and hyper chaotic systems are deterministic nonlinear systems, possessing several intrinsic characteristics, such as extreme sensitivity to initial conditions, broadband power spectrum, and random-like behaviors making them suitable to a variety of disciplines including secure communication [3]. The methods of confusion-diffusion or permutation-substitution are followed obviously for encryption of data. Chaos or hyper-chaos based methods use various chaotic system and hyper-chaotic system of 3, 4, or 5 dimensions. Some such techniques are discussed in [2, 4, 5] and in the references thereof.

Also DNA technology based encryption, where hyper chaotic map is used for confusion stage and DNA sequence is used for diffusion stage, is reported in [6, 7, 8, 9]. It is reported in [10] that chaos based algorithm may be weak against chosen-cipher text and chosen-plaintext attacks because of prevalent correlations among adjacent pixels in an image. The authors have proposed an algorithm to decorrelate pixels employing two hyper-chaotic systems to overcome such attacks. Authors in [11] combined SHA-1 with hyper-chaotic system and claim to generate of robust secret key for fast and secure digital encryption system.

Color images have more redundant information than the gray scale images. Watermarking of digital objects are with the objective of protecting the copyright. Here the digital objects such as images and videos are embedded with some types of watermarks keeping the object itself visible. Literatures are abundant on research to design spatial domain watermarking schemes [13]. In [14] authors segregate in a medical image data the region of interest from the region of non interest, proposing to create watermark using logistic map chaotic system. They encrypt the region of interest and watermark with patient's information the region of non-interest. Watermarking algorithm is also designed in transform domain [15, 16]. In [17], authors propose secure and robust gray level image watermarking using coefficient differencing and chaotic encryption. For medical image security using chaos [18], authors in [19] proposes multimedia security application using ten-term chaotic system without equilibrium. Other than chaos based algorithm,

Revised Manuscript Received on March 16, 2020.
* Correspondence Author
Md. Anwar Hussain*, Department of Electronics and Communication Engineering, North Eastern Regional Institute of Science and Technology, Nirjuli, Arunachal Pradesh, India-791109. ah@nerist.ac.in
Popi Bora, Department of Electronics and Communication Engineering, North Eastern Regional Institute of Science and Technology, Nirjuli, Arunachal Pradesh, India-791109. popibora2015 @gmail.com

reports are available in chaos embedded genetic algorithm for data hiding applications [20]. Combining watermarking and encryption using chaos, multilayer security applications are reported in [21] for health data. Combining chaotic map and wavelet transform methodology, a chaos- based video watermarking in wavelet domain is reported in [22]. In spatial domain, with analysis in spatial and frequency domain characteristics, authors in [23] reports secure authentication technique sing dual chaotic image watermarking. Authors in [24], claim to design robust watermarking technique, using 2D logistic map and elliptic curve cryptosystem in wavelets.

In this paper, we report an integrated encryption and watermarking technique for application in short duration entertainment color video. It is a partial encryption of the color frames which is carried out in two layers, integrated with two phase watermarking. For encryption in the first layer, we apply pixel value diffusion using ***bitxoring*** with a support image; the support image is pre-modified by pixel value substitution. In the second layer encryption, we apply diffusion ciphering based on the method reported in [25] and the modified Rabinovich 4 D hyper-chaotic system [26]. For watermarking, we use simple LSB steganography in secret pixel positions which are obtained with chaotic logistic map and a support gray level image.

We take help of two support images, one gray and one color of same frame size as the video frames, for robust pixel position selections for watermarking and robust diffusion ciphering for encryption of color frames. We call it integrated technique as we use chaos and hyper chaos as tools and that second phase of watermarking can never be approached unless encryption is undone. Although the technique is described for application in digital video, it may be used for integrated encryption and watermarking of digital image for authentic distribution and copyright protection.

II. SYSTEM MODEL AND METHODOLOGY

As we want to integrate watermarking and encryption of digital video, an entertainment video of short size in particular, we divide the complete system into several sub-systems as described below. We applied chaotic logistic map for generation of (a) unique random pixel sequences for watermark embedding, (b) for generating robust random binary sequences for encrypting the watermark, and (c) for pixel value substation based first layer encryption. For second layer encryption we utilized Rabinovich 4 dimensional hyper-chaotic system. We considered a sequence of consecutive 16 color frames, each of size 144x176 pixels, from 400 frames of "*Foreman.avi*" video to describe our proposed integrated watermarking and encryption. The following are the processing steps:

1. Full size binary watermark of around 1840 bits, and half size binary watermarks around 920 bits are constructed from the secret iris information of the authentic user. The company logo may also be used for constructing watermarks. Watermarks are encrypted for security and secrecy.
2. 16 consecutive color frames from the video is selected, and respective luminance frames are constructed.
3. On each luminance frame from step 2, we carry full size (or half size) watermark embedding using LSB steganography. Respective watermarked color frames are reconstructed. This process is termed as first phase watermarking which may be optional.
4. Each watermarked color frame is divided into 16 blocks. Choosing one block from one frame, with no common block positions, one color frame is constructed combining 16 blocks. We call this as cropped color frame and it contains traces of watermarks from the first phase.
5. On the luminance frame of the cropped color frame, the second phase of watermarking is executed. Full size binary watermark is embedded using LSB steganography. Color frame is reconstructed.
6. R, G, and B frames obtained from the color frame from the step 5, we execute first layer and then second layer encryption.
7. Respective color blocks, which also carry traces of watermarks from both phases, are returned to their respective frames. Thus we have a sequence of 16 color frames which are partially encrypted, and watermarked.

Chaotic Maps:

Nonlinear chaotic map functions are highly complex in behavior with unpredictable time evolution which may be used for designing security algorithms. A highly secure pixel sequence and a secure robust random binary sequence can be derived using chaotic logistic maps. There are various chaotic sequences. A few of them, defined mathematically are as below.

