IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-11, Nov 2018 E-ISSN: 2347-2693

Hybrid Technique for Improving the Watermarking and Encryption Scheme for Online Multimedia Copyright Protection to using Chaotic Maps Cryptography

J. Udayakumar[1*], G. Prabakaran[2]

[1]Department of Computer Science & Engineering, FEAT, Annamalai University
[2]Department of Computer Science & Engineering, Annamalai University
[1,2]Annamalai Nagar, Tamilnadu, India

Available online at: www.ijcseonline.org

Accepted: 21/Nov/2018, Published:30/Nov/2018

***Abstract*—**Encryption and watermarking are two innovative techniques that are used for protecting the traditional multimedia files. In this research paper, a proposed hybrid encryption-watermarking algorithm for content copyright protection is proposed. The watermarking steps of this proposed algorithm is based on combining the three techniques like Discrete Wavelet Transform (DWT), the Discrete Cosine Transform (DCT), and the Singular Value Decomposition(SVD), while the encryption phase is based on using different chaotic maps with different dimensions to improve the performance of algorithms efficiency. The proposed watermarking scheme uses a new PN-codes for embedding strategy of the watermark into the cover image. This scheme allows to decreasing the embedding strength factor of the scheme to a value that maximizes imperceptibility performance, while maintaining acceptable robustness and imperceptibility measures of the watermarking scheme. The performance of the proposed watermarking scheme is implemented individually based on the metrics like robustness and the imperceptibility measures. This scheme is compared with some very recent existing algorithms and experimental results show the improvements of the proposed algorithm over other important algorithms. On the other hand, the proposed chaos-based encryption algorithms used different chaotic maps of different dimensions to improve the performance of algorithms efficiency. The proposed encryption algorithm is tested using different set of experiments. The experimental results demonstrate that the proposed encryption algorithm research shows advantages of large key space, high resistance against differential attacks and high security analysis such as (i)Statistical analysis, and (ii)Sensitivity analysis. Compared to some traditional and recent encryption algorithms, our proposed encryption algorithm is much more secure. Finally experimental test demonstrate that the proposed hybrid encryption-watermarking algorithm introduces high degree of efficiency, robustness, and security as compared to previously developed techniques/algorithms.

***Keywords*—** Chaotic maps, Encryption, Digital Watermarking, Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), Singular Value Decomposition (SVD).

I. INTRODUCTION

Fast development of Internet technology in recent years has improved the ways to distribute and exchange digital multimedia with less time, lower complexities and better efficiency than ever. Online and offline digital multimedia can be manipulated or reproduced easily without the loss of information by using powerful multimedia processing tools that are widely available. In particular, safe distribution and management of online multimedia content have become the real challenge. To satisfy these needs, several techniques have been developed, among them digital watermarking and encryption techniques. Digital watermarking and Encryption are two complementary techniques that are used for protecting the online and offline multimedia content.

Encryption provides a means for secure delivery of multimedia content to the consumer. The legitimate consumers are provided with a key to decrypt the content in order to view or listen to it. After the decryption phase, an untrustworthy consumer may alter or copy the decrypted content in a decent manner that is not permitted by the content owner; hence encrypted content need an additional security level in order to keep control on them. On the other hand, one may want to check the presence of a watermark without deciphering the data. Therefore, the challenging goal seems to be the achievement of both levels of protection simultaneously in order to allow jointly exploiting the benefits of the two mechanisms [1].

Digital watermarking schemes can be classified based on the watermarking domain into two categories: (i)Spatial domain and (ii)Transform domain watermarking schemes. In spatial domain watermarking schemes, the watermark is embedded by directly modifying the pixel values of the image [2-4]. In transform domain watermarking schemes, the transformation technique, such as the discrete cosine transform (DCT) [5-6], discrete wavelet transform (DWT) [7-9], and singular value decomposition (SVD) [10-11] is applied to an image and then the watermark is embedded by modifying the transform domain coefficients. Discrete Cosine Transform (DCT) is a technique for converting a signal into elementary frequency components [12]. It decomposes an image into (i) low frequency (LF), (ii) medium frequency (MF), and (iii) high frequency (HF) sub-bands as shown in Figure.1(a). It has a strong "energy compaction" property that most of the image energy tends to be concentrated in the low frequency sub-band of the transformed image. DWT provides multi resolution representation of an image and can be efficiently implemented using digital filters[13]. An image can be decomposed using 1-level DWT into four sub-bands: (i) low frequency sub-band (LL), (ii) horizontal sub-band (HL), (iii) vertical sub-band (LH), and (iv) diagonal sub-band (HH) as shown in Figure.1(b). The high frequency sub-bands HL, LH, and HH are good regions for embedding the watermark because human naked eyes are less sensitive to modification in these sub-bands than the LL sub-band [26-27]. SVD for any image 'A' of size N×N is a factorization of the form given by: , where U and V are orthogonal matrices and S is a diagonal matrix of singular values in decreasing order. The main properties of SVD are (i) A small agitation added in the image does not cause large variation in its singular values (SVs), and (ii) the singular values represent algebraic image properties which are intrinsic and not visible [14]. These transformation domain techniques show good robustness and security against various attacks as compared to spatial domain techniques. In the last few years, researchers start to combine between these techniques such as combining between SVD-DCT [15-16], DWT-SVD [17-18], DWT-DCT [19-20], and DWT-DCT-SVD [21] in order to improve the performance of watermarking process.

