Chaotic in image and video protection

Huda Khurshed Shawkat Aljader

Sarah Ali Abdulkareem

University of Diyala

Abstract

With the vast development of network and communication protecting digital data like images and videos became a must to protect the sensitive information from exploiters and vandals. Data encryption and its security is playing a prim role for individuals and industries in securing data transformation and transportation. Therefore, true random numbers (TRN) are used to provide unpredictability and robustness to the encrypted data which is proved to be better and stronger than Pseudorandom numbers (PRN). Chaotic features provide high randomness, sensitivity to initial conditions and periodicity. this paper intends to provide a review firstly, on image protection copyrights by watermarking using the (TRN)s generated by different chaotic techniques. Secondly, on video encryption using the latest chaotic techniques which proved to provide a higher protection in the field of video encryption. Finally, we derived our own conclusion of using true random generation in encryption with chaos.

Introduction

Generation a random number series is a fundamental point at cyber security issues. After the massive development of internet use, the necessity for protecting information is highly increased which raised the need for robust security systems [1,2]. Therefore, the encryption system must include powerful algorithms and unpredictable key generation, which are an essential factor in the field of information security [3,4]. Random number (RN) is a vital factor in the field of cryptography algorithms, statistics and simulation [5] where generating these numbers used in image encryptions and as a parameters of public key crypto systems (as in ECC, RSA) [6-8].

As known random numbers can be divided in to two categories the True random numbers (TRN's) and Pseudo random numbers (PRN's) [9]. However, TRN is primary and intrinsic in cryptography it is used in many fields (mathematical, stochastic, quantum) [10] where it could be generated by physical processes providing a non-repeatable TRN series which can be used in high security required systems [11]. In parallel with the TRN's, the pseudo random number generation (PRNG) played its significant role for the cryptography system to be robust for significant attacks. It was developed and defined as an algorithm with a main advantage of rapidity and repeatability process in producing a series of (RN's) which is vital in stream Entropy cryptography. Besides, the implementation of PRNG in personal computers and imbedded systems [12-14].

Recently, many researches used chaotic maps for watermarking in image, audio and video protection [15-17]. duo to the sensitivity digital information which multimedia have, the characteristics of chaos, such as non-periodicity, wide spectrum, unpredictability, and sensitivity to initial conditions are good agreement with the properties of random numbers [18]. Various simple and complex chaotic systems are applied to watermarking. 3-D Logistic maps [19] was used to generate random sequence while one- to- one mapping [20,21], and Arnold cat map [22] was used to permutation. Duo to the satisfactory results that chaotic system performed in generating series of random numbers providing, more complex hyper chaotic systems is used in digital watermarking to provide a higher level of media protection [23]. Watermarking is used mostly in image for copywrite protection [24].

In this paper we are going to review the latest chaotic methods that is used in security researches and the results that the came on. According to the importance of the chaotic and the success that chaotic method added to the random number generation field in the last decade. Section one proposed the latest researches in some of watermarking techniques in the last few years in digital image protection. Section two proposed researches and its results in the field of digital video protection.

1- image protection by watermarking using chaotic

The massive increment in data over network and media in the past decade raised the need for strong secured methods to protect the transferring and storing from possible attacks. Various schemed was proposed to reach the highest possible secured modules. As copywrites is one of the protection technologies, the algorithm divided into many domains and in this paper is proposing some of the domains that have been studied widely recently.

1-1 Special domain

This domain is one of the methods that is used to imbedded watermarking to protect the copywrite digital-colored images. This domain needs to use algorithms that provide high robustness, good imperceptibility and short execution time. In 2022[25] proposed a combination of spatial domain with singular value decomposition (SVD) by a blind image watermarking algorithm. The watermarking information embedded directly to the maximum singular value (MSV) of the host in the spatial domain.

In [26] a novel color image watermarking technique utilized in spatial domain providing a new robust, rapid and efficient protection. The technique used the direct current (DC) coefficient of 2D-DFT and the change Fourier transformation in each pixel in the spatial domain. The experiment produced a stronger method and lower running time than the frequency domain after the excluding of the true 2D-DFT. Arnold transform and hash pseudorandom scrambling algorithm is also used. The watermarking method which is used in this paper belongs to blind watermarking method.