Chaotic Logistic Map:

$$x_{n+1} = 4rx_n(1-x_n) \quad \text{for } n = 0,1,2,..$$
$$\text{where} \quad 0.8925 \le r \le 1 \quad \text{and} \quad 0 \le x_n \le 1 \tag{1}$$

Or

$$x_{n+1} = \frac{\alpha^2(2x_n-1)^2}{4x_n(1-x_n)+\alpha^2(2x_n-1)^2} \qquad n = 0,1.2,..... \tag{2}$$
$$\text{where} \quad 0.5 \le \alpha \le \infty \quad \text{and} \quad 0 \le x_n \le 1$$

***Coupled Chaotic Logistic Map*:**

$$x_{n+1} = f_1(x_n, \beta_1)$$
$$y_{n+1} = f_2(x_n, \beta_2) \tag{3}$$

where $n = 0,1,2,3,.....$, and

$$y_n = Rx_{n+1}$$
$$x_n = Ry_{n+1}$$

f_1, f_2 are one parameter family maps as in (1), (2) and β1, β2 are keys and R is cross-coupling factor.

Quantum Chaotic Map:

$$x_{n+1} = \lambda(x_n - |x_n|^2) - \lambda y_n$$
$$y_{n+1} = -y_n e^{-2\beta} + e^{-\beta}\lambda[(2 - x_n - x_n^*)y_n - x_n z_n^* - x_n^* z_n]$$
$$z_{n+1} = -z_n e^{-2\beta} + e^{-\beta}\lambda[2(1-x_n^*)z_n - 2x_n y_n - x_n]$$

where λ is an adjustable parameter, β is dissipation parameter and x_n^*, z_n^* are complex conjugate of x_n and z_n

(4)

Modified Rabinovich 4 D Hyper-chaos system:

By adding a new parameter to the Rabinovich 3D hyper-chaotic system, the modified Rabinovich 4 D hyper-chaotic system is obtained which is expressed as below [26].

$$\dot{x} = ry - ax + yz$$
$$\dot{y} = rx - by - xz$$
$$\dot{z} = -dz + xy + u^2$$
$$\dot{u} = xy + cu \qquad (5)$$

The system exhibits chaotic behavior for $a=4$, $b=-0.5$, $c=2.2$, $d=1$, and $r=8.1$. The initial state values x_0, y_0, z_0, and u_0 are used as keys. The four *Lyapunov exponents* are L_1= *1.090046*, L_2=*0.012243*, L_3=*-3.105106*, and L_4=*-4.697183*, the *Kaplan-Yorke* dimension D_{KY}=*2.5736132*.

ROW/COLUMN INDEX GENERATION:

Using any chaotic map as shown in Eq. 1, Eq. 2, or Eq. 3, and using initial key along with appropriate parameter values, a sequence of random values x_n, for $n=1, 2, 3, \ldots$, is obtained. A sequence row indices R_i obtained using the following mathematical operation, with initial key $x1_0$.

$$R_n = mod\ (x1_n \,.\, 10^{15},\ 144) + 1 \qquad (6)$$

Similarly, a sequence of column indices C_i is obtained by the mathematical operation, with initial key $x2_0$.

$$C_n = mod\ (x2_n \,.\, 10^{15},\ 176) + 1 \qquad (7)$$

Unique sequences comprising (R_i, C_i) pairs such that no two pairs are same, are obtained for LSB embedding of watermark binary bits. A block diagram is shown below where $Key^R = x1_0$ and $Key^C = x2_0$ are the initial values.

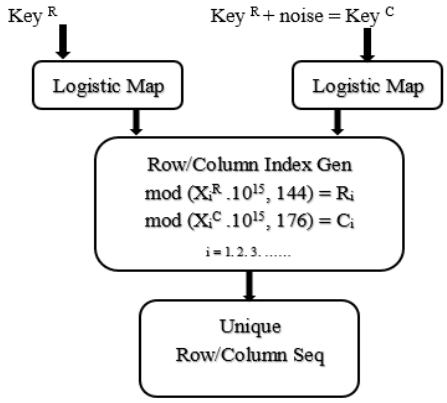

Fig. 1 (a)

A variation and more robust unique Row/Column sequence generation may be formulated if we use a grey support image S_G of size 144x176 pixels. Here the initial row/column sequence is used to find the corresponding pixel values *Pi* of S_G which is then used as the number of iterations of the chaotic map to find the next random values to be used in Eq. 5 and Eq. 6. Same is expressed in a block diagram shown below:

The watermarks, which are arranged as linear binary sequence, used in this report are encrypted by *bit xoring* with an equal length random binary sequence obtained using chaotic map. With an initial key $x3_0$ and other appropriate parameter values, the random binary sequence is obtained using the following mathematical operation for *n=1, 2, 3….*

$$b_n = mod\ (x3_n \,.\, 10^{15},\ 2) \qquad (8)$$

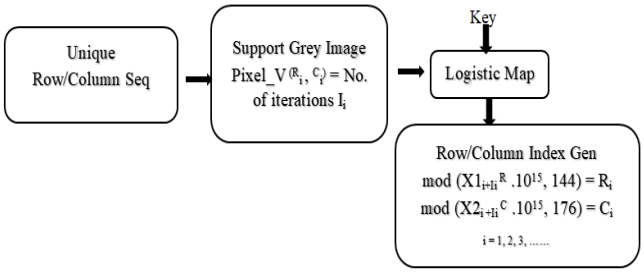

Fig. 1 (b)

The grey support image S_G, as in row/column index sequence generation explained above, may be used similarly in binary sequence generation using Eq. 8. As is clear from the use of support image S_G, the initial keys to chaotic logistic map is not sufficient for unique pixel sequence and binary sequence generations. Unless we know the S_G, mere knowledge of initial keys will never produce pixel sequences or the binary sequences.

WATERMARK GENERATION:

To explain the proposed technique in this paper, we use the iris of the authentic user as the source of the watermark, although the company logo may be similarly used. The color digital object considered here is of size 144x176 pixels color frames. The LSB steganography technique is used to watermark in the LSB plane of the luminance frame (s) of the color digital video. The secret personal data of the authentic user is obtained by processing the irises of the user. Fig. 2 shows an example iris of a user of size 120x200 pixels. Considering a folder of 10 eye images for a person, and with further processing, Eigen Irises of size 120x200 pixels, an example shown in Fig.3, are obtained.

