ISSN 2278-3091
Volume 9, No.5, September - October 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse28952020.pdf
https://doi.org/10.30534/ijatcse/2020/28952020

An Efficient Chaotic Encryption with Video Watermarking Technique using Improved Whale Optimization Algorithm

J. Udayakumar[1], Dr. G. Prabakaran[2], Dr. R. Bhavani[3], Dr. P. Sudhakar[4]
[1]Research scholar, Dept., of CSE, FEAT, Annamalai University,uday.ja@gmail.com
[2]Associate Professor, Dept of CSE., FEAT, Annamalai University, gpaucse@yahoo.com
[3]Professor, Dept of CSE., FEAT, Annamalai University, bhavaniaucse@gmail.com
[4]Associate professor, Dept of CSE., FEAT, Annamalai University,kar.sudha@gmail.com

ABSTRACT

Due to the advancements and familiarity of the Internet and the rise of different live broadcasting environments, digital videos have become a part of every day's life. On the other hand, security of videos poses a major threat in the common public networks. Digital watermarking is an effective approach commonly used to secure the digital information. Watermarking is a process of hiding data into multimedia content with no loss of the quality of the content in such a way that the watermark can be extracted by the legal user. This paper proposes a new digital video watermarking with encryption (DVWE) technique using improved whale optimization algorithm. The proposed model initially splits the input video into a sequence of frames and watermark data is hidden into every individual frame. Then, the image frames are decomposed using multi-level discrete wavelet transform (DWT). Besides, improved whale optimization algorithm (IWOA) is derived by incorporating the benefits of whale optimization algorithm (WOA) with levy flight (LF) concept for optimal pixel selection in the cover image. Followed by, the R, G and B components in the watermark data is encrypted by three encryption techniques namely elliptic curve cryptography (ECC), double logistic chaotic map (DLCM) and signcryption. As a result, the encrypted watermark image data is embedded into the cover image and then converted into a watermarked video. At the receiving end, the reverse process takes place to retrieve the secret watermark video. In order to assess the performance of the proposed model, an extensive experimental results analysis takes place. The simulation outcome depicted the effective performance of the presented model over the existing models.

Key words: Digital watermarking, Encryption, Data hiding, Whale optimization, Levy flight

1. INTRODUCTION

The digitization of multimedia details with the establishment of computer techniques and systems have resulted in better efficiency in production, memory, and broadcasting the digital contents, like images, audios, and videos. In particular, network bandwidth as well as computer memory were enhanced using Moore's law [1]. At the same time, with the help of Internet, multimedia details are interchanged and induced globally. Recently, webcast as well as video-on-demand (VOD) facilities were invoked and distributed robustly all over the world, and establishments of TV, film, represents the growth of industries. Finally, the number and time of online videos are enhanced progressively, and contents are encompassed. Under the application of Internet, user perform the operations like copying, pasting, and forward videos, songs, collect essential details that makes better convenience for users. Therefore, it is also followed by illegitimate actions like intrusion, infringement, and stealing, that ruins the intellectual rights of digital owners; however it affects market order of digital publications. Moreover, pirated works have major risk in protection of users as it is inferior and shares the viruses. The problem of piracy infringement is a massive barrier for developing video industry. Thus, copyright security for digital video is significant in recent decades. Data concealing model hides significant details in digital product, and secret message has been forwarded by delivering open carrier, that is considered as efficient model for analyzing the secured transmission of secret data in a system [2]. This model is composed of steganography, digital watermark, and covert communication.

When compared with these models, digital watermark is an effective part of data hiding, which is applicable to resolve the issues of copyright security for digital goods. It encloses unknown symptoms into digital things like copyright data. Along with that, unauthenticated individuals are not able to examine hidden details as well as copyright security has been accomplished. If pirated thongs are displayed, product descriptors could extract concealed data for ensuring the copyright ownership and track performs of infringement. Followed by, it offers legal witness to charge illegitimate infringement. The main aim of digital watermarking is to provide copyright safety. Under the application of this model, the scope is progressively developed along with copyright

security, copy management, fingerprint analyzing, content authorization, broadcast observation, video monitoring, and so forth [3]. At the same time, the application objects are expanded from traditional digital images to alternate applications like videos, texts, speech etc. Concurrently, video content is considered as major stream of data appeared in web pages, thus the copyright security of video is highly essential. Finally, video watermarking model has become one of the important topics in recent times.