Traditional encryption algorithms such as Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), and Advanced Encryption Standard (AES) etc. are not suitable for real time multimedia encryption as these ciphers require a large computational time and high computing power. The chaos-based encryption has suggested new and efficient ways to deal with the intractable problem of fast and highly secure multimedia encryption. It provides a good combination of speed, high security, complexity, reasonable computational overheads and computational power. After Matthews proposed the chaotic encryption algorithm in 1989[22], increasing researches of image encryption technology are based on chaotic systems [23-25]. Chaotic systems have many important properties, such as the sensitive dependence on initial conditions and system parameters, pseudorandom property, non-periodicity and topological transitivity, etc. Most properties meet some additional requirements such as diffusion and mixing in the sense of cryptography [23]. Therefore, chaotic cryptosystems have more useful and practical applications. Chaos-based multimedia encryption schemes are usually composed of two processes generally: chaotic confusion of pixel positions by permutation process and diffusion of pixel grey values by diffusion process.

Encryption and watermarking can be combined in many different ways. Bas et al. [26] give an overview on the possible scenarios where the combination of both level of protection can be exploited, while Merhav [27] presents a theoretical analysis of this problem. The watermarking is suitable for copyright protection purposes where the invisible embedded watermarks carries some secret information that may be considered attributes of the cover host image in the multimedia such as copyright. To enhance the security of the user specific secret information in the networked multimedia system the watermark can be first encrypted using a secret key. The encrypted watermark is then embedded in the host video and transmitted to the intended user.

In this research paper, a hybrid DWT-DCT-SVD watermarking scheme combined with a chaos-based encryption algorithm is proposed for copyright protection. The multi resolution representation that DWT provided, the strong energy compaction property of DCT and the stability of SVs of an multimediaare combined in the proposed hybrid watermarking scheme to improve the scheme imperceptibility and robustness. The proposed hybrid watermarking scheme uses a new PN-codes embedding strategy of the watermark bits that highly improved the performance of the watermarking scheme. Each of PN-Codes was embedded into the singular values (SVs) of a sixteen elements that were chosen from the mid-frequency sub-band elements of a DCT block which also was selected from either the High-Low (HL) or Low-High (LH) sub-bands of DWT domain of the cover image depending on a shared secret Pseudorandom Noise (PN) code to increase the security level of the digital watermarking scheme. This code select between embedding the watermark bit into HL or LH block. The proposed hybrid encryption algorithm is based on combining four different dimensions chaotic maps (1D, 2D, 3D logistic map and 2D Henon map) to improve the algorithm security. An additional diffusion stage is used before the confusion stage to maximize the encryption speed, through minimizing the number of algorithm iterations. This diffusion stage contains a new shuffling function that shuffles the video frame bit panes depending on a round key which is sequentially updated for every pixel. This diffusion stage improves also the algorithm resistance against

differential attacks. The remainder of this research paper is organized as follows. Details and simulation results of the proposed hybrid watermarking scheme and are described in Section 2. In Section 3 Details and simulation results of the proposed hybrid encryption algorithm are introduced. In Section 4, the experimental results are presented to demonstrate the effectiveness of the proposed hybrid encryption-watermarking scheme. Conclusions are finally introduced in Section 5.

A. Video Watermarking

Today however, growing popularity of video based applications such as Internet multimedia, wireless videos, personal video recorders, video-on-demand, set-top box, videophone and video conferencing has increased the demand for a secure distribution of videos which is shown in Figure.3. Apparently any image watermarking technique can be extended to watermarking videos, but in reality video watermarking techniques need to meet other challenges than that in image watermarking schemes. Some of the video characteristics that impact watermarking include:

• High correlation between successive frames. If independent watermarks are embedded on each video frame, an attacker could perform frame averaging to remove significant portions of the embedded watermark.