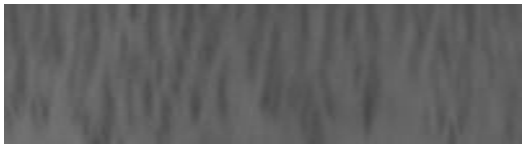

Fig. 2 Example Iris of the authentic user

Fig. 3 Corresponding Eigen Iris

Although the actual sizes of the irises are 120x400 pixels, for reduced computations we have considered both irises and Eigen irises of size 120x200 pixels. A Feature of size 10x10 fractional decimal values which is converted to a binary sequence is applied here as the watermark.

Table 1 shows example 5x5 values from the 10x10 fractional decimal values. The personal secret data or the watermark is 1842 bits long. We also generate a half size watermark of 921bits long by random collection from the full size watermark of 1842 bits. For security of the watermark, it is first encrypted by ***bit xoring*** with an equal length random binary sequence. The schematic is shown in the block diagram of Fig. 4. Output from the Fig. 4 is the encrypted full size watermark *EF_SzWk* or the encrypted half size watermark *EH_SzWk*.

TABLE I. Example 5x5 (out of 10x10) Decimal values of the Feature of Fig. 4

-0.316227766016838	0.023512135937644 5	0.0419838670416731	0.0985816609184200	0.012287075692276 3
-0.316227766016839	-0.105310239090576	-0.500089550709615	-0.606662921445246	0.127736641223312
-0.316227766016838	0.161488110249829	0.345592752557867	0.337093463161233	0.556846816357094
-0.316227766016838	0.623623549221724	-0.0292935812398052	-0.0925535784562298	0.061985454779614 9
-0.316227766016838	-0.673076895267504	-0.0255616606521121	0.148227747265397	0.340436888551032

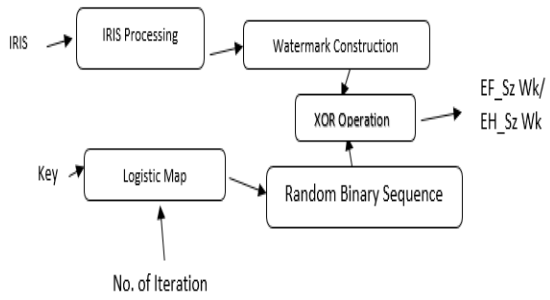

Fig. 4 Iris Processing and Encryption of the Watermark

As the watermarking is separately embedded in each frame, if there is overlapping in pixel positions between frames, there is no difficulty in retrieving the watermark later. The 16 frames are converted back to color frames. It may be noted that we can also apply half size watermark, instead of the full size, in this phase. The schematic is shown in Fig. 5 below.

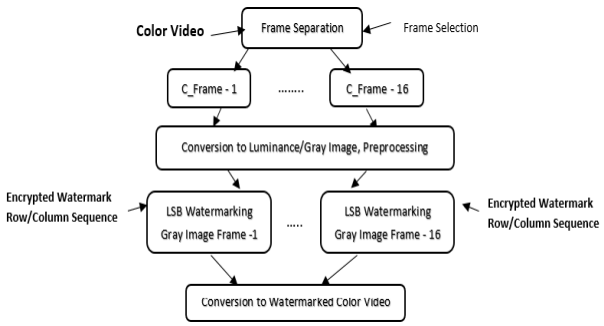

Fig. 5 First phase watermarking

WATERMARKING: SECOND PHASE:

The 16 color frames obtained from the previous step is cropped and combined to form a single color frame for the second phase watermarking. Luminance frame is constructed as usual and is embedded in the LSB plane by the full size watermark. A unique sequence of pixel positions is used; the watermark is always encrypted before embedding. The schematic is shown in Fig, 6. The luminance frame, chrominance blue frame and the chrominance red frame are combined to a single color frame. It is noted that this frame contains traces watermark from the first phase and also the full watermark from the second phase. Next we separate R, G, and B frame from the single frame for two-layer encryption as explained above.

WATERMARKING: FIRST PHASE:

In this proposed technique, the watermarking is in two phases. In the first phase, the full size watermark is LSB embedded in the Luminance frames constructed from 16 consecutive color image frames. The unique pixel position sequence for LSB watermarking in each frame is uniquely and separately generated so that the pixel positions are non-overlapping between frames.

PROCESSING OF COLOR VIDEO

As stated earlier, we consider 400 frames of "*Foreman.avi*" color video of 33.33 seconds duration to explain our proposed technique of integrated encryption and watermarking. The technique is particularly suitable for partial encryption for entertainment video of short duration. The following is the standard relation of Luminance Frame L_F to the source R, G, and B frames.

$$L\_F = 0.2989.R_s + 0.5870.G_s + 0.1140.B_s \quad (9)$$

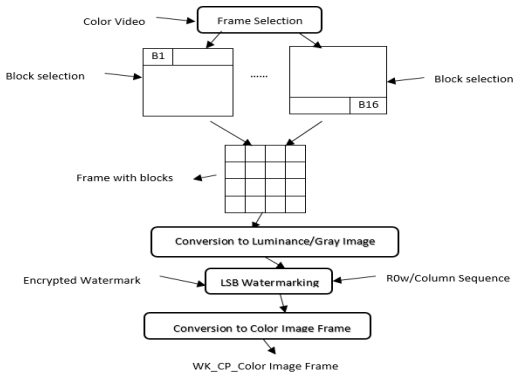

Fig. 6 Watermarking of the Luminance frame with the Full Size Watermark

Retrieval Number: D6485049420/2020©BEIESP
DOI: 10.35940/ijeat.D6485.049420
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

where R_s, G_s, B_s are the source red, green, and blue colors. On the *L_F* we apply simple LSB steganography to watermark the full size encrypted watermark *EF_Sz WK*. A unique sequence of random 1842 pixel positions are selected first, where no pixel position reappears in the sequence, using chaotic logistic function as explained above. The schematic is shown in the following block diagram of Fig. 6. After watermarking the L_F, the color frame is recomposed by using the following standard equation for PAL systems.

$$Y=L\_F;\ U=0.493.(B_s - L\_F);\ V=0.877.(R_s - L\_F) \quad (10)$$

$$A=[R_s\ ;\ G_s\ ;\ B_s]$$

$$M=[Y;\ U;\ V]$$

$$Q=[0.299\ 0.587\ 0.114;-0.147\ -0.289\ 0.437;0.615\ -0.515\ -0.100] \quad (11)$$

The watermarked color frame, W_K CP_Color Image frame, is then encrypted in two layers, first by pixel value substitution and then using Rabinovich modified 4 D hyper-chaos system with pixel diffusion as explained in [25] and shown by the schematic block diagram of Fig. 7. The corresponding blocks are put back to the 16 respective color frames from which they were taken. Hence the watermark is now existing in 1/16 part of every color frame in the luminance partial frame.

