Asian Journal of Computer Science and Technology
ISSN: 2249-0701 (P) Vol.7 No.S1, 2018, pp.73-77
© The Research Publication, www.trp.org.in
DOI: https://doi.org/10.51983/ajcst-2018.7.S1.1801

Video Watermarking and Encryption Scheme for Online Multimedia Copyright Protection to Using Chaotic Maps Cryptography

J. Udayakumar[1], G. Prabakaran[2] and R. Madhan Mohan[3]
[1]Research Scholar, [2&3]Assistant Professor,
[1,2&3]Department of Computer Science & Engineering, FEAT, Annamalai University, Tamil Nadu, India
E-Mail: uday.ja@gmail.com, gpaucse@yahoo.com, madhanmohan_mithu@yahoo.com

(Received 28 September 2018; Revised 10 October 2018; Accepted 27 October 2018; Available online 4 November 2018)

Abstract - **Nowadays, there is an explosive growth in the digital multimedia creation, capturing, processing and distribution. Protecting the multimedia contents from copyright in fingerprint has become a major concern. Encryption and watermarking are two complementary techniques that are used for protecting the multimedia data. In this paper, a proposed hybrid encryption-watermarking algorithm for copyright protection is proposed. The watermarking phase of this proposed algorithm is based on, the discrete cosine transform (DCT), while the encryption phase is based on using four chaotic maps with different dimensions. The proposed watermarking scheme uses a new PN-codes embedding strategy of the watermark into the cover image. This strategy allows decreasing the embedding strength factor of the scheme to a value that maximizes imperceptibility performance while maintaining acceptable robustness of the watermarking scheme. On the other hand, the proposed chaos-based encryption algorithm used four chaotic maps of different dimensions and it has two diffusion stages rather than one to improve the algorithm efficiency. The proposed encryption algorithm is tested using different experiments. The experimental results demonstrate that the proposed encryption algorithm shows advantages of large key space, high resistance against differential attacks and high security analysis such as statistical analysis, and sensitivity analysis.**

Keywords: **Chaotic Maps, Encryption, Digital Watermarking, Discrete Cosine Transform (DCT)**

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].

II. LITERATURE REVIEW

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 water marking 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.

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), an (iv) diagonal subband (HH). The high frequency subands 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. 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.,

1. A small agitation added in the image does not cause large variation in its singular values
2. 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] ignored 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 [23-24]. 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. 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 multimedia are 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 Pseudo random 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 around 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 video watermarking scheme and are described in Section 3. In Section 4 deals with experimental results and analysis. Further these videos are tested with watermarking. Conclusion is finally introduced in Section 5.

III. PROPOSED FRAMEWORK

Although, there have been tremendous research works on digital 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 up loader, youtube.com, does not have the sophisticated framework for the protection of rightful ownership. It has proposed a unified framework for protecting the rightful ownership of digital data. Parameters of Multimedia Encryption. Online multimedia encryption techniques are being compared upon 3 parameters which an area follows:

1. *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.

2. *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.

3. *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

The problem in digital watermarking of online multimedia for protection of copy right and preventing online piracy is addressed. Multimedia watermarking schemes based on DCT is 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.

C. DCT

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 a cute 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. Zig-Zag Scanning

Zig-zag 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 macro blocks, 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 macro block commonly has a size of 16×16 pixels. With the macro block in the base frame and its two dimensional motion vector, the current frame can be predicted from the previous frame. In MPEG-4 standard, the region in which the macro block 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 macro block 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 color space to YcbCr color space is performed using the following expression: 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,

$i,j = 0,1,\dots,N-1,$

Where p(m,n) are the pixels of the previous block in the searching region.

$m,n = -R,-R+1,\dots,0,1,\dots,R+N-1,$

Where the size of the macro block 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 macro block. 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.

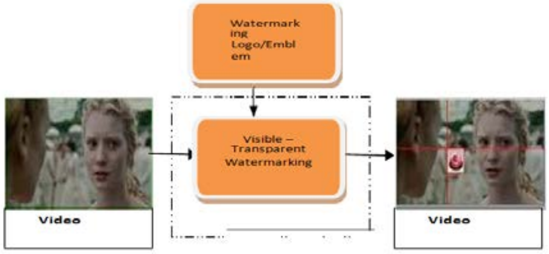

Fig. 1 Real-Time Logo Insertion through Watermarking

H. Proposed Watermarking Algorithm

Step 1: Convert RGB color frames to YCbCr frames for the input video.
Step 2: Resample YCbCr frames according to 4:2:0 sampling rate.
Step 3: Divide Y frame and watermark image into 8 x

8blocks.

Step 4: Achieve DCT for each 8 x 8 block to generate DCT coefficients.

Step 5: Carry out perceptual analysis of the host video frame.

Step 6: Calculate scaling and embedding factor for different blocks.

Step 7: Each block of Y DCT matrix is watermarked with an 8 x 8 watermark DCT matrix at same location as at DCT domain.

Step 8: Make 2-D IDCT for each 8 x 8 watermarked matrix to transform it back to Y color pixels.

Step9: Buffer watermarked Y component, non-watermark Cb and Cr frames which holds a GOP.

