DOI: 10.21917/ijivp.2019.0278

PRIVACY PRESERVATION OF VIDEOS USING NEUTROSOPHIC LOGIC BASED SELECTIVE ENCRYPTION

Sayyada Fahmeeda Sultana[1] and D.C. Shubhangi[2]

[1]*Department of Computer Science and Engineering, Poojya Doddappa Appa College of Engineering, India*
[2]*Department of Computer Science and Engineering, Visvesvaraya Technological University, India*

Abstract

Having great photos and video phone, but what happens when you decide to buy a new phone or your storage becomes too full to take any more, back it all on the cloud. It's no secret that videos are a valuable way of communicating information. With attention spans dropping and the need to get larger amounts of information across in a shorter period of time, a well-placed video can take your presentation to the next level these presentations need to be up to date and available wherever you are, back it all on the cloud. Better collaboration and communication through the use of cloud as cloud allows users to access the latest versions of any multimedia data (text, video, images, audio, etc), so they can stay on top changes, which can help businesses to better manage their work flow, regardless of geographical location or spread. Multimedia data like videos stored on cloud are vulnerable to various types of threats like known plain text attach, threat to data, denial of service, etc. To overcome these problems videos need to be encrypted before it gets stored on cloud. Encrypting whole video is a time consuming task, to get rid of time complexity videos can be encrypted using selective encryption many researchers in the state of art have proposed techniques for selective image encryption. In this paper, a frame work is proposed for selective encryption of videos in two stages. The first stage is, Region of interest (ROI) identification performed based on Neutrosophic Logic, watershed image segmentation method. Second Stage is ROI encryption which is performed using the proposed Decision Based Encryption (DBE) Algorithm. The proposed frame work is fast, robust, highly scalable and accurate to meet the need of current internet bandwidth and speed.

Keywords:

Selective Video Encryption, Privacy Preservation, Neutrosophic Logic, Cloud, Decision Based Encryption Algorithm, DBE

1. INTRODUCTION

In this era of non-local storage and with high storage availabilities on cloud the security of most revealing data images/videos becomes more and more important. In addition, special and reliable security in storage and transmission of digital images/videos is needed in many digital applications, such as medical imaging systems, confidential video conferencing and pay-TV etc. Generally, the well-developed modern cryptography should be the perfect solution to this task. As we know, many perfect ciphers have been established and applied widely since 1970s, such as AES, DES, IDEA and RSA. But most conventional ciphers cannot be directly used to encrypt digital video in real-time systems because their encryption speed is not very fast enough, especially when they are applied on complete video contents. Selective encryption of video frames reduces the time of video encryption.

The proposed frame work performs selective encryption on videos in three stages;

Stage 1: Convert the frame into Neutrosophic domain

The Neutrosophic logic which is proposed by smarandache [6]-[10] define the notion of Neutrosophic Set, which is a generalized of Zadeh's fuzzy set and Atanassov's intuitionistic fuzzy set. Neutrosophic logic is an extension/combination of fuzzy logic, intutionistic logic, Para-consistent logic and the three valued logic to describe determinate and indeterminate values. In Neutrosophic logic every element being investigated is described by three values, the degree of membership (*T*), Indeterminacy (*I*) and the degree of non-membership (*F*). In this paper Neutrosophic logic is applied to video frame to convert video frame to neutrosophic domain then neutrosophic logic is applied to convert video frame to binary image.

Stage 2: Identify the Region of Interest

Regions of Interest are identified based by applying Image segmentation on binary image formed by applying Neutrosophic logic. Various image segmentation algorithms are available like, Histogram based, edge based, region based, model based, watershed method. watershed image segmentation algorithm splits a video frame into areas based on topology. The value of the gradients is used for elevation data then the catchment basins are constructed to separate Objects, Edges and Background.