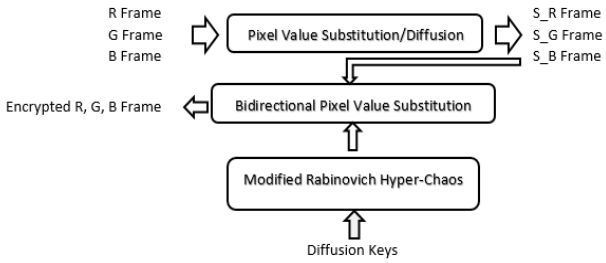

Fig. 7 Two-layer Encryption of the Watermarked Color Image

FIRST LAYER ENCRYPTION:

The first layer partial encryption of color video frames is based on pixel value substitution, Chaotic Logistic map, and a support color image of size 144x176 pixels. The encryption is carried out in R, G, and B frames individually and they are combined back to a color image. The idea can be explained by the following block diagram of Fig. 8.

The chaotic logistic map takes a key as the initial value as in Eq. 1 and support image provides the pixel value as the number of iterations for the chaotic logistic map. As a result, the chaotic logistic map outputs a value which is converted to a value in the range [0 – 255], as shown in the Fig. 7, and substitutes the pixel value in the same position of the support image. This is carried out for all pixels of the R, G, or B frame, and the result is substituted support images. As shown the respective frame is converted to binary string and bit ***xored*** with the binary converted string of the respective R, G, B frame of the color digital image to be encrypted, resulting in XORED encrypted image as shown in Fig. 8. The pixel values in the support R, G, B images are changed using substations as explained above, and this is needed to randomize the values resulting in decorrelation between adjacent pixel to pixel values. This results in breaking of pixel to pixel correlations among the adjacent pixels of the *XRD ENRD* image of Fig. 8. The R, G, and B frames of the color frame could be optionally encrypted by row-column shuffling before *bitxoring*.

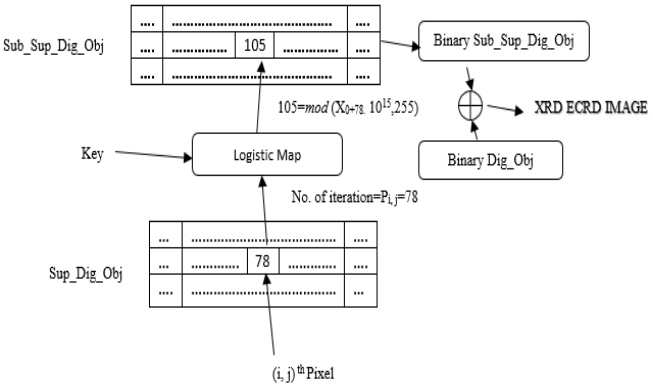

Fig. 8 First layer Encryption of Color Image

SECONDLAYER ENCRYPTION:

After the first layer encryption in the respective R, G, or B frame of the color image, the second layer encryption is carried out on each R, G, or B frame using Eq. 5 and diffusion step as explained in [25] as shown in Fig. 7. The R, G, or B of the color image is arranged in a linear array and encrypted twice, one from top to bottom and the other from bottom to top. The linear array is then converted to a frame of size 144x176 pixels. For clarity of explanation, we repeat a few steps of [25] as below:

The Eq. 5 is iterated continuously to obtain four key k_{Rn} streams after each iteration *n*, as shown in Eq. 12.

$$k_{g_n} = \mathrm{mod}[round((abs(R_n) - floor(abs(R_n)).10^{15}), 2^8]$$
$$R \in [x, y, z, u] \quad (12)$$

where k_{Rn} is circularly shifted by I_Q units for the current pixel value $P_{4(n-1)+l}$, *(l=1, 2, 3, 4)*, where I_Q is obtained from the previously operated pixel of the color image R, G, or B frame, and as shown in Eq. 13 below.

$$I_x = \mathrm{mod}(P_{4(n-1)}, 2^8), \quad I_y = \mathrm{mod}(P_{4(n-1)+1}, 2^8),$$
$$I_{xz} = \mathrm{mod}(P_{4(n-1)+2}, 2^8), \quad I_u = \mathrm{mod}(P_{4(n-1)+1+3}, 2^8) \quad (13)$$

The current pixels are ciphered by using the shifted keys, as shown in Eq. 14. P_0 is assumed any value in the range *[0-255]*.

$$C_{4(n-1)+1} = k_{xn} \oplus \{[P_{4(n-1)+1} + k_{xn}] \bmod 2^8] \oplus P_{4(n-1)}$$
$$C_{4(n-1)+2} = k_{yn} \oplus \{[P_{4(n-1)+2} + k_{yn}] \bmod 2^8] \oplus P_{4(n-1)+1}$$
$$C_{4(n-1)+3} = k_{zn} \oplus \{[P_{4(n-1)+3} + k_{zn}] \bmod 2^8] \oplus P_{4(n-1)+2}$$
$$C_{4(n-1)+4} = k_{un} \oplus \{[P_{4(n-1)+4} + k_{un}] \bmod 2^8] \oplus P_{4(n-1)+3} \quad (14)$$

where $C_{4(n-1)+i}$, $i=1, 2, 3, 4$, are the four ciphered pixels. After two cycles of encryption, the second layer encryption is completed.