• Some applications like broadcast monitoring require real time video processing and therefore should have low complexity.

• The unbalance between the motion and motionless regions.

• Watermarked video sequences are very much susceptible to pirate attacks such as frame averaging, frame swapping, statistical analysis and lossy compressions.

Figure 1: Shows the watermarking after and before

II. MOTIVATIONS AND PROPOSED FRAMEWORK

Although there have been tremendous research works on digtal watermarking for the copyrights protection still the practical and real-life applications do need much attention, specifically in the area of online privacy of digital data. For example, a public domain of video uploader, youtube.com, does not have the sophisticated framework for the protection of rightful ownership. Let say, for instance, Bob has uploaded his video and after some time (days), Alice has downloaded that video and uploaded it again by her name. At the time of uploading, Alice has been granted the permission of uploading that video which should not be the case. The management of that public domain eventually remove that video after some days, and if the name of the video uploaded by Alice is significantly different from the one given by Bob, then it can take even more time to look up for that video and eventually in removing the video. Similarly, other than videos, piracy of digital images face the same problem.

In this research work, it have proposed a unified framework for protecting the rightful ownership of digital data. The proposed framework is shown in Figure 1. It works as follows: let say a user wants to upload his/her data on a public domain. First, she/he requests that domain upload that data. The public domain upon receiving the request applies the proposed inverse watermarking function $\Delta-1$ to see if there is any watermark present in it or not. If there is any watermark present in that data, the domain will deny the upload request. Furthermore, the public domain will match the extracted watermark with the database. If the extracted watermark is matched with someone else watermark, the domain will notify the rightful owner of that data so that he or she can move with the legal case. In the case in which there is no watermark present in it, the domain will grant the permission of uploading that data and also will apply the proposed hybrid watermarking function Δ with the unique watermark associated with the user. In that way, let say, in future, if Alice tries to download and upload that data, not only will the permission be denied, but the domain will also notify to make a case against her legally.

III. REVIEW OF RELATED RESEARCH

Various types of digital watermarking techniques have been previously reported for images to provide robust and effective watermarking including authenticity, perceptibility and integrity. Some of such recent researches are briefly described in this section.

Lu Xu et al. 2016 [25], presented a algorithm for image encryption using piecewise linear chaotic maps which was deployed at bitlevel. After applying binary bitplane decomposition, diffusion and confusion strategy has been applied and hence successfully achieved good security with just single round.

Xiangyuan Wang et al. 2015[12], proposed color image encryption with various types of permutation among bits and correlated chaos which improves permutation efficiency and full use of chaotic maps and hence increased the security.

Xiangyuan Wang et al. 2015[13], proposed image encryption technique using the combinations of chaotic maps and random growth. It eliminate cyclical phenomenon and

generate the random streams which result into improve the security level.

Muhammad Rafiq Abuturab et al. 2015[14], suggested an individual channel color image encryption with hartley and graytor transform. The unsymmetric keys, random phase mask provides high robustness and changed angle of graytor transform offers as principal key which is highly sensitive.

Xing Yuan Wang et al. 2015[17], in their work proposed a technique which depend upon combination of DNA cryptosystem and chaotic system. Scrambling was done by using various operations like XOR operation on pixels, DNA encoding rules were responsible for creating more confusions and permutation. So in this way it provide more security.

Wang et al. 2015[23], presented an algorithm which depends upon cyclic shifts and chaotic system. The arbitrary integers taking the exact same size of the original image were made to do scrambling for cyclic shift operations, then keys are produced by chaotic system. İn this way it is superior and resist exhaustive attack.

Yicong Jhou et al.2014 [9], introduced a image encryption employing a bitplane of a plain image as the secret key bitplane to encode images. İt demonstrated an excellent performance of the encryption.

R Huang et al. 2014 [20], have proposed a method in which a block cipher framework consisted of scrambling, jumbling up S-box and chaotic lattice for encrypting the quantized measurement data. İt was not only achieved confusion, diffusion and sensitivity but also outperforms the existing parallel image encryption methods with respect to the compressibility and the encryption speed.

Zhang Ying-Qian et al. 2014 [12], presented an encryption technique using mixed linear-nonlinear coupled map lattices. İt permits the lower bit planes and the higher bitplanes of pixels permute interchangeably without any additional storage space. İt results into superior security and high efficiency.