Video watermarking varies from image watermarking. Initially, video signals are malicious for pirate attacks, like interpolation, frame interchanging, frame dropping, frame averaging, and so on. Then, offering imperceptibility of watermark on a video is complicated when compared to an image, as the watermark embedding strategy has to apply temporal difference to 3D features of a video. Thirdly, video watermarking is based on incorporating the similar watermark in all frames, in which an intruder collude the frames from diverse cases to extract the watermark, that results in statistical perceptual invisibility supervising issues for all frames, where the attacker consider the benefits of motionless regions in former video frames for eliminating the watermark when compared to frames averaging.

Fast Fourier Transform (FFT), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD), Contourlet Transform and hidden markov model (HMM) in wavelet domain has been presented [3]. Therefore, watermarking methods are dependson discrete Fourier transform (DFT) experiences cropping intrusions and if the aspect ratio is modified, it is impossible for watermark to retain the modifications as it affects the image frequency content. Recently, massive works have been developed with the objective of digital watermarking according to DCT. In [4], a new digital watermarking method was established by applying DFT-DCT. The performances have recommended the demerits and merits of DCT-related execution.

[5] examined an unknown as well as effective speech watermarking system under the application of DCT and SVD methodologies. [6] investigated the Quantization Index Modulation (QIM) watermarking approach to images in DCT space. Therefore, the DCT-aided watermarking models suffer from worse robustness as opposed to high level compression. Besides, this model shows ineffective function over the attacks of de-synchronization such as geometric distortions. Then, DCT has been implemented while combining DWT for accomplishing improved watermarking function [7]. Moreover, the unified DWT-DCT related watermarking approaches are expanded by developing a hybrid as well as smart SVD-aided perceptual approach [8].

A block smart fragile watermarking model by applying DCT has been reported in [9] that finds and retrieves tampered photographs. [10] extended DCT-DWT and SVD related watermarking methods to color images and examined for normalizing the benefits. By the integration of DCT and Spatio-temporal HVS relied video watermarking frameworks are addressed in [11], that applies QIM scheme for embedding and predicting the watermark in 2DDCT space. Followed by [12], an effective bio-metric watermarking scheme has been executed by securing the format of biometrics such as fingerprints as well as iris features. Moreover, a fusion principle has been deployed for maximizing the entire function of bio-metric watermarking.

Blind audio watermarking by applying discrete wavelet packet transform (DWPT) and DCT has been established in [13], where a perceptual QIM is utilized for embedding the watermarked bits within the cover audio. Furthermore, a back-propagation neural network (BPNN) has been applied to approve the watermark objectives in harsh environments. Even though the DWT and parameters are effective, such as dual-tree complex wavelet transform (DT-CWT), non-redundant CWT (NR-CWT) and DWT-relied multi-resolution transforms still suffers from limited way in filtering design. In general, watermarked images are composed of acute message among scene objects namely, lines, textures, corners and edges. Because of worst directionality, exact implication of these structures becomes impossible using DWT based multi-resolution transforms.

Using improved whale optimization algorithm (IWOA). The proposed model involves different processes namely frame extraction, optimal pixel selection, encryption, embedding and reconstruction. At the initial stage, the cover video and the watermark video are divided into sequences of frames. Next, image decomposition process is carried out using multi-level discrete wavelet transform (DWT). Also, improved whale optimization algorithm (IWOA) is derived by incorporating the benefits of whale optimization algorithm (WOA) with levy flight (LF) concept for optimal pixel selection in the cover image. Followed by, the R, G and B components in the watermark data is encrypted by three encryption techniques namely elliptic curve cryptography (ECC), double logistic chaotic map (DLCM) and signcryption. As a result, the encrypted watermark image data is embedded into the cover image and then converted into a watermarked video. At the receiving end, the reverse process takes place to retrieve the secret watermark video.