The R, G, B encrypted framed are combined to give watermarked and encrypted color image. From this watermarked and encrypted color frame, blocks are separated and put back to original color 16 frames. The 16 color frames now are partially encrypted, and watermarked in its partial luminance frame. The schematic is shown in the block diagram Fig. 9.

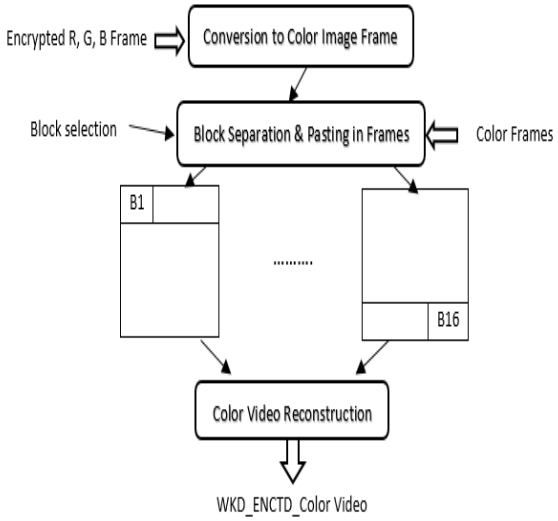

Fig. 9 Construction of the watermarked and encrypted color video

KEY GENERATION:

As we can see from the first phase watermarking, we need 16 different keys for generating 16 unique row/column or pixel position sequence generation. To reduce the need to memorize 16 different keys, we extend the Fig. 1 (a) to Fig. 10 where we use only two keys with a noise value and the support grey image. The final chaotic map uses a key and the number of iterations which are the pixel values of the locations in the gray support image S_G indicated by the unique Row/Column sequence block.

A total of 48 keys are generated of which 32 keys are used for generating 16 unique pixel positions sequences, 16 keys for 16 row sequences and another 16 keys for 16 column sequences generations. The rest 16 keys are used in the chaotic logistic map for generating 16 random binary sequences for encrypting the watermark 16 times. The 16 random binary sequences are almost uncorrelated to each other. Hence only two keys are needed in this stage, and 48 different keys can only be obtained if the support gray image is known. It is important that the same grey support image is kept secret by the manufacturer of the entertainment video.

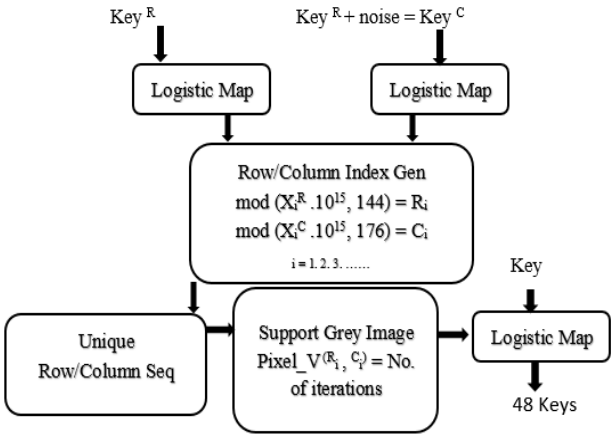

Fig. 10 Different key generation block

SUPPORT IMAGES:

In this paper we use two support images, one is a grey image and the other is a color image, each of size 144x176 pixels. The grey level image is used for different key generation as in Fig. 10 for unique row/column sequence generations and binary random sequence generations. The color support image is used for the first layer pixel value substitution based encryption.

III. RESULTS AND DISCUSSIONS

To show results of our proposed integrated encryption and watermarking, we consider the multimedia video file "*Foreman.avi*" which is of 400 color frames, each of size 144x176 pixels and total duration 33.332 seconds. We consider only the first 16 color frames for the experiment. Conversion to luminance frame, and reconversion to color frames are obtained using Eqs. 9-11. We watermark on each of the16 luminance frames by LSB embedding the full size watermark obtained from IRIS processing of the authentic user. We use 32 keys, as shown in Fig. 10 for generating 16 unique row/column sequences for watermarking on 16 frames. We covert back to color frames, crop a block from each frame as stated in step 4 of system model and methodology, and construct one color frame. We again watermark on the luminance frame obtained from this single color frame. Here we use quantum logistic map for generating the unique row/column sequence for embedding, and for generating random binary sequence. As cited above, we use two support images of size 144x176 pixels as shown in Fig. 11 and Fig. 12. The Fig. 13 shows the first color frame of the digital video of *Foreman.avi.* As is shown in Fig. 5 of first phase watermarking, the luminance or gray level frames 1 – 16, to defy stega-analysis for detection of hiding, we optionally can prepossess such frames before watermarking on them [27]. In this report we show results on successive gray frames and hence to defy stega-analysis we prepossess grey frames before first phase of watermarking. For this we randomly alter 50% of the LSB bits row by row.

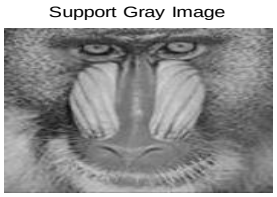

Fig. 11 Support Grey Image

Fig. 12 Support Color Image Fig. 13 First frame of digital video

As explained above, the second phase watermarking is on the luminance frame of the single color frame constructed from 1/16 cropped parts of 16 color frames. We have taken serial blocks for construction. Figs. 14 and 15 show the cropped color frame and the corresponding luminance frame. Figs. 16 and 17 show the corresponding watermarked frames.

Fig. 14 Cropped Color Image **Fig. 15 Cropped Grey Image**

Fig. 16 Watermarked Color Image Fig. 17 Watermarked Grey

For watermarking on the Fig. 15, the unique row/column pixel positions are shown in Fig. 18. Hence Fig 15 and Fig. 16 are obtained after first phase of watermarking. For brevity of space, we do not show the watermarked frames. The first layer of encryption is on R, G, and B frames obtained from Fig. 16. The corresponding substitution based encryption is shown in Figs. 19 - 21.