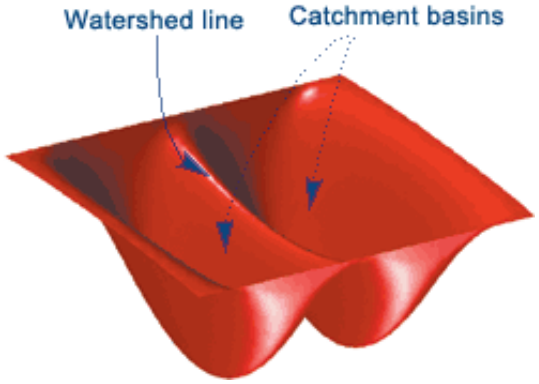


Fig.1. 3D image of watershed concept

The key idea behind watershed transform for segmentation is to change image under processing into another image whose catchment basins are the objects that need to be identified.

Stage 3: Encrypt identified Region of Interest (ROI)

The region of interest includes objects and background, the ROI is encrypted using the proposed Decision Based Encryption (DEB) algorithm.

Rest of the paper is organized with brief review of literature survey in related work in section 2. Section 3, the methodology of our proposed neutrosophic logic based selective encryption. Section 4 exhibits the examination analysis for results of the

proposed method along with the comparison of result with others state of art methods. Concluding remarks and future work of proposed method in section 5 along with contribution of proposed method.

2. RELATED WORK

Neutrosophic Logic (NL) can distinguish between absolute truth and relative truth. NL, like dialetheism, can describe paradoxes, NL(paradox) = (1,*I*,1), while Intuitionistic Fuzzy Logic (IFL) cannot describe a paradox because the sum of components should be 1 in IFL [1]. Watershed segmentation approach based on neutrosophic logic [2]. Real-time selective and format complaint video encryption solution in the scalable extension of (HEVC) standard. The encryption process is performed at the CABAC binstring level and fulfills both constant bit-rate and format compliant video encryption requirements [3]. Encryption algorithms for MPEG video streams and evaluated them with respect parameters like security level, encryption speed, and encrypted MPEG stream size [4]. Multiple techniques for partial video encryption are investigated, for a low impact on rate-distortion performance and having a broad range in scrambling performance [5]. The faro based video encryption [19]. A scheme to source chaotic selective image encryption to the cloud. The plain image is encrypted by the cloud but not exposed to it by steganography. The client can extract the embedded secret data directly in its encrypted form [6]. The plain image is divided into a number of equal size and non-overlapping blocks. Entropy calculation is applied to the individual image blocks to determine the entropy values. To recognize the region of interest (ROI) or sensitive area, the blocks having the highest entropy values are selected. For small encryption time and high security the selected blocks should constitute 25% of the size of the plain image. Arnold's cat map scrambling technique used for encryption [7]. Encryption of videos based on two methods are suggested. The first one is DCEA (DC Coefficient Encryption Algorithm), which is dedicated to protecting the DC component of MPEG video sequences. The second algorithm is "Event Shuffle" for the AC component of MPEG video, it is relatively vulnerable to some attacks [8].

3. PROPOSED METHODOLOGY

Privacy preservation of videos is performed by implementing the following stages on individual frames of video as shown in Fig.2.

3.1 MAPPING ORIGINAL FRAME *I* TO NEUTROSOPHIC SET (I_1)

Let *M* be a subset of a universe of discourse *U*, each element $x \in U$ has degrees of membership, indeterminacy, and non-membership in *M*, which are subsets of the hyper real interval]-0, 1+ [. The notation $x(T,I,F) \in M$ means that Degree of membership of *x* in *M* is *T*

- Degree of indeterminacy of *x* in *M* is *I*
- Degree of non-membership of *x* in *M* is *F*.

M is called neutrosophic set, whereas *T*, *I*, *F* are called neutrosophic components of the element *x* with respect to *M*.

Neutrosophic set is a generalization of the intuitionistic set [21], fuzzy set [22], paraconsistent set [23], dialetheist set [24], paradoxist set and tautological set [25].