IV. PARAMETERS OF MULTIMEDIA ENCRYPTION

Online multimedia encryption techniques are being compared upon 3 parameters which are as follows:

- Key space – It can be determined by calculating the total number of keys which are utilized in the encryption procedure. Greater the value, more will be the security level. İt is calculated as {n round X N0 (iteration times) X Computational precision}. Normally size of the key should be greater than 2100.
- Compressive sensing – It is a sampling technique which reduces the sampling rate at the exposure of a complex reconstruction on the recipient. So it enables us to work on compressed images.
- Speed–The speed of an algorithm is determined by two main factors known as computational cost and complexity of algorithm used. Computational cost checks the number of rounds during encryption and also consider how many permutation and diffusion operations occurred within a round. It is observed that many of the techniques are more inclined towards providing high security and ignoring the speed.

A. Problem Identification

So, in this research work, the problem in digital watermarking of online multimedia for protection of copyright and preventing online piracy is addressed. Multimedia watermarking schemes based on DCT and SVD are developed for improving the performance of watermarking schemes in terms of robustness, imperceptibility, payload and security. The need for unique watermark for digital watermarking is also addressed. Further, module for unique watermark generation using the auditory features extracted from the speech of any individual is developed.

B. Watermarking in MPEG-4

There is a need for real-time copyright logo insertion in emerging applications, such as Online Video content. This is demonstrated in Figure.4. The visible transparent watermarking unit accepts broadcast uncompressed video and the broadcaster's logo. The output is real-time compressed video with the logo embedded. Embedded systems that are involved in broadcasting need to have embedded copyright protection. Existing works are targeted towards invisible watermarking, not useful for logo insertion. The main steps for MPEG-4 are color space conversion and sampling, DCT and its inverse (IDCT), quantization, zigzag scanning, motion estimation, and entropy coding. A simpler approach is a single watermarking step in the compression framework because the computation requirements of watermarking are comparable to these steps.

The sampling rate is chosen to be 4:2:0 so that in a 4 pixel group, there are four Y pixels, a single Cb pixel and a single Cr pixel to meet digital online multimedia broadcasting standards.

C. DCT OR IDCT

DCT is one of the computationally intensive phases of video compression. The two dimensional DCT and IDCT algorithms can be implemented by executing the one dimensional algorithms sequentially, once horizontally (row wise) and once vertically (column-wise).

D. Quantization

After the DCT, the correlation of pixels of an image or video frame in the spatial domain has been de-correlated into discrete frequencies in the frequency domain. Since human visual system (HVS) perception is more acute to the DC coefficient and low frequencies, a carefully designed scalar quantization approach reduces data redundancy while maintaining good image quality. In the MPEG-4 video compression standard, a uniform scalar quantization is adopted. The feature of the scalar quantization scheme is an adaptive quantized step size according to the DCT coefficients of each macro block. For computational efficiency the scalar quantization step size can be chosen from predefined tables.

E. ZIGZAG SCANNING

Zigzag scanning sorts the matrix of DCT coefficients in ascending order. For progressive frames and interlaced fields, zigzag scanning routes are provided by predefined Tables.

F. Motion Estimation

Prior to performing motion estimation, an image (video frame) is split into smaller pixel groups, called macroblocks, as the basic elements of the video frame rather than a single pixel. This is driven by a compromise between efficiency and performance to analyze a video's temporal model. A macroblock commonly has a size of 16×16 pixels. With the macroblock in the base frame and its two dimensional motion vector, the current frame can be predicted from the previous frame. In the MPEG-4 standard, the region in which the macroblock is bought for match could be a square, diamond, or of arbitrary shape. For most applications, a square region is considered. For example, if the macroblock has pixel size, the searching region will be a pixel block. The similarity metric for two blocks is the minimized distance

COLOR SPACE CONVERSION The conversion from RGB colorspace to YcbCr colorspace is performed using the following expression:

$$Y = 0.299R + 0.587G + 0.114B$$
$$Cb = 0.564(B - Y)$$
$$Cr = 0.713(R - Y)$$

between them. For simplicity, the sum of the absolute difference (SAD) is applied as the criterion for matching. where c(i, j) are the pixels of the current block, i, j=0,1, . . ., N−1; p(m, n) are the pixels of the previous block in the searching region, and m, n =−R, −R+1, . . ., 0,1, . . ., R +N−1, where the size of the macroblock is R pixels. Motion estimation is in the critical path of video compression coding and most time delay will occur at this step. The SAD algorithm will search the square target region exhaustively to find a matching macroblock. The output of this procedure is the prediction error for motion compensation and the motion vector.