2. THE PROPOSED METHOD

Figure 1 depicts the structural flow of newly developed model. Initially, the cover video and the watermark video are divided into sequences of frames. The presented approach contributes in modifying the cover image as R, G and B units in a separate manner. Followed by, Multilevel DWT transformation has been used for decomposing the modules of cover image. Under the application of transformation units, better pixels are chosen under the application of IWOA. Next, embedding is carried out in the effectively decided pixels. The isolated units are encrypted using various encryption

approaches. The 'R' units are encrypted using ECC; 'G' units are encrypted by applying DLCM, as well as 'B' units are encrypted by utilizing signcryption method. Hence, encrypted part of secret video frame is again incorporated into effectively selected part of cover image. Finally, the stego frames are again merged to generate a watermarked video.

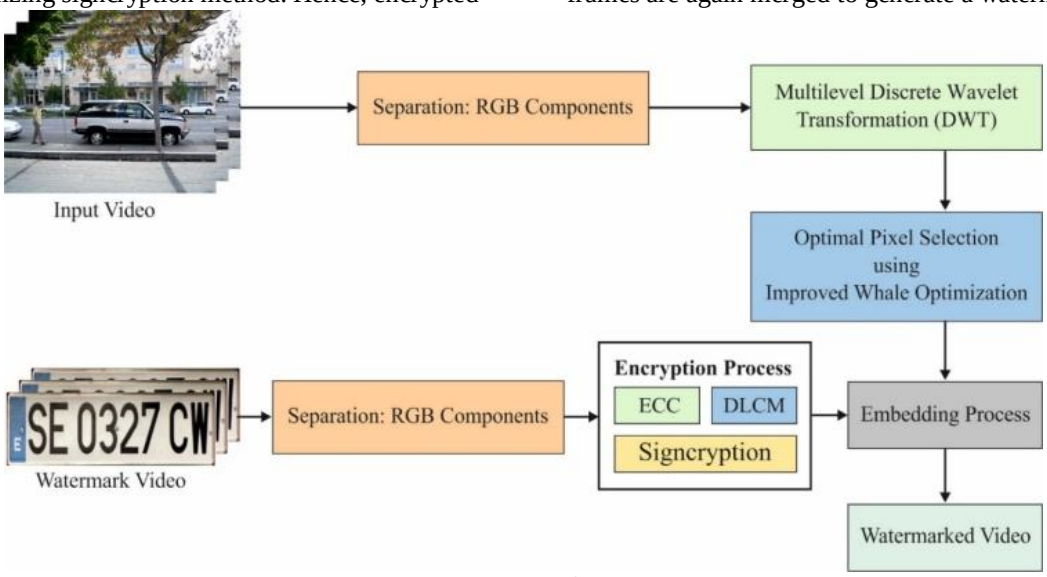

Figure 1: Block diagram of proposed model

2.1 Image Decomposition

The input image is classified into R, G and B modules individually to examine the modules of the initial colors of all parts of the image [14]. In RGB, the cover image is separated on the basis of LL, LH, HL and HH bands for determining the pixels' position. The 2-D DWT are significant spatial fields to frequency field transformation method. A splitting is completed by 2 processes, namely Horizontal and Vertical processes. The horizontal processes decay an image into Low (L) and High (H) frequency bands. After that the vertical function decays an image into LL_1, LH_1, HL_1 and HH_1 frequency bands. In 2nd level of decay, LL_1 band is decayed again into LL_2, LH_2, HL_2 and HH_2. Assume the size of the image be M^*N'. Initially, to filter and down sample, the horizontal decay diminishes the image to $M \times \frac{N}{2}$ size. The vertical one decreases the samples of the image to $\frac{M}{2} \times \frac{N}{2}$. The single□level decay outcome is established as

$$[C_1 C_2 C_3 C_4] = DWT(C) \quad (1)$$

where 'C_1', 'C_2', 'C_3', and 'C_4' signify the coefficient values of the decay frequency bands. 'C_1' is the lesser level frequency band that is adding decay for extracting the sub□bands and is provided under:

$$[C_1^{LL1} C_1^{LH1} C_1^{HL1} C_1^{HH1}] = DWT(C) \quad (2)$$

A coefficient in the lesser frequency band C_1^{LL1} is yet again decay, as it gives the texture and edge□related data of the image. Another level of decomposition is executed on the lesser band LL_1. A decomposed type of the frequency band is provided as follows:

$$[C_1^{LL2} C_1^{LH2} C_1^{HL2} C_1^{HH2}] = DWT(LL) \quad (3)$$

where C_1^{LL2} implies the low level frequency band of the 2nd□level decomposition.