{*A*} is an even to entity, {*Non-A*} is not of {*A*}, and {*Anti-A*} is the opposite of {*A*}. Also {*Neut-A*} is defined as neither {*A*} nor {*Anti-A*}. For example, if {*A*} = white, then {*Anti-A*} = black. {*Non-A*} = blue, yellow, red, black, etc. (any color except white). {*Neut-A*} = blue, yellow, red, etc. (any color except white and black).

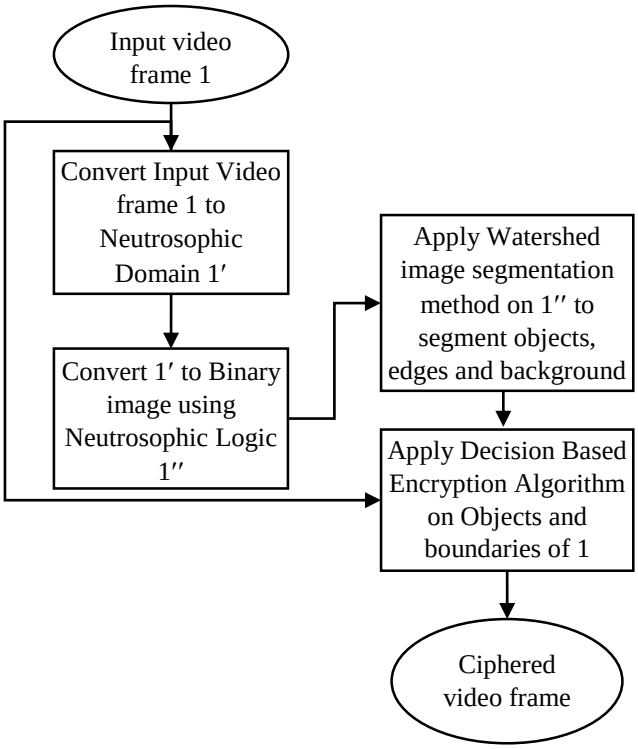


Fig.2. Block diagram proposed video frame encryption frame work

An element $A(T,I,F)$belongs to the set in the following way: it is *t* true ($t \in T$), *i* indeterminate $i \in I$, and *f* false ($f \in F$), where *t*, *i*, and *f* are real numbers in the sets *T*, *I*, and *F*. As in [2], an image is transferred to the neutrosophic domain by representing pixel in the neutrosophic domain as *P*(*T*, *I*, *F*), where pixel is *t*% true, *i*% indeterminate and *f* % false, where *t* varies in *T*, *i* varies in *I*, and *f* varies in *F*. In this method objects are *T* and backgrounds are *F*.

Choose the object to be encrypted based on neutrosophic set <*T*, *I*, *F*>

The image is converted into objects (*T*) and background (*F*) through the following steps [2]:

- Convert image using *S* function:

Given an image *IM*, Pixel(*i*,*j*) is a pixel at coordinate (*i*,*j*) and *T*(*i*,*j*)is defined as

$$T(i,j) = S(g_{ij},a,b,c) \quad (1)$$

$$S = 0 \text{ if } 0 \le g_{ij} \le a \quad (2)$$

$$S = \frac{\left(g_{ij} - a\right)^2}{(b-a)(c-a)} \text{ if } a \le g_{ij} \le b \quad (3)$$

$$s = 1 - \frac{(g_{ij} - c)^2}{(c-b)(c-a)} \text{ if } b \le g_{ij} \le c \quad (4)$$

$$s = 1 \text{ if } g_{ij} \ge b \quad (5)$$

where, $F(i,j) = 1\text{-}T(i,j)$, g_{ij} is the intensity value of pixel, to find the value of S function for each pixel need value of a, b, c.

$$a = (1 - f)(g_1 - g_{min}) + g_{min} \text{ if } a > B_1 \text{ then } a = B_1 \quad (6)$$

$$c = f(g_{max} - g_n) + g_n \text{ if } (c > B_2) \text{ then } c = B_2 \quad (7)$$

where, g_1, g_2,….g_n are the intensity of first to last pixel, respectively. g_{min} is the minimum intensity and g_{max}.