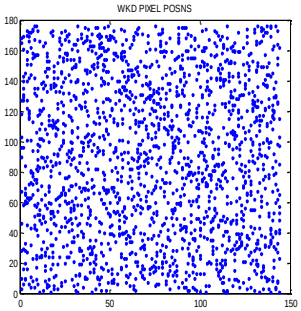

Fig.18 Pixel positions

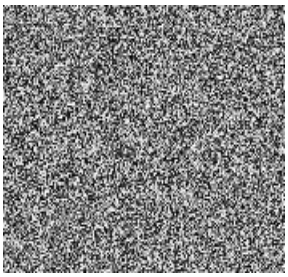

Fig. 19 Encryption -1-R

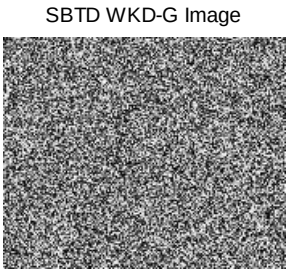

Fig. 20 Encryption-1-G

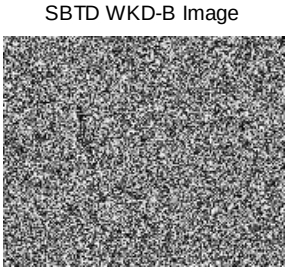

Fig. 21 Encryption-1-B

We have twice encrypted each frame for robustness using the same substitution rule. The second layer of encryption is on the corresponding encrypted frames by substitution. Here also we encrypted twice each frame using the modified Rabinovich hyper-chaotic system and the ciphering rules using Eqs. 11-13. Fig.22 to Fig. 24 shows the results.

For the second layer encryption, we take help of the support color image of Fig. 12. After combining the frames in Figs. 22 – 24, we obtain the watermarked and encrypted color frame shown in Fig. 25, which is the two layer encryted version of Fig. 16. The cropped blocks, after second phase watermarking and two layer encryption, are returned from Fig. 25 to original 16 first phase watermarked color frames. Figs. 26 – 28 show the partial encrypted three frames which also contain watermarks of first phase and traces of watermark from the second phase. As shown in Fig. 10, with two intial keys we can generate a bunch of keys by taking help of a grey support image of Fig. 11.

Fig. 22 Encryption -2-R

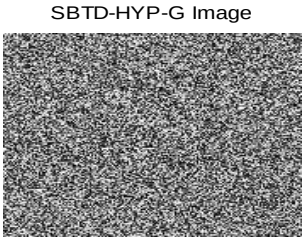

Fig. 23 Encryption -2-G

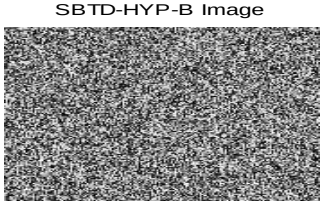

Fig. 24 Encryption -2-B

ENCRYPTED Color Image

Fig. 25 Encrypted Clor Frame **Fig. 26 First frame**

CPD WKD ECRD Col Image

Fig. 27 Seventh Frame **Fig.28 Sixteenth Frame**

Key Space Analysis:

Considering only two secret keys for first layer encryption, four secret keys for second layer encrytion, and support secret gray image , the key spcaee is very large ~ $(10^{15})^2$. $(10^{15})^4 \sim 2^{300}$. As the value indicates, the proposed technique is seen to be very robust. The involvement of the support color image makes it more robust and secure.

Analysis of Pixel Position Sequences and Random Binary sequences:

Correlation Analysis of Random Binary Sequences:

We also find the correlation coefficients between every two different row/column sequences of pixel sequences for LSB embedding, some of which are shown below in table.II The correlation coefficients are very small indicaticating almost no correlation between pixel sequences.Hence no row/column sequence can be generated from the knowledge of any other row/column sequence.

The random binary sequences for ***bitxor*** operation of full size watermark and first phase watermarking are also obtained from 16 different keys from Fig. 10. The correlation coefficients between every two different random sequences are shown below in Table.III As is clear from the values, the random sequences have almost no correlation between them. Hence no random sequence can be obtained from the knowledge of any other random sequence.

TABLE II. ROW/COLUMN correlation coefficients of pixel sequences

-0.0275/ 0.0574	0.0136/ -0.0501	0.0144/ 0.0207	-0.0361/ 0.0014	-0.0150/ -0.0181	0.0054/ 0.0682	-0.0024/ -0.0085	-0.0089/ -0.0237
-0.0036/ 0.1361	-0.0196/ -0.0216	0.0068/ 0.0383	-0.0152/ -0.0182	-0.0532/ -0.0417	0.0055/ -0.147	0.0287/ 0.0295	0.0042/ 0.0577
-0.0144/ 0.0560	-0.188/ -0.0297	0.0192/ -0.0030	0.0012/ -0.0538	-0.0155/ 0.0029	-0.0575/ -0.0014	-0.0202/ 0.0370	-0.0087/ 0.0197
-0.0085/ -0.0215	0.0125/ -0.0508	-0.0158/ 0.0385	0.0073 / -0.0091	-0.0027/ -0.0299	0.0100/ -0.0091	0.0131/ 0.0269	-0.0456/ -0.0249
0.0359/ -0.0305	0.0626/ - 0.0361	-00.0349/ -0.0344	-0.0165/ 0.0349	0.0063/ -0.0094	-0.0020/ 0.0612	-0.0039/ 0.0442	0.0148/ 0.2092

TABLE III. Correlation coefficients between Random Binary Sequences

0.0575	0.0194	-0.0068	0.0083	-0.0361	0.0187	-0.0264	-0.0098
0.0161	0.0099	-0.0265	0.0210	-0.0286	0.0056	-0.0187	-0.0164
-0.0176	0.0063	-0.0199	0.0325	0.0268	-0.0007	0.0207	-0.0153
-0.0118	0.0409	-0.0417	-0.0127	0.0024	-0.0024	-0.0577	-0.0108
-0.0219	-0.0097	0.0188	0.0000	0.0197	0.0029	0.0339	0.0295

Correlation Analysis of Adjacent Pixels:

For analysis of correlation [25] between various vertical and random pairs of pixels in the first layer and second layer of encrypted R, G, B frames, we consider 4000 pairs in each case randomly and find correlation coefficients by using the following mathematical relationships.

$$C_{mn} = \frac{\frac{1}{s}\sum_{i=1}^{S}(m_i-\bar{m})(n_i-\bar{n})^2}{\sqrt{(\frac{1}{s}\sum_{i=1}^{S}(m_i-\bar{m})^2)}\sqrt{(\frac{1}{s}\sum_{i=1}^{S}(n_i-\bar{n})^2)}} \quad (15)$$

$$\bar{m} = \frac{1}{s}\sum_{i=1}^{s} m_i; \quad \bar{n} = \frac{1}{s}\sum_{i=1}^{s} n_i; \quad (16)$$

where C_{mn} is the correlation coefficient, S is the total number of samples, m_i and n_i are the ith pair of sample values. Table.IV shows the results of correlation analysis of the proposed two-layer encryption system. The very small values of correlation coefficients indicate almost no correlation between the vertical, horizontal random pixel pairs.