G. **Entropy Coding**

After DCT and quantization compression, additional compression can be achieved via entropy coding, which includes Huffman coding, Arithmetic coding, etc. Unlike lossy compression, as in the color space, DCT and quantization procedures, the entropy coding compression is lossless. The entropy coding efficiency depends on the precision of calculating the probability of occurrence of each coefficient. However, calculating probabilities of all the coefficients is impossible in real-time MPEG-4 coding and watermarking. The approach we followed is to utilize pre-calculated Huffman code.

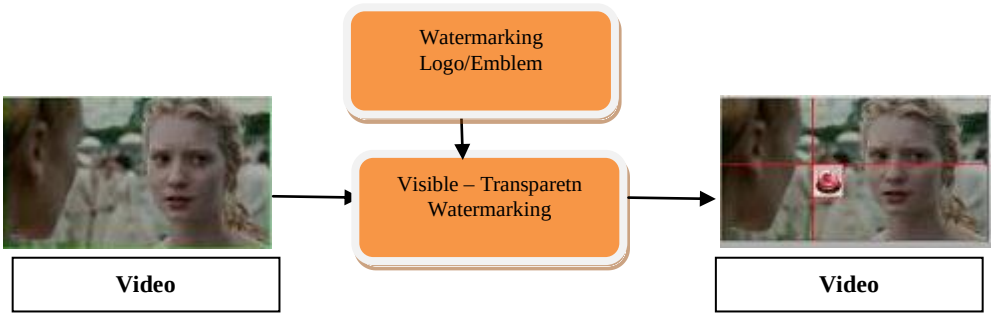


Fig 2. Real-time logo insertion through watermarking

V. THE PROPOSED WATERMARKING ALGORITHM

• Convert RGB color frames to YCbCr frames for the input video.
• Resample YCbCr frames according to 4:2:0 sampling rate.
• Split Y frame and watermark image into 8 x 8 blocks.
• Perform DCT for each 8 x 8 block to generate DCT coefficients.
• Perform perceptual analysis of the host video frame.
• Compute scaling and embedding factor for different blocks.
• Each block of Y DCT matrix is watermarked with an 8 x 8 watermark DCT matrix at same location as at DCT domain.
• Perform 2-D IDCT for each 8 x 8 watermarked matrix to transform it back to Y color pixels.
• Buffer watermarked Y component, non watermark Cb and Cr frames which holds a GOP.
• Split Y component into 16 x 16 blocks and Cb and Cr into 8 x 8.
• Perform motion estimation for Y component.
• Obtain the motion vectors (MV) and prediction errors of residual frame for motion compensation (MC) for Y component.
• Obtain motion vector and prediction error for Cb , Cr components and residual frame for motion compensation.
• Perform 2-D DCT on blocks of different frames.
• Quantize 2-D DCT coefficient matrix.
• Zigzag scan quantized 2-D DCT coefficient matrix.
• Entropy coding re-ordered 2-D DCT coefficient matrix and motion vector.
• Build structured compressed stream from the buffer. The robustness of DCT watermarking arises from the fact that if an attack tries to remove watermarking at mid frequencies, it will risk degrading the fidelity of the video frame because some perceptive details are at mid frequencies. The other important issue of visible watermarking, transparency comes from making the watermark adaptive to the host frame. The proposed hybrid watermarking algorithm is presented as a flow chart in Figure 5. For gray scale, the watermark is applied to Y frames. For a color watermark image, the Cb and Cr color space are watermarked using the same techniques for Y frames. To protect against frame interpolating attacks on watermarking, all I, B, P frames must embed the watermark. The watermark embedding approach used is formulated as: $Cw(i,j)= \alpha n\ C(i, j) + \beta nW(i,j)$ where Cw(i,j) is a DCT coefficient after watermark embedding, αn is the scaling factor and ,βn is the watermark strength factor, C(i,j) is the original DCT coefficient, and W(i,j) is the watermark DCT coefficient. The relative values of αn and βn determine the strength of the watermark. Their values are computed based on characteristics of the host video frame. Given that human perception is sensitive to image edge distortion, for edge blocks the value of αn should be close to its maximum value αmax while the value of, βn should be close to its minimum value, βmin. The user inputs that serve as quality control parameters are αmax, αmin, βmin, and , βmax. Since the watermark DCT coefficients will be added to the video frame DCT coefficients, it will be advantageous to adjust the strength of the watermark such that the distortion of these coefficients is minimal.