Maximum intensity f=0.01 is calculated using local maxima of histogram [2].

Parameter b is calculated using maximum entropy principal [2] defined as,

$$H(i) = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} S_n(T(i,j)) \quad (8)$$

where, S_n is a Shannon function, the optimal b will result the largest $H(i)$.

Homogeneity in intensity domain decides (I). The value of $I(i,j)$ has a range of [0,1]. The more uniform the region surrounding a pixel is, the smaller the value of the pixel.

- Convert the image to a binary image based on (T,I,F)

Divide the given image into three parts: objects (O), edges (E), and background (B). $T(i,j)$ represents the degree of being an object pixel, $I(i,j)$ is the degree of being an edge pixel, and $F(i,j)$ is the degree of being a background pixel for pixel $Pixel(i,j)$, respectively. The O, E and B are defined as,

$$O(i,j) = \begin{cases} true & T(i,j) \ge t_t \quad I(i,j) < \gamma \\ false & otherwise \end{cases} \quad (9)$$

$$E(i,j) = \begin{cases} true & T(i,j) < t_t VF(i,j) < t_f \quad I(i,j) \ge \gamma \\ false & otherwise \end{cases} \quad (10)$$

$$B(i,j) = \begin{cases} true & F(i,j) \ge t_t \quad I(i,j) < \gamma \\ false & otherwise \end{cases} \quad (11)$$

where, t_t and t_f are the thresholds of T, γ = 0.01. After O, E, B is determined the image is mapped to binary using,

$$binary(i,j) = 0 \text{ if pixel}(i,j) \in O \text{ or } E \text{ or } B \quad (12)$$

$$binary(i,j) = 1 \text{ if pixel}(i,j) \notin O \text{ or } E \text{ or } B \quad (13)$$

Further, Watershed algorithm is applied on converted binary image to obtain optimal image boundaries. Objects and boundaries are the ROI. Apply the proposed Decision Based Encryption (DBE) algorithm on ROI pixels in original frame I.

3.2 PROPOSED DECISION BASED ENCRYPTION (DBE) ALGORITHM

In this paper the Decision based Encryption Algorithm is applied to only the objects, Edges and Boundaries obtained from the above stages to reduce the encryption time of video and also to perform content based retrieval on encrypted videos.

3.2.1 Convert Pixel Magnitude to Modified BCD Form:

The proposed DBE algorithm works on the bases of modified BCD (Binary Coded Decimal) form as BCD representation of number require more than 8 bits to represent all 255 pixel magnitudes. The proposed algorithm uses the following pattern of representing each pixel magnitude as shown in Table.1, where example a = 04 is represented as "00000100" in modified BCD form which is same as binary representation. All the pixel magnitude from 0 to 7 follows the same binary representation so example with a=07 follows the same explanation. Third example in Table.1, a = 72, 72 is represented in modified BCD form as "0111 0010" and 72 in binary form is written as 1001000. Same pattern follows for all pixel magnitudes between the range 10 and 159.

The pixel magnitudes from the range 160 to 255 follows a different pattern as shown in example with value of a as 160, 217, 255. 160 in binary is represented as 10100000, 160 in BCD form is written as 1 0000 0 000 and in modified BCD 160 is represented as 00001000 so as 217 and 255. As explained in Table.1.

Table.1. Examples of Pixel magnitude in Modified BCD form

b8	b7	b6	b5	b4/b9	b3	b2	b1
0	0	0	0	0	1	0	0

a=04 (Decimal form of modified BCD 04)

b8	b7	b6	b5	b4/b9	b3	b2	b1
0	0	0	0	0	1	1	1

a=07(Decimal form of modified BCD 07)

b8	b7	b6	b5	b4/b9	b3	b2	b1
0	1	1	1	0	0	1	0

a=72(Decimal form of modified BCD 114)