2.2 Optimal Pixel Selection using IWOA

The multilevel DWT transformed image provides vector coefficients of an image. When compared with diverse vector coefficients, a best pixel has been elected under the application of IWOA. Generally, WOA is stimulated by the hunting performance of humpback whales that applies the shrinking encircling method, spiral for simulating bubble□net assaulting method and surrounds the prey [14].Here, 3 functions accelerate the performances of humpback whales are encircling victim, exploring the victim (exploration stage) and bubble-net foraging (exploitation stage), correspondingly.

2.3 Secret image encryption

The secret image is modified as RGB modules independently. The divided R, G and B components undergoes encryption by applying 3 modules like ECC, DLCM and Signcryption, correspondingly. Thus, the separate RGB encryption ensures the better security of embedding principle.

A. Encryption of R components using ECC

In ECC, a prime number is chosen as n_p and private key is chosen as H. Afterwards, an Elliptic curve cubic equation is derived as given below:

$$B = p(i))^3 + u * p(i) + v \quad (4)$$

Where, u and v are the constants and it is $u = v = 2$. When the condition $X = Y$ is fulfilled, an optimal point is chosen to the elliptic curve. The X and Y is defined by

$$X = mod\ (E, n_p) \quad (5)$$

$$Y = mod\ ((p(j))^2, n_p) \quad (6)$$

where, $p(i,j)$ denotes the point of elliptic curve. n_p refers the prime number. A doubling procedure is utilized for finding X and Y values. An optimal point $P_e(k,l)$ and P_f is the public key. A public key P_f is represented as

$$P_f = H * P_e \quad (7)$$

Encryption method

In encryption technique, all shares have block and all blocks section is encrypted by encryption technique. A numbers of blocks are illustrated as $b(i,j)$, where i and j are row and column of the block shares [15]. During these processes, all 2 parts of the data in provided as input to the encrypted technique. A data $D_x(i,j)$ and $D_y(i+1,j)$ and the point is

$$C_1 = H * P_e (8)$$

$$C_2 = (D_X, D_y) + C_1 \quad (9)$$

Decryption method

In decryption model, private key (H) is utilized for decrypting the message and point C_{11} is utilized for decrypting the pixel point.

$$C_{11} = \mathrm{H} * C_1 \quad (10)$$

$$C_{ij} = C_2 - C_{11} \quad (11)$$

From the outcomes of C_{ij}, all pixels value of the image is retrieved and obtains back the original image (R,G,B) as individually. At last, the decrypted image is obtained as

$$F_{image} = R + G + B \quad (12)$$

B. Encryption of G components using DLCM

Based on the smart cryptosystem, encryption and decryption procedures are applied by using transformation procedure of encryption as well as decryption key. A desire of encryption is plaintext space, whereas the aim of decryption is ciphertext space. In case of cryptographic approach, plaintext space P equivalent to group of pixels of actual digital image which has to be encrypted, and ciphertext space C equivalent to collection of image pixels once the encryption is completed. A ciphertext space C attained by plaintext space P is forwarded in an indefinite module. The key K is defined as a key which performs encryption transform and decryption transform process. A similar key would be applied to diverse encryption and decryption keys on the basis of elected encryption approach [16]. In key space {K}, control implementation of encryption approach has been evaluated that has a space with essential data accomplished from plaintext and ciphertext space. It is executed using 2 chaotic maps, and it can be named as double chaotic digital image encryption mechanism, and alternate approaches are enclosed with encryption and decryption approaches as well as transmission module.