A.Testing of Watermarking Quality

Here it is performed exhaustive simulations to make assessment of watermarking quality with a large variety of watermark images and video clips. Standard video quality metrics mean square error (MSE) and Peak-Signal-to-Noise Ratio(PSNR) are applied to quantify the system's performance. Where p(m,n,k) and q(m,n,k) are the pixels after and before processing, respectively. It may be noted that the low PSNR did not degrade the perceptual quality of the video, as the low value is due to the fact that the watermark logo inserted is visible and consequently becomes noise for the host video and affects the PSNR.

VI. EXPERIMENTAL RESULTS & ANALYSIS

The proposed work is done in MATLAB Tool. The visible and invisible watermarking is done in DCT domain. Here its take different video clips and it is perform the PSNR values. These values are better when compared to previous works.

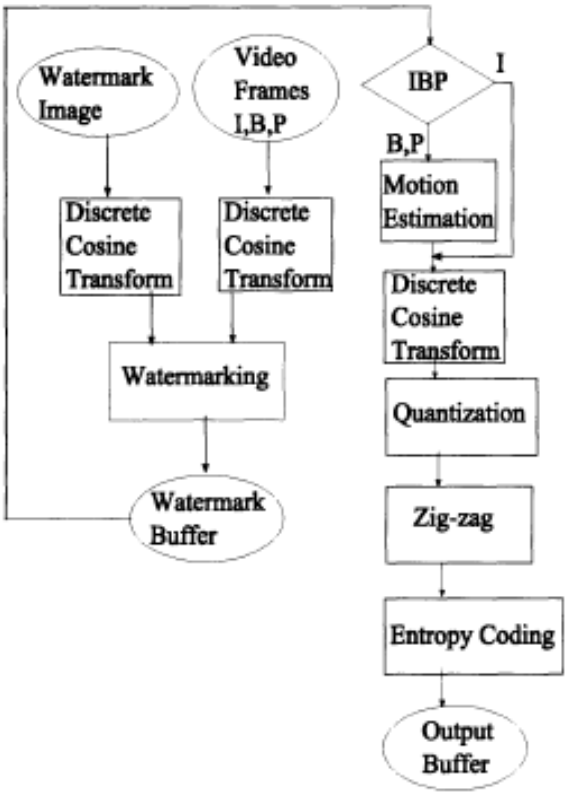


Fig 3. The flow of the proposed video watermarking algorithm

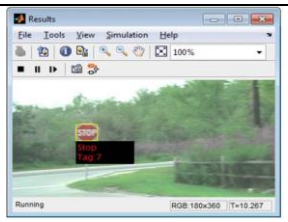
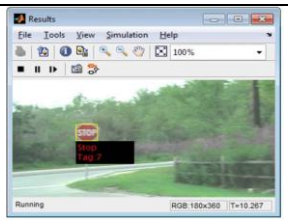
Table 1: Video Quality Metrics for Visible Watermark				
Clips	Watermarking	Video	Domain	PSNR(DB)
MATLAB Video	Visible		DCT	53.2441
Wild Life Movie	Visible		DCT	61.5548
Video Editor Vedio	Visible		DCT	59.5845
Jargon: Video Editing	Visible		DCT	37.5458
VCD Cutter Video	Visible		DCT	79.2321

Table 2: Video Quality Metrics for Invisible Watermark.

Clips	Watermarking		Domain	PSNR(DB)
MATLAB Video	Invisible		DCT	63.2546
Wild Life Movie	Invisible		DCT	75.8654

Video Editor Vedio	Invisible		DCT	68.8588
Jargon: Video Editing	Invisible		DCT	71.2525
VCD Cutter Video	Invisible		DCT	85.2564

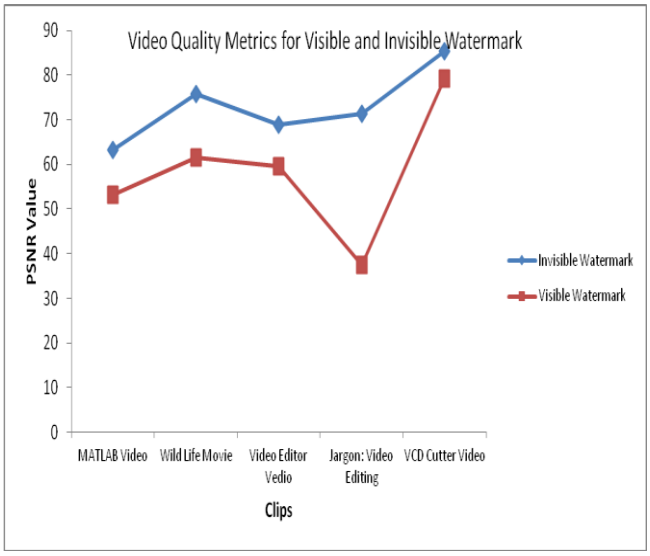


Figure 4. Video Quality Metrics for Visible and Invisible Watermark

Tables I & II gives the PSNR values for visible and Invisible watermarking. Figure.4 is the watermark image which is going to be embedded in to the original number series video.