Step 10: Split Y component into 16 x 16 blocks and Cb and Cr into 8 x8.

Step 11: Perform motion estimation for Y component.

Step 12:Obtain the motion vectors (MV) and prediction errors of residual frame for motion compensation (MC) for Y component.

Step 13: Attain motion vector and prediction error for Cb, Cr components and residual frame for motion compensation

Step 14:Achieve 2-D DCT on blocks of different frames.

Step 15: Quantize 2-D DCT coefficient matrix.

Step 16: Zigzag scan quantized 2-D DCT coefficient matrix.

Step 17: Entropy coding re-ordered 2-D DCT coefficient matrix and motion vector.

Step 18: 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 Fig.2. 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.

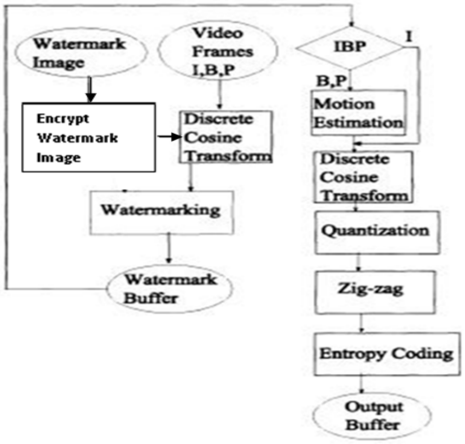

Fig. 2 Proposed Video Watermarking Algorithm

To protect against frame interpolating attacks on watermarking, all I, B, P frames must embed the watermark. The watermark embedding approach used is formulated in Equation 1:

$$C_w(i,j)= \alpha_n C(i, j) + \beta_n W(i,j) \qquad (1)$$

where $C_w(i,j)$ is a DCT coefficient after watermark embedding, α_n is the scaling factor and ,β_n 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 α_n and βn determined 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 α_{max} while the value of, βn should be close to its minimum value, β_{min}.

The user inputs that serve as quality control parameters are αmax, αmin, βmin,and β_{max}. 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.

TABLE I VIDEO QUALITY METRICS FOR DCT BASED VISIBLE WATERMARK

Clips	Water marking	Video	PSNR (dB)
Wild Life Movie	Visible		61.5548
Video Editor Video	Visible		59.5845
Jargon: Video Editing	Visible		37.5458
VCD Cutter Video	Visible		79.2321
MATLAB Video	Visible		64.6020

IV. 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 performing the PSNR values. These values are better when compared to previous works. Tables 1 show that the PSNR values for visible and invisible watermarking. The watermark image is going to be embedded in to the original number series video. We performed exhaustive simulations to make assessment of watermarking quality with a large variety of digital watermark images and video clips.

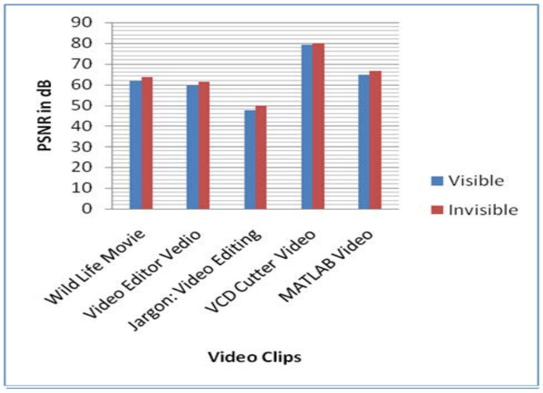

Fig. 3 Video Clips Vs PSNR in dB

A. Testing of Watermarking Quality

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.

V. CONCLUSION

The proposed method developed a unified watermarking algorithm using three different and distinct chaotic maps in which hybrid 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 encouraging 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.

REFERENCES

[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] 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] 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] 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] Anees, A.M. Siddiqui, and F. Ahmed, “Chaotic substitution for highly auto correlated data in encryption algorithm”, *Communications in Nonlinear Science and Numerical 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 on Mobile Computing*, Vol. 14, No. 8, pp. 1545–1559, 2015.

[9] 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”, *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. Aneesand, and Z. Ahmed, “A Technique for Designing Substitution Box Based on Vander 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] Anees and M.A. Gondal, “Construction of Nonlinear Component for Block Cipher Based on One-Dimensional Chaotic Map”, *3D Research*, Vol. 6, No. 2, 2015.

[14] A. Aneesand 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, NCIA2013*, 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] X.Y. Wang, and H.L. Zhang, “A color image encryption with heterogeneous bit- permutation and correlated chaos”, *Opt. Communication* Vol. 342, pp. 51–60, 2015

[22] X.Y. Wang, L.T. Liu, Y.Q. Zhang, “A novel chaotic block image encryption algorithm based on dynamic random growth technique”. *Opt. Lasers Eng* Vol. 66, pp. 10–8, 2015

[23] MR. Abuturab, “An asymmetric single-channel color image encryption based on Hartley transform and gyrator transform”. *Opt. Lasers Eng* Vol. 69, pp.49–57, 2015

[24] Xu, Lu, *et al*, “A novel bit-level image encryption algorithm based on chaotic maps”, *Optics and Lasers in Engineering* Vol. 78 pp.17-25, 2016.