C. Encryption of B components using signcryption

Signcryption is defined as a public key cryptosystem that offers sufficient protection for confidential image under the production of electronic signature and encryption. The variables applied in Signcryption model are sender 'S', standard parameter 'cp', secret key of sender 'xs', public key of receiver 'yr' as well as sender and receiver's public key 'ys', 'yr' as 'binfo' are defined as inputs for Signcryption approach. The variable 'binfo' is significant to protect the Signcryption that is composed of strings used for finding transmitter and receiver's public keys hash values [14]. The working process involved in DLCM technique is shown in Figure 2.

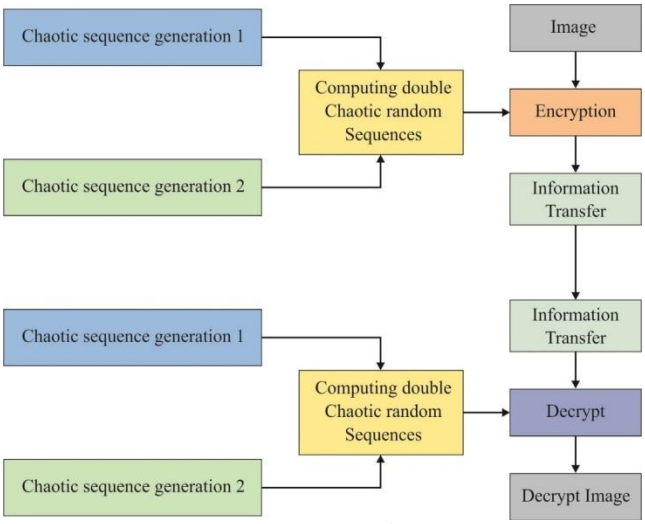

Figure 2: Working process of DLCM Model

3. PERFORMANCE VALIDATION

This section elaborates the results analysis of the presented models interms of different measures namely mean square error (MSE), peak signal to noise ratio (PSNR), structural similarity (SSIM) and normalized cross-correlation (NCC).

Table 1 offers the detailed analysis of the IWOA with WOA and GWO algorithms interms of MSE and PSNR. For effective performance, the value of MSE should be low and PSNR should be high.Figure3 examines the performance of the IWOA with existing methods interms of MSE under different frames. The figure stated that the IWOA has exhibited superior results by attaining minimum MSE under all the applied frames. At the same time, the GWO algorithm has obtained poor performance by achieving higher MSE value over the other methods. Though the WOA has seemed to be better than GWO algorithm, it has failed to outperform the IWOA and ended up with a moderate MSE value. For

instance, under the frame number 1, the IWOA has shown better performance with the lower MSE of 0.102 whereas the WOA and GWO algorithms have exhibited higher MSE of 0.247 and 0.534 respectively.

Table 1: Result Analysis of Existing with Proposed IWOA Model in terms of MSE and PSNR

Frame Number	MSE			PSNR		
	IWOA	WOA	GWO	IWOA	WOA	GWO
Frame 1	0.102	0.247	0.534	58.04	54.20	50.86
Frame 2	0.098	0.361	0.487	58.22	52.56	51.26
Frame 3	0.131	0.276	0.589	56.96	53.72	50.43
Frame 4	0.118	0.194	0.420	57.41	55.25	51.90
Frame 5	0.124	0.342	0.519	57.20	52.79	50.98
Frame 6	0.107	0.377	0.472	57.84	52.37	51.39
Frame 7	0.094	0.289	0.483	58.40	53.52	51.29
Frame 8	0.087	0.280	0.564	58.74	53.66	50.62
Frame 9	0.128	0.310	0.421	57.06	53.22	51.89
Frame 10	0.097	0.328	0.530	58.26	52.97	50.89

In line with this, under the frame value 2, the IWOA has showcased moderate function with the least MSE of 0.098 while the WOA and GWO methodologies have shown maximum MSE of 0.361 and 0.487 correspondingly. Followed by, under the frame value 3, the IWOA has illustrated moderate function with least MSE of 0.131 while the WOA and GWO technologies have represented greater MSE of 0.276 and 0.589 respectively. Meantime, under the frame number 4, the IWOA has demonstrated considerable function with the minimal MSE of 0.118 and the WOA and GWO algorithms have showcased high MSE of 0.194 and 0.420 correspondingly. In addition, under the frame value 5, the IWOA has depicted best function with lesser MSE of 0.124 and the WOA and GWO approaches have shown maximal MSE of 0.342 and 0.519 respectively. Additionally, under the frame value 6, the IWOA has illustrated reasonable performance with less MSE of 0.107 while the WOA and GWO techniques have represented better MSE of 0.377 and 0.472 correspondingly.