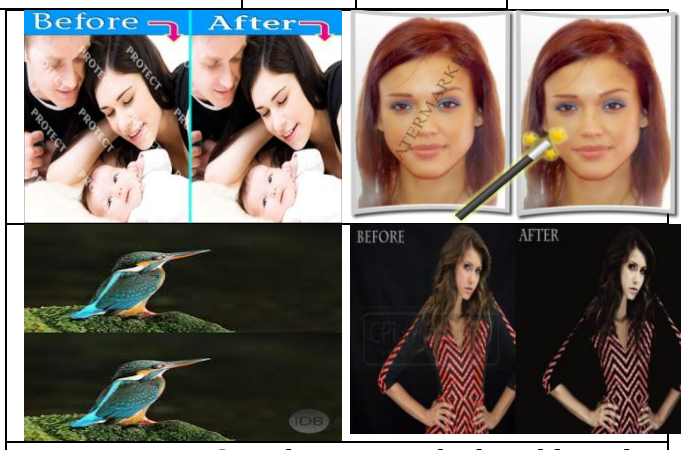


Fig 5.Sample watermarked visible and invisible videos using watermark

We performed exhaustive simulations to make assessment of watermarking quality with a large variety of digital watermark images and video clips. For brevity we present selected examples of watermarked video in Figure. 7.

VII. CONCLUSION

Here it have developed a unified watermarking algorithm using three different and distinct chaotic maps in which hybrided one map is proposed in this work. The embedding of the watermark is operated by the individual chaotic sequence generated by a different chaotic map. The simulation results and security analysis confirmed that the proposed algorithm is secure against well-known attacks. Like all new proposals, here it is strongly encourage the analysis of our framework before its immediate deployment. The proposed hybrid algorithm is a generalized watermarking model that can incorporate changes as

required. For instance, the number of substitution boxes (S-Box)can be increased for better security, but at the expense of more computational complexity. Furthermore, the work can be extended for the application of steganography as well in which instead of the watermark, the secret message can be inserted for information hiding.

REFERENCE

[1] Dongyan Wang, Fanfan Yang, and Heng Zhang, "Blind Color Image Watermarking Based on DWT and LU Decomposition ," Journal of Information Processing Systems, vol. 12, no. 4, pp. 765~778, 2016.

[2] Y.-M. Chu, N.-F.Huang, and S.-H. Lin, "Quality of service provision in cloud-based storage system for multimedia delivery," IEEE Systems Journal, vol. 8, no. 1, pp. 292–303, 2014.

[3] I. Hussain, T. Shah, M. A. Gondal, and H. Mahmood, "An efficient approach for the construction of LFT S-boxes using chaotic logistic map," Nonlinear Dynamics, vol. 71, no. 1-2, pp. 133–140, 2013.

[4] I. Hussain, A. Anees, M. Aslam, R. Ahmed, and N. Siddiqui, "A noise resistant symmetric key cryptosystem based on S-Boxes and chaotic maps," The European Physical Journal Plus, vol. 133, no. 4, 2018.

[5] I. Hussain, A. Anees, A. H. AlKhaldi, A. Algarni, and M. Aslam, "Construction of chaotic quantum magnets and matrix Lorenz systems S-boxes and their applications," Chinese Journal of Physics, 2018.

[6] I. Hussain, A. Anees, and A. Algarni, "A novel algorithm for thermal image encryption," Journal of integrative neuroscience, pp. 1–15, 2018.

[7] A. Anees, A.M. Siddiqui, and F. Ahmed, "Chaotic substitution for highly autocorrelated data in encryption algorithm," Communications in Nonlinear Science andNumerical Simulation, vol. 19, no. 9, pp. 3106–3118, 2014.

[8] T. T. Mapoka, S. J. Shepherd, and R. A. Abd-Alhameed, "A new multiple service key management scheme for secure wireless mobile multicast," IEEE Transactions onMobile Computing, vol. 14, no. 8, pp. 1545–1559, 2015.

[9] A. Anees, W. A. Khan, M. A. Gondal, and I. Hussain, "Application of mean of absolute deviation method for the selection of best nonlinear component based on video encryption,"Zeitschrift fur Naturforschung - Section A Journal of Physical Sciences, vol. 68, no. 6-7, pp. 479–482, 2013.