Chi Square Test:

We also carried the Chi square test on the various encrypted frames. The following is the mathematical relationship for Chi square statistics of the data set represented by the first layer second layer encrypted pixel values of R, G, and B frames.

$$\chi^2 = \sum (X_{ij} - KI)^2 / KI); \quad KI = \frac{144.176}{255} \quad (17)$$

where X_{ij} is the pixel value at the *(i, j)* position in the frame. The *Chi square* test values, shown in Table-4 are large and they indicate that there are no relationships between the pixel values in the respective encrypted frames.

TABLE IV. Various Correlation and Chi Square Test Values

Frame Types: Non Encd, Encd	First Layer Encryption (L1)			Second Layer Encryption (L2)		
	Vertical Corrn.	Horizontal Corrn.	Chi Square	Vertical Corrn.	Horizontal Corrn.	Chi Square
R_ENC	0.0184	0.0005	252.7273	-0.0020	0.0067	237.8182
G_ENC	-0.0138	0.0085	254.9293	-0.0973	0.0486	217.7778
B_ENC	-0.0028	-0.0132	283.6364	-0.0654	-0.0016	279.0303

Encryption Sensitivity Analysis:

Adversaries generally try to establish relationship between the plain text image and the encrypted image frames. If the secret keys are available by some means, the adversaries may try to observe influences on the overall encryption output. As explained above, the support color image is involved in the first layer encryption and hence it is very difficult to crack it. We use the concept of plain text sensitivity to the sensitivity of the two encryption layers. The Number of pixel change rate *NPCR* is used to measure the percentage of different pixel numbers between two image frames, one is encrypted R, G, or B frame I_1 using the first layer encryption and the other is the respective encrypted R, G, or B frame I_2 using the second layer encryption. Also for this analysis, the parameter Unified average changing intensity *UACI* is used as follows and the results are shown in Table-5. The results indicate that the proposed technique is robust against availability of the keys used in the second layer encryption.

$$NPCR = \left(\sum_{i=1}^{H}\sum_{j=1}^{W} Diff(i,j)/W.H\right).100\%$$

$$UACI = \frac{1}{W.H}\left[\sum_{i=1}^{W}\sum_{j=1}^{H}\frac{I_1(i,j)-I_2(i,j)}{256-1}\right].100\% \quad (18)$$

TABLE V. Encryption Sensitivity Analysis Test Values

METRICS	FRAME TYPES & ENCRYPTION LAYER		
	R_L1_Enc, R_L2_Enc	G_L1_Enc, G_L2_Enc	B_L1_Enc, B_L2_Enc
NPCR	0.9965	0.9958	0.9963
UACI	0.3361	0.3294	0.3351

IV. CONCLUSION

We report here a novel integrated partial encryption, and watermarking of short duration entertainment color video. The technique uses chaotic logistic map, 4D hyper-chaos system, and two support images. The partial encryption is very robust and in two layers, and also the watermarking is in two phases. The technique assumes two prong remedy against unauthenticated attempt to use patented entertainment videos. Watermarks are constructed from the iris images of an authentic user or producer, which are binary sequence of full size 1842 bits or half size 920 bits long. Luminance gray level frames are obtained for the first phase watermarking using LSB embedding using full size or half size watermarks. Before first phase watermarking, the gray level frames are preprocessed to defy stega analysis. Blocks from a number of color video frames are assembled to construct one color frame; the second phase of watermarking is carried on the gray level luminance frame of this color frame. The color frame is encrypted in two layers and blocks are redistributed to their original frames. Unauthenticated users cannot decrypt the blocks and hence would be caught. Retrieved watermarks would identify the authentic user or producer. The second phase of watermarking cannot be disturbed as encryption is carried on the watermarked frame. We carry out various analyses which establish the robustness of the proposed integrated technique.

REFERENCES

1. E. Hasanzadeh and M. Yaghoobi, “A novel color image encryption algorithm based on substitution box and hyper-chaotic system with fractal keys” Springer Science + Business Media, LLC, part of Springer Nature 2019.
2. Chong Fu, Gao-yuan Zhang, Mai Zhu, Zhe Chen, and Wei-min Lei, “A New Chaos-Based Color Image Encryption Scheme with an Efficient Substitution Keystream Generation Strategy”, Security and Communication Networks Volume 2018, Article ID 2708532, 13 pages.
3. Xia Huang, Tiantian Sun, Yuxia Li, and Jinling Liang,” A Color Image Encryption Algorithm Based on a Fractional-Order Hyperchaotic System”, Entropy 2015, 17, pp. 28-38
4. T. Gao and Z. Chen, “A New Image Encryption Algorithm Based on chaos”, Physics Letters A 372 (2008), pp. 394-400.
5. Z. Hua, Y. Zhou, and H. Huang, “Cosine-transform based chaotic system for image encryption”, Information Sciences 480 (2019), pp. 403-419.
6. X. Huang and G. Ye, “An image encryption algorithm based on hyper-chaos and DNA sequence”, Multimed Tools Appl., Springer Science + Business Media New York 2012.
7. Ye Liu, Tao Lin, Jun Wang, Hong-Mei Yuan, “Bit Image Encryption Algorithm Based on Hyper Chaos and DNA Sequence”, Journal of Computers Vol. 29 No. 3, 2018, pp. 43-55.
8. Peng Li, Ji Xu, Jun Mou, and Feifei Yang, “Fractional-order 4D hyperchaotic memristive system and application in color image encryption”, EURASIP Journal on Image and Video Processing, (2019) 2019:22.
9. Ying Niu, Xuncai Zhang, and Feng Han, “Image Encryption Algorithm Based on Hyperchaotic Maps and Nucleotide Sequences Database”, Computational Intelligence and Neuroscience Volume 2017, Article ID 4079793, 9 pages.
10. Benyamin Norouzi and Sattar Mirzakuchaki, “A fast color image encryption algorithm based on hyper-chaotic systems”, Nonlinear Dyn, Springer Science + Business Media Dordrecht 2014.
11. N. B. Slimane, K. Boullegue, and M. Machhout,” A novel image encryption scheme using chaos, hyper-chaos systems and the Secure Hash Algorithm SHA-1”, ICCAD’17, Hammamet - Tunisia, January 19-21, 2017.
12. XiangjunWu1, Yang Li, and Jürgen Kurths, “A New Color Image Encryption Scheme Using CML and a Fractional-Order Chaotic System”, PLoSONE 10(3): e0119660, 2015.