In line with this, under the frame value 7, the IWOA has depicted acceptable function with minimum MSE of 0.094 while the WOA and GWO schemes have showcased highest MSE of 0.289 and 0.483 correspondingly. Moreover, under the frame number 8, the IWOA illustrated gradual performance with the lesser MSE of 0.0.87 while the WOA and GWO technologies have depicted maximum MSE of 0.280 and 0.564 correspondingly. Meantime, under the frame number 9, the IWOA has demonstrated better function with the least MSE of 0.128 while the WOA and GWO methodologies have represented greater MSE of 0.310 and 0.421 respectively. In addition, under the frame value 10, the IWOA has exhibited best function with the low MSE of 0.097 and the WOA and GWO schemes have implied maximum MSE of 0.328 and 0.530 respectively.

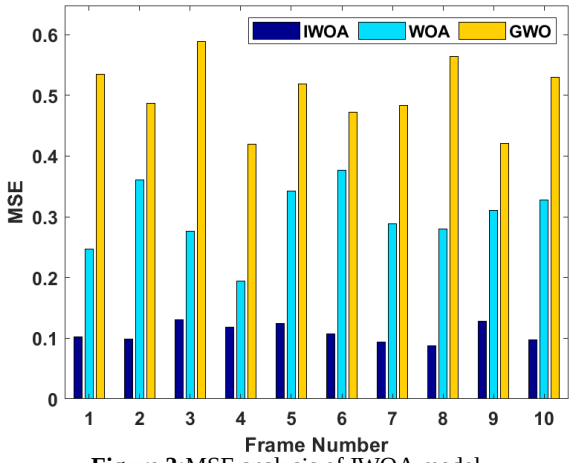

Figure 3:MSE analysis of IWOA model

Figure4 depicts the PSNR analysis of the IWOA with existing algorithms interms of PSNR. The experimental outcome stated that the IWOA has found to be effective by the accomplishment of maximum PSNR values under all the test frames applied. On looking into the figure, it is appeared that the WOA and GWO algorithms have demonstrated ineffective results by achieving lower PSNR values. For instance, under the frame number 1, the IWOA has exhibited its effectiveness by achieving higher PSNR of 58.04dB whereas the WOA and GWO algorithms have portrayed lower PSNR values of 54.20dB and 50.86dB respectively.Likewise, under the frame number 2, the IWOA has showed its efficiency by accomplishing better PSNR of 58.22dB while the WOA and GWO methods have exhibited lesser PSNR measures of 52.56dB and 51.26dB correspondingly.

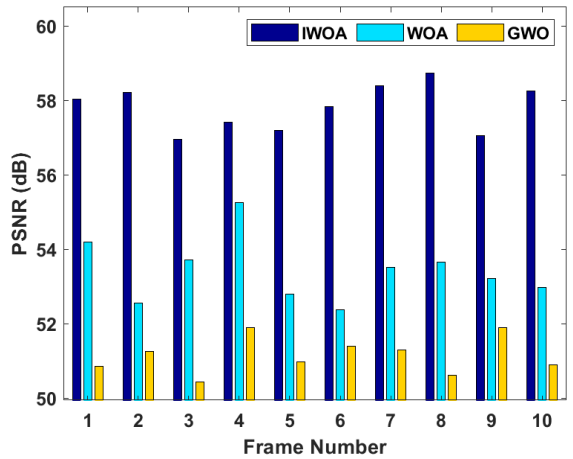

Figure 4:PSNR analysis of IWOA model

Then, under the frame number 3, the IWOA has portrayed the importance by attaining moderate PSNR of 56.96dB and the WOA and GWO technologies have showcased least PSNR measures of 53.72dB and 50.43dB respectively. Similarly, under the frame value 4, the IWOA has demonstrated its

significance by reaching best PSNR of 57.41dB and the WOA and GWO methods have demonstrated minimum PSNR values of 55.25dB and 51.90dB correspondingly. In addition, under the frame number 5, the IWOA has represented the efficacy by obtaining highest PSNR of 57.20dB and the WOA and GWO schemes have depicted minimal PSNR values of 52.79dB and 50.98dB correspondingly.