b8	b7	b6	b5	b4/b9	b3	b2	b1
1	1	1	1	0	1	1	1

a=159 (Decimal form of modified BCD 247)
(8 and 9 are represented as 7)

b8	b7	b6	b5	b4/b9	b3	b2	b1
0	0	0	0	1	0	0	0

a=160 (Decimal form of modified BCD 8)

b8	b7	b6	b5	b4/b9	b3	b2	b1
0	1	0	1	1	1	1	1

a=217 (Decimal form of modified BCD 195)

b8	b7	b6	b5	b4/b9	b3	b2	b1
1	0	0	1	1	1	0	1

a=255(Decimal form of modified BCD 157)

To make a difference of each pixel with its neighboring pixel the modified BCD form is XOR with Key to generate ciphered value. The proposed DBE algorithm is shown in algorithm1 Decryption is performed with Algorithm 2 Decision Based Decryption Algorithm.

Algorithm 1: Decision Based Encryption Algorithm

Input: Pixel Magnitude a, Key K

Output: Ciphered Pixel magnitude a_{new}

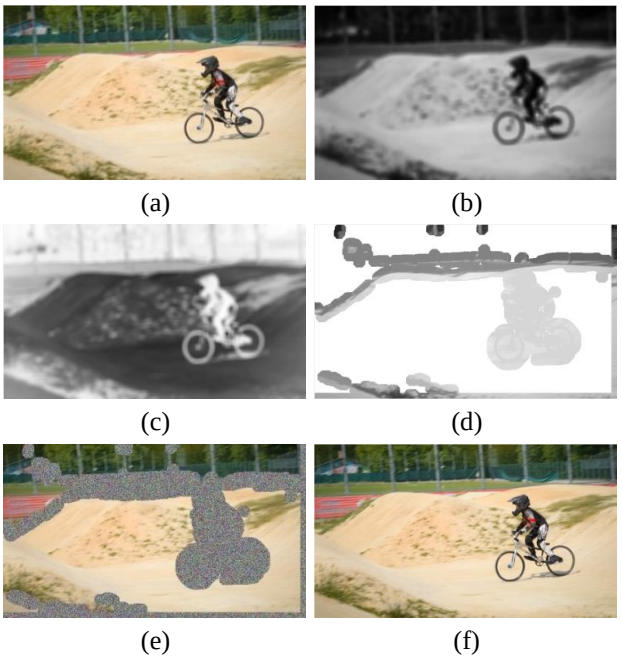
Step 1: *Count_no*_10 = 0, *temp*=0;
Step 2: While *a*>9 do
a=*a*-10;
*Count_no*_10 = *Count_no*_10+1;
end
Step 3: if *Count_no*_10 == 0 then
temp = *binary*(*a*,8);
end
Step 4: if *Count_no*_10 < 160 then
$Temp_1$ = *binary*(*Count_no*_10,8);
$Temp_2$ = *binary*(*a*,8);
$Temp_1$ = *Circular_Shift*($Temp_1$,4);
temp = OR($Temp_1$,$Temp_2$);
end
Step 5: if Count_no_10>=160 then
$Temp_1$ = *binary*(*Count_no*_10,8);
$Temp_2$ = *binary*(*a*,8);
$Temp_1$ = *Circular_Shift*($Temp_1$,4);
$Temp_1$ = *LeftShift*($Temp_1$,1);
temp = OR($Temp_1$,$Temp_2$);
temp = Setbit(*temp*(4),1);
end
Step 6: a_{new} = XOR(*temp*,*K*);

Algorithm 2: Decision Based Decryption Algorithm

Input: Ciphered Pixel Magnitude a_{new}, Key *K*
Output: Deciphered Pixel Magnitude *a*
Step 1: *temp* = XOR(a_{new},*K*);
Step 2: *D* = Getbit(*temp*(4));
Step 3: *C* = Getbits(*temp*(9…5));
a = Getbits(*temp*(4…1));
Step 4: if *D* == 0 then
C = binary_to_decimal(*C*);
a = binary_to_decimal(*a*);
a = (*C**10)+*a*;
end
Step 5: if *D*!=0 then
a = Setbit(*temp*(4),0);
C = binary_to_decimal(*C*);
a = binary_to_decimal(*a*);
a = ((*C*+16)*10)+*a*;
end
Step 6: return (*a*)