1-2   Discrete Cosine Transformation (DCT):

DCT is known as mathematical transformation which is used in watermarking and frequency domain. DCT is developed to enhanced the security of the watermarking and the imperceptibility which led to produce a high computed complexity in schemes and enhanced robustness. [27] proposed (2D-DCT) which is obtained with multiple AC coefficients and one DC coefficient and dividing these bands ecoefficiencies in to (high, media, low) frequencies. This technique

considered as a new fast and robust image watermarking scheme beside it is simple with low complexity.

Another technique provided robust solution for copywrite and ownership issues proposed in [28] where a semi- blind color watermarking scheme introduced depending on DWT, FRT, SVD, PSO and Arnold transformation. Furthermore, the false positive problem (FPP) is avoided by the principle component (PC) which inserted directly singular value of the colored image. FPP occurs when false watermark is extracted from a cover image. [29] dual watermarking algorithm with chaotic system based on radial hormonic Fourier moments (RHFM) and (DWT-DCT) to achieve copyright protection. This study was based on blind watermarking. To achieve a better in watermarking embedding process a non-adjacent coupled map lattice chaotic system was used. DCT performed on the original image obtained by zero- watermarking. The direct information transformed by one- level DWT, each block transformed by DCT. By embedding the watermarking in the low-frequency area the robustness of the proposed method was tested from one direction. Another direction was applying various types of attacks (noise, cooping, rotation) to test the robustness and the invisibility. However, there was some limitations in this scheme where the direction information was not accurate enough and the time consuming could be approved more.

Discreate Wavelet Transformation (DWT):

It is a digital tool that convert the digital image from the spatial domain to the frequency transform domain [30, 31]. Robust wavelet – domain watermarking algorithm proposed in [32] based on chaos for still images. the WT is applied only locally while the whole image transformed in the frequency domain. A comparation applied between the watermark Coefficients and the watermark signals to detect the watermark and without using the original image, but by using a statistical assumption with Neyman-Pearson criterion. The research shows gaining in fidelity and high robust under typical geometric operation attack.

A multi-layer security of medical data presented by watermarking and chaotic encryption for tele-health applications using the transformation domain presenting a robust and secure watermarking approach. For better annotation, identification and authentication the patient identifier in to host medical image. The chaos-based encryption algorithm applied on watermarking for better confidentiality. The proposed results show a high robust and sufficient secured without distortion between watermarking and cover image. In the proposed research a combination of DWT, DCT and SVC presenting hybrid approach of watermarking and cryptography. A two-dimensional logistic chaotic map applied for better confidentiality of the patient information report providing a multi-level security [33].

For partial image encryption [34] implemented DWT and texture segmentation to a colored image. The image is divided for four sub-band. By using the texter segmentation Gaber filter and k- means clustering applied for the lowest frequency band. The resulted texture used as a method for scrambling the new image based on another image features which is finally used interchanged AES and RC4 algorithms to encrypt the preferred image. The work resulted a suitable robust image encryption scheme that is applicable to be used in real- time applications.

2- Chaotic in video protection

In video protection chaotic system is used to produce a stronger protection for the video content over networks specially after the abilities included in using computer and the spreading of videos abilities that the network included the ease of manipulating. Traditional techniques like encryption does not provide a hole protection for multimedia since the protection last till decoding process [35]. The invasion of privacy raises a high attention between people to the pervasive and intrusive surveillance practices.