Figure5 illustrates the SSIM analysis of the IWOA with traditional model with respect to SSIM. The experimental outcome defined that the IWOA has found to be effective by the accomplishment of maximum SSIM values under all test frames used. From the figure, it is evident that the WOA and GWO technologies have depicted poor results by achieving lower SSIM values.

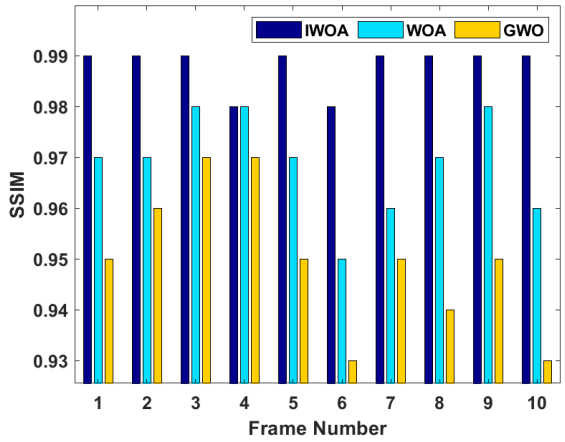

Figure5: SSIM analysis of IWOA model

For sample, under the frame number 1, the IWOA has represented the efficiency by reaching high SSIM of 0.99 while the WOA and GWO algorithms have exhibited low SSIM values of 0.97 and 0.95 respectively. Likewise, under the frame number 2, the IWOA has exhibited its effectiveness by accomplishing higher SSIM of 0.99 whereas the WOA and GWO algorithms have implied lower SSIM values of 0.97 and 0.96 respectively. Besides, under the frame number 3, the IWOA has exhibited its effectiveness by achieving higher SSIM of 0.99 whereas the WOA and GWO methodologies have depicted low SSIM values of 0.98 and 0.97 respectively. Likewise, under the frame number 4, the IWOA has represented its effectiveness by achieving higher SSIM of 0.98 whereas the WOA and GWO algorithms have exhibited lower SSIM values of 0.98 and 0.97 respectively. Moreover, under the frame number 5, the IWOA has displayed its effectiveness by achieving higher SSIM of 0.99 whereas the WOA and GWO algorithms have displayed less SSIM values of 0.97 and 0.95 respectively. Concurrently, under the frame number 6, the IWOA has exhibited its effectiveness by achieving maximum SSIM of 0.98 whereas the WOA and GWO algorithms have portrayed lower SSIM measures of 0.95 and 0.93 respectively. In addition, under the frame number 7, the IWOA has implied its effectiveness by achieving optimal SSIM of 0.99 whereas the WOA and GWO algorithms have portrayed lower SSIM values of 0.96 and 0.95 respectively. In addition, under the frame number 8, the IWOA has showcased the significance by reaching greater SSIM of 0.99 whereas the WOA and GWO algorithms have portrayed lower SSIM measures of 0.97 and 0.94 respectively.Along with that, under the frame number 9, the IWOA has illustrated its effectiveness by achieving higher SSIM of 0.99 whereas the WOA and GWO algorithms have implied less SSIM values of 0.98 and 0.95 respectively. Also, under the frame number 10, the IWOA has represented its importance by accomplishing maximum SSIM of 0.99 whereas the WOA and GWO algorithms have portrayed lower SSIM measures of 0.96 and 0.93 respectively.