4. RESULT AND ANALYSIS

Simulation on the DBE encryption algorithm is done on Akiyo, Big Buck Bunny, Bridge (close), Bridge (Far), Bus, Carphone, Claire, Coastguard, Container, Elephants Dream, Waterfall, Tempete test video files and around 100 video clips from YouTube. The Fig.3 shows the stages of ciphering video frame. The results show that perceptibility of ciphered video is decreased as the object of interest gets encrypted.



(a) (b) (c) (d) (e) (f)

Fig.3. Stages of Video frame encryption (a) Original Video frame (b) Neutrosophic T domain image (c) Neutrosophic F domain image (d) Image Segmented using Watershed Algorithm (e) Object of Interest Pixels encrypted using DBE algorithm and (f) Decrypted Video frame

4.1 ANALYSIS OF RESULT

In this section, the proposed algorithm is subjected to various performance and security analyses to ascertain it robustness.

4.1.1 Procession Time:

The Table.2 contains the time taken by some of the most commonly used cryptographic algorithms for single pixel, AES, XOR. RSA algorithms are coded in Matlab and Blowfish algorithm in C++. DBE takes less encryption time then other algorithm with less complexity.

Table.2. Encryption and Decryption time for single pixel (Time in Seconds)

State of Art Algorithms	Encryption Time (s)	Decryption Time (s)
Blowfish	0.119	0.119
AES	0.119	0.119
XOR	0.22	0.22
RSA	0.7	2.0
Proposed DBE	0.12	0.101

The proposed DBE encryption algorithm take least encryption and decryption time as compared to other state of art techniques

4.1.2 Visual Degradation:

The peak signal-to-noise ratio (PSNR) is used to measure the level of visual distortion of cipher video. Together with the Mean Square Error (MSE), image compression quality can be compared. MSE depicts the cumulative squared error between the compressed and the original image, whiles PSNR depicts a measure of the peak error. A lower value of MSE implies a lower error created. However, a lower value of the PSNR implies a higher visual degradation in cipher image. PSNR and MSE are calculated as shown in Equation and Equation respectively.

$$P_{SNR} = 10\log_{10}(M^2/MSE) \tag{14}$$

where, M is maximum fluctuation in input image.

$$MSE = \sum_{i=1:m}\sum_{j=1:n}\frac{\left[I_1(i,j)-I_2(i,j)\right]^2}{m*n} \tag{15}$$

The average PSNR and MSE values for selected plain and cipher video frames are shown in Table.3. The lower values of PSNR and higher values of MSE gives difference exists between the cipher video and their plain form.

4.1.3 VIFP (Visual Information Fidelity in Pixel) Domain:

The VIFP is based on two data variables the statistics between initial and final stage of visual channel when there is no distortion, and Second variable is mutual data between the input of distortion block and the output of visual system blocks. For reference image or in the absence noise, signal first passes through visual channel before entering the brain, which selects cerebral data from it. Where, as in case of noisy images source signal passes through another biased channel before coming in to perceptible channel. Combining the above stated two variables, a fidelity measure is extracted out.

Table.3. Comparison of Original frame to Ciphered Frame

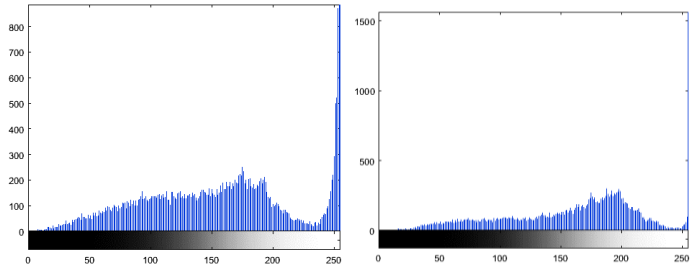
Comparison of Original frame to Ciphered Frame	Result
MSE	2.6488e+03
PSNR	13.9002
SSIMVAL (Structural similarity index value)	0.3555
VIFP	0.0219