[10] H. Liu and X. Wang, "Color image encryption based on onetime keys and robust chaotic maps," Computers & Mathematics with Applications. An International Journal, vol. 59, no. 10, pp. 3320–3327, 2010.

[11] A. Anees and Z. Ahmed, "A Technique for Designing Substitution Box Based on Van der Pol Oscillator," Wireless Personal Communications, vol. 82, no. 3, pp. 1497–1503, 2015.

[12] J. Daemen and V. Rijmen, The Design of Rijndael: AES-The Advanced Encryption Standard, Springer, Berlin, Germany, 2002.

[13] A. Anees andM. A. Gondal, "Construction of Nonlinear Component for Block Cipher Based on One-Dimensional Chaotic Map," 3D Research, vol. 6, no. 2, 2015.

[14] A. Anees and A. M. Siddiqui, "A technique for digital watermarking in combined spatial and transform domains using chaotic maps," in Proceedings of the 2013 2nd National Conference on Information Assurance, NCIA 2013, pp. 119–124, pak, December 2013.

[15] S. S. Jamal, M. U. Khan, and T. Shah, "A Watermarking Technique with Chaotic Fractional S-Box Transformation," Wireless Personal Communications, vol. 90, no. 4, pp. 2033–2049, 2016.

[16] S. S. Jamal, T. Shah, and I. Hussain, "An efficient scheme for digital watermarking using chaotic map," Nonlinear Dynamics, vol. 73, no. 3, pp. 1469–1474, 2013.

[17] X. Wang and D. Chen, "A parallel encryption algorithm based on piecewise linear chaotic map," Mathematical Problems in Engineering, vol. 2013, 2013.

[18] A. Anees, A. M. Siddiqui, J. Ahmed, and I. Hussain, "A technique for digital steganography using chaotic maps," Nonlinear Dynamics, vol. 75, no. 4, pp. 807–816, 2014.

[19] F. Ahmed, A. Anees, V. U. Abbas, and M. Y. Siyal, "A noisy channel tolerant image encryption scheme," Wireless Personal Communications, vol. 77, no. 4, pp. 2771–2791, 2014.

[20] F. Ahmed and A. Anees, "Hash-Based Authentication of Digital Images in Noisy Channels," Robust Image Authentication in the Presence of Noise, pp. 1–42, 2015.

[21] Wang XY, Zhang HL. A color image encryption with heterogeneous bit- permutation and correlated chaos. Opt Commun2015; 342:51–60.

[22] Wang XY, Liu LT, Zhang YQ. A novel chaotic block image encryption algorithm based on dynamic random growth technique. Opt Lasers Eng 2015; 66:10–8.

[23] Abuturab MR. an asymmetric single-channel color image encryption based on Hartley transform and gyrator transform. Opt Lasers Eng 2015; 69:49–57.

[24] Xu, Lu, et al. "A novel bit-level image encryption algorithm based on chaotic maps." Optics and Lasers in Engineering 78 (2016): 17-25.

[25] Zhang YQ, Wang XY. Asymmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice.InfSci2014; 273(20):329–51.

[26] Zhenjun Tang, JuanSong, Xianquan Zhang, Ronghai Sun, "Multiple-image encryption with bit-plane decomposition and chaotic maps", Optics and Lasers in Engineering, Volume 80, May 2016

[27] Benyamin Norouzi, Sattar Mirzakuchaki, "Breaking an Image Encryption Algorithm based on the New Substitution Stage with Chaotic Functions", Optik - International Journal for Light and Electron Optics 127(14), Volume 127, Issue 14, July 2016

[28] Adrian-Viorel Dianconu, "Circular inter-intra bit-level permutation and chaos-based image encryption", Information Sciences, Volumes 355–356, Elsevier, August 2016

[29] XiaoweiLi, ChengqingLi, In-Kwon Lee, "Chaotic image encryption using pseudo-random masks and pixel mapping", European Association for Signal Processing, Volume 125, Elsevier, August 2016

[30] Wenhao Liu, Kehui Sun, Congxu Zhu, "A fast image encryption algorithm based on chaotic map", Elsevier, 2016

[31] Akram Belazi, Ahmed A. Abd El-Latif, Safya Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos", European Association for Signal Processing, Elsevier, 2016

[32] Khadijeh Mirzaei Talarposhti, Mehrzad Khaki Jamei, "A secure image encryption method based on dynamic harmony search (DHS) combined with chaotic map", Optics and Lasers in Engineering, Volume 81, Elsevier, 2016.