4. CONCLUSION

This paper has proposed a new DVWE method using IWOA. The proposed model involves different processes namely frame extraction, optimal pixel selection, encryption, embedding and reconstruction. Once the videos are segregated and decomposed, optimal pixel selection process is done by IWOA. Followed by, the encryption of watermark video frames takes place using three encryption techniques. Afterwards, the encrypted part of secret video frame is again incorporated into effectively selected part of cover image. Finally, the stego frames are again merged to generate a watermarked video. At the receiving end, the reverse process takes place to retrieve the secret watermark video. A detailed experimentation process takes place to verify the effective outcome of the proposed model. The obtained results verified the goodness of the presented model under diverse aspects.

REFERENCES

1. Ahmed. A. A. Gad-Elrab, Shereen A. El-aal, Neveen I. Ghali and Afaf A. S. Zaghrout, A Dynamic Genetic-Based Context Modeling Approach in Internet of Things Environments, International Journal of Advanced Trends in Computer Science and Engineering, Volume 8 No. 6 (2019), pp. 2699 – 2709.
2. S. Mahalakshmi and Dr.R.Latha, Detection of single-trial EEG of the neural correlates of familiar faces recognition using machine-learning algorithms, International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE),Volume 8 No. 6 (2019), pp. 2855 – 2860.
3. M. Amini, M.O. Ahmad, M.N.S. Swamy, A new locally optimum watermark detection using vector-based hidden markov model in wavelet domain, Signal Process. 137 (2017) 213–222.
4. M. Hamidi, M.E. Haziti, H. Cherifi, M.E. Hassouni, Hybrid blind image watermarking technique based on DFT-DCT and Arnold transform, Multimedia Tools Appl. 77 (20) (2018) 27181–27214.
5. B.Y. Lei, Y. Soon, Z. Li, Blind and robust audio watermarking scheme based on SVD–DCT, Signal Process. 91 (8) (2011) 1973–1984.
6. A. Phadikar, S.P. Maity, B. Verma, Region based QIM digital watermarking scheme for image database in DCT domain, Comput. Electr. Eng. 37 (3) (2011) 339–355.

7. S. Saadi, A. Merrad, A. Benziane, Novel secured scheme for blind audio/speech norm-space watermarking by Arnold algorithm, Signal Process. 154 (2019) 74–86.
8. F. Golshan, K. Mohammadi, A hybrid intelligent SVD-based perceptual shaping of a digital image watermark in DCT and DWT domain, Imaging Sci. J 61 (1) (2013) 35–46.
9. S. Shivani, D. Singh, S. Agarwal, DCT based approach for tampered image detection and recovery using block wise fragile watermarking scheme, in: Iberian Conference on Pattern Recognition and Image Analysis, Lecture Notes in Computer Science, Springer, 2013, pp. 640–647.
10. N. Divecha, N.N. Jani, Implementation and performance analysis of DCT-DWT-SVD based watermarking algorithms for color images, in: International Conference on Intelligent Systems and Signal Processing, 1-2 March, IEEE, Gujarat, India, 2013, pp. 204–208.
11. A. Cedillo-Hernandez, M. Cedillo-Hernandez, M. Garcia-Vazquez, et al., Transcoding resilient video watermarking scheme based on spatio-temporal HVS and DCT, Signal Process. 97 (2014) 40–54.
12. M. Paunwala, S. Patnaik, Biometric template protection with DCT-based watermarking, Mach. Vis. Appl. 25 (1) (2014) 263–275.
13. H.T. Hu, L.Y. Hsu, H.H. Chou, Perceptual-based DWPT-DCT framework for selective blind audio watermarking, Signal Process. 105 (2014) 316–327.
14. Ambika, Biradar, R.L. and Burkpalli, V., 2019. Encryption-based steganography of images by multiobjective whale optimal pixel selection. International Journal of Computers and Applications, pp.1-10.
15. Shankar, K. and Eswaran, P., 2017. RGB based multiple share creation in visual cryptography with aid of elliptic curve cryptography. China Communications, 14(2), pp.118-130.
16. Pan, H., Lei, Y. and Jian, C., 2018. Research on digital image encryption algorithm based on double logistic chaotic map. EURASIP Journal on Image and Video Processing, 2018(1), p.142.