Table.4. Comparison of Original frame to Ciphered Frame

Comparison of Original frame to decrypted Frame	Result
MSE	8.32
PSNR	38.92
SSIMVAL (Structural similarity index value)	0.9967
VIFP	0.9845

4.1.4 Chosen Known-Plain Text Attacks:

The Fig.5 shows the histogram analysis of the effect of chosen or known-plaintext attacks. The plain video frame a) and its corresponding cipher frame b). Since the histogram of part a) and part b) are different at objects of interest, the proposed technique is resistant against chosen/known-plaintext attacks given limited resources and the value of the video over time.



(a) (b)

Fig.5. Histogram (a) Original video frame (b) encrypted video frame

4.1.5 Decryption Efficiency:

The sum of the difference between the pixels of the original and the recovered frames are computed to be 99.8% same as the original image. These results indicate that the decryption process recovers plain video with an efficiency of 99.8% the encryption algorithm produce error of 0.2%.

5. CONCLUSIONS AND FUTURE WORK

The proposed privacy preservation of video using Neutrosophic Logic based Selective Encryption is a three-phase process for video frames through the use of Neutrosophic domain. In this first phase, we convert the frame into neutrosophic logic<*T*, *I*, *F*>. The second phase, Watershed image segmented algorithm is applied on Neutrosophic Frame to extract Region of Interest for encryption. The third and last phase is to encrypt ROI through the proposed Decision Based Encryption and Decryption algorithm. The Proposed methodology reduces the encryption and decryption time as only the selected regions need to be encrypted. Use of Neutrosophic Logic gives more accuracy intuitionistic fuzzy logic. Proposed DBE algorithm is fast robust and secure for any type of data. The proposed frame is helpful for content based retrieval on encrypted videos. The proposed frame work can be extended for content based retrieval from given images to encrypted video retrieval.

REFERENCES

[1] Florentin Smarandache, "Neutrosophic Logic-A Generalization of the Intuitionistic Fuzzy Logic", *International Journal of Pure and Applied Mathematics*, Vol. 24, No. 3, pp. 287-297, 2005.

[2] Ming Zhang, Ling Zhang, H.D. Cheng, "A Neutrosophic Approach to Image Segmentation based on Watershed Method", *Signal Processing*, Vol. 90, No. 5, pp. 1510-1517, 2010.

[3] W. Hamidouche, M. Farajallah, N.O.-Sidaty, S.E. Assad and O. Deforges, "Real-Time Selective Video Encryption based on the Chaos System in Scalable HEVC Extension", *Signal Processing: Image Communication*, Vol. 58, No. 1, pp. 73-86, 2017.

[4] L. Qiao and K. Nahrstedt, "Comparison of MPEG Encryption Algorithms", *Computers and Graphics*, Vol. 22, No. 4, pp. 437-448, 1998.

[5] G.V. Wallendael, A. Boho, J.D. Cock, A. Munteanu and R.V.D. Walle, "Encryption for High Efficiency Video Coding with Video Adaptation Capabilities", *IEEE Transactions on Consumer Electronics*, Vol. 59, No. 3, pp. 634-642, 2013.

[6] Tao Xiang**,** Jia Hu and Jianglin Sun, "Outsourcing Chaotic Selective Image Encryption to the Cloud with Steganography", *Digital Signal Processing*, Vol. 43, pp. 28-37, 2015.

[7] Ahmed M. Ayoup, Amr H Hussein and Mahmoud Ali, "Efficient Selective Image Encryption", *Multimedia Tools and Applications*, Vol. 75, No. 24, pp. 17171-17186, 2016.