13. M., Khan, U. A. khan, A. Ali, F. Hussain, and W. N, "A Robust Color Image Watermarking Scheme using Chaos for Copyright Protection", Mehran University Research Journal of Engineering & Technology Vol. 38, No. 2, 361-378 April 2019.
14. Rania Salah El-Sayed, "Embed Watermark Computing Using Logistic Map Chaotic System for Securing Medical Images", Australian Journal of Basic and Applied Sciences, 11(16) December 2017, Pages: 25-35
15. Heng Zhang, Chengyou Wang, and Xiao Zho, "Fragile Watermarking for Image Authentication Using the Characteristic of SVD", MDPI Journal Algorithms, 2017, 10, 27.
16. Cheng Wei, Li Zhaodan, "Robust Watermarking Algorithm of Color Image Based on DWT-DCT and Chaotic System", 2016 First IEEE International Conference on Computer Communication and the Internet, pp. 370-373.
17. N. Loan, N. N. Hurrah, S. A. Parrah, J. W. Lee, J. A. Sheikh, and M. Bhat, "Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption", Special Section On Information Security Solutions for Telemedicine Applications, Volume 6, 2018, pp. 19876-19897.
18. K. Shankar, M. Elhosney, E. D. Chelvis, S. K. Lakshmanaprabu, and W. Wu, "An Efficient Optimal Key Based Chaos Function for Medical Image Security", Special Section on New Trends in Brain Signal Processing and Analysis, Volume 6, 2018, pp. 77145-77154.
19. Xiong Wang, Akif Akgul, Sezgin Kacar, and Viet-Thanh Pham, "Multimedia Security Application of a Ten-Term Chaotic System without Equilibrium", Wiley Complexity, Volume 2017, Article ID 8412093, 10 pages.
20. Sengul Dogan, "A new data hiding method based on chaos embedded genetic algorithm for color image", Artif Intell Rev (2016) 46:129–143.
21. S. Thakur, A. K. Singh, S. P. Ghrera, and M. Elhoseny, "Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications", Multimed Tools Appl (2019) 78:3457–3470.
22. Somayyeh Mohammadi, "A Chaos- Based Video watermarking in Wavelet Domain", Ciência e Natura, v. 37 Part 2 2015, pp. 364–370.
23. Zhengmao Ye, Hang Yin, and Yongmao Ye, "Security Authentication of Dual Chaotic Image Watermarking in Spatial Domain with Spatial and Frequency Domain Characteristics Analysis", MDPI Appl. Syst. Innov. 2018, 1, 40, 11 pages.
24. C. Pradhan, B. J. Saha, K. K. Kabi, and A. K. Bisoi, "Robust Watermarking Technique using 2D Logistic Map and Elliptic Curve Cryptosystem in Wavelets", Int. J. on Recent Trends in Engineering and Technology, Vol. 10, No. 2, Jan 2014.
25. Chong Fu, Jun-Bin Huang, Ning-Ning Wang, Qi-Bin Hou, and Wei-Min Lei, "A Symmetric Chaos-Based Image Cipher with an Improved Bit-Level Permutation Strategy", Entropy 2014, 16, pp. 770-788.
26. Xiaojun Tong, Yang Liu, Miao Zhang, Hui Xu, and Zhu Wang, "An Image Encryption Scheme Based on Hyperchaotic Rabinovich and Exponential Chaos Maps", Entropy 2015, 17, pp. 181-196.
27. Shreelekshmi R, and M. Wilscy, "Preprocessing of Cover image for More Secure LSB Steganography", International journal of Computer Theory and Engineering", Vol 2, Np. 4, Aug 2010, pp. 1793-8201.

AUTHORS PROFILE

Md. Anwar Hussain, received a B.Sc. degree in Physics from Gauhati University, Assam, India, in 1981, B.Tech. and M.Tech. in Radio Physics & Electronics from Calcutta University, West Bengal, India, in 1985 and 1987 respectively. Also, he received a PhD degree in Electronics and Communication Engineering from Jadavpur University, West Bengal, India, in 2002. He is currently a professor in the Department of Electronics and Communication Engineering at North East Regional Institute of Science and Technology (NERIST), Arunachal Pradesh, India. He has more than 31 years of experience in research and teaching field. His research interests include massive MIMO, High data rate wireless communication & networks, Routing & scheduling in Multi-hop wireless networks, Key distribution in Sensor networks, Multimedia data encryption & security, Mobile computing security, Time-series data modeling and prediction, Networks-on-Chip.

Popi Bora, received B.Sc degree in Physics from North Lakhimpur College under Dibrugarh University in 1997, M.Sc. degree in Physics from Dibrugarh University in 2000, Assam. She is presently a Ph.D Scholar in the Department of Electronics and Communication Engineering, North Eastern Regional Institute of Science and Technology (NERIST), Nirjuli, Arunachal Pradesh. Her research interest includes Digital image processing and security.