[8] G. Liu, T. Ikenaga, S. Goto and T. Baba, "A Selective Video Encryption Scheme for MPEG Compression Standard", *IEICE Transaction on Fundamentals*, Vol. 89, No. 1, pp. 194- 202, 2006.

[9] Zafar Shahid and William Puech, "Visual Protection of HEVC Video by Selective Encryption of CABAC Bin-Strings", *IEEE Transactions on Multimedia*, Vol. 16, No. 4, pp. 24-36, 2014.

[10] Wassim Hamidouche, Mickael Raulet and Olivier De-Forges, "Real time SHVC Decoder: Implementation and Complexity Analysis", *Proceedings of IEEE International Conference on Image Processing*, pp. 233-239, 2014.

[11] Jiri Fridrich, "Symmetric Ciphers based on Two-dimensional Chaotic Maps", *International World Scientific Journal on Bifurcation and Chaos*, Vol. 8, No. 6, pp. 1259-1284, 1998.

[12] Safwan E1 Assad and Hassan Noura, "Generator of Chaotic Sequences and Corresponding Generating System", US Patent-US20130170641A1, University of Nantes, 2014.

[13] Mousa Farajallah, Z Fawaz, Safwan E1 Assad and Olivier Dforges, "Efficient Image Encryption and Authentication Scheme based on Chaotic Sequences", *Proceedings of International Conference on Emerging Security Information Systems and Technologies*, pp. 150-155, 2013.

[14] Rukhin Andrew, Soto Juan, Nechvatal James, Smid Miles and Barker Elaine, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", Technical Report, Department of Commerce, National Institute of Standard and Technology, 2001.

[15] Vivienne Sze and Madhukar Budagavi, "High Throughput CABAC Entropy Coding in HEVC", *IEEE Transactions on Circuits and System for Video Technology*, Vol. 22, No. 2, pp. 1778-1791, 2012.

[16] Nakkl Masuda, Goce Jakimoski, Kazuyuki Aihara and Ljupco Kocarev, "Chaotic Block Ciphers: from Theory to Practical Algorithms", *IEEE Transactions on Circuits and Systems I: Regular Papers*, Vol. 53, No. 6, pp. 1341-1352, 2006.

[17] Xingyuan Wang, Dapeng Luan and Xuemei Bao, "Cryptanalysis of an Image Encryption Algorithm using Chebyshev Generator", *Digital Signal Processing*, Vol. 25, No. 2, pp. 244-247, 2014.

[18] Shiguo Lian, Jinsheng Sun, Jinwei Wang and Zhiquan Wang, "A Chaotic Stream Cipher and the usage in Video Protection", *International Journal of Chaos Solitons and Fractals*, Vol. 34, No. 3, pp. 851-859, 2007.

[19] S.F. Sultana , and D.C. Shubhangi, "Video Encryption Algorithm and Key Management using Perfect Shuffle", *International Journal of Engineering Research and Applications*, Vol. 7, No. 2, pp. 1-5, 2017.

[20] K.T. Atanassov, "Intuitionistic fuzzy sets", *Fuzzy Sets and Systems*, Vol. 20, No. 1, pp. 87-96, 1986.

[21] L.A. Zadeh, "Fuzzy Sets", *Information and Control*, Vol. 8, No. 3, pp. 353-383, 1965.

[22] G. Priest, "*Paraconsistent Logic*", Kuluwer Academic Publishers, 2002.

[23] W. Bruno, "Dialethesim, logical consequence and hierarchy", *Analysis*, Vol. 64, No. 4, pp. 318-326, 2004.

[24] F. Smarandache, "*A Unifying Field in Logics Neutrosophic Logic, Neutrosophy, Neutrosophic Set*", American Research Press, 2003.

[25] Mario Preishuber, Thomas Hütter, Stefan Katzenbeisser and Andreas Uhl, "Depreciating Motivation and Empirical Security Analysis of Chaos-Based Image and Video Encryption", *IEEE Transactions on Information Forensics and Security*, Vol. 13, No. 9, pp. 2137-2150, 2018.