Surveillance system played a hot role in the last decade in privacy protection approach. However, most mechanisms developed have a negative influence on the subsequent action recognition in the monitoring system. In this paper researchers depended on encrypting human face region. Three main steps implemented to localize human face. First, pedestrian detection. Second, extract face region by using skin color information YCbCr which is used as the recognition space between the faces and other domains. Finally, a spatial chaotic map which is developed to encrypt facial region [36]. The privacy is vulnerable to be exploit by adversaries and by people who are in charge of the mass-surveillance system. To increase the surveillance system privacy [37] proposed PriSev, a privacy- preserving selective video surveillance method. A dynamic chaotic image enciphering (DyCIE) algorithm is also used and connected with object scanner. DNN based frame classifier implemented in this paper to classifies frames as "aggressive" and "innocuous". A multi agent system is also implemented to decrypt the keys between senders and receivers. The result was preventing privacy breach duo to possible abuses or lakes by authorized people.

A biometric watermarking embodied in the audio part of video file by using a two robust mathematical transformation DWT and DCT instead of the video images. A multi chaotic sequence is also applied to find a video file location to embed the bio-watermarking "hid it in multi frequency domain" whereas, the bio-watermarking decrypted and encrypted by using the sequence. The digital videos used as a cover file. PSNR, SNR and MSE objective tests is applied for the proposed method with applying simple attacks that may hit the cover file [38].

According to the high- bandwidth that the networks have which raise the chance of different types of attacks and fraud including digital videos. Therefore, video copywrites and data protection gain a strong attention in the last decade. [39] a robust blind watermarking presented for video copyrights based on integer wavelet transformation (IWT), Singular value decomposition (SVD) and 3D generalized chaotic sine map(3D-GCSM). IWT applied for each main frame. Where the watermarking technique evaluated depending on data resilience, data capacity and three concepts of content quality. The embedding of watermarked video was in low frequency coefficients. To increase the efficiency and the functionality of the watermarking a security level added by the chaotic map. The Normalized Correlation Coefficient applied between the main watermark and the extracted watermark and the result was 1 or very close to 1. The proposed method showed a good term of quality and resistance to a variety of attacks.

In real time video encryption/ decryption techniques,[40] proposed a colored video encryption / decryption based on hybrid chaotic maps to prevent un authorized accessibility. Based on the research methodology, a quick, secured and efficient encryption/ decryption formula proposed also the confusion diffusion procedures was integrated to enhance the security. the results shows that the algorithm used has a high robustness and security beside low elapsed time and a resist for analytical attack, brute- force attack, known- plain text, chosen plain text and differential.

Conclusion

To identify the image protection in the field of watermarking and copyrights. Chaotic techniques have been reviewed concluding the efficiency of chaos in three domains. First, the special domain where some of the latest methods and algorithms were proposed. Second, the Discrete Cosine Transformation (DCT) which is a mathematical transformation which is viewed with the latest algorithms that conclude a higher result and its effect in enhancing robustness and lowering complicity using chaos techniques. Third, Discreate Wavelet Transformation (DWT) that proposed with some algorithms and methods which aimed to enhance robustness, fidelity and confidentiality. In the video protection chaos is used to provide a stronger key encryption by taking the advantage from the chaos characteristics such as non-periodicity, wide spectrum, unpredictability, and sensitivity to initial conditions. Surveillance system, video watermarking , biometric watermarking , colored video encryption are methods reviewed in this paper which specified the latest best results in video protection.

References

1- Zhou, L., Tan, F., & Yu, F. (2019). A robust synchronization-based chaotic secure communication scheme with double-layered and multiple hybrid networks. IEEE Syst J.

2- Gu, K., Wu, N., Yin, B., & Jia, W. (2019). Secure data query framework for cloud and fog computing. *IEEE Transactions on Network and Service Management*, *17*(1), 332-345.

3- Gu, K., Wu, N., Yin, B., & Jia, W. (2019). Secure data sequence query framework based on multiple fogs. *IEEE Transactions on Emerging Topics in Computing*, *9*(4), 1883-1900.

4- Gu, K., Wang, K., & Yang, L. (2019). Traceable attribute-based signature. *Journal of Information Security and Applications*, *49*, 102400.

5- Bai, B., Huang, J., Qiao, G. R., Nie, Y. Q., Tang, W., Chu, T., ... & Pan, J. W. (2021). 18.8 Gbps real-time quantum random number generator with a photonic integrated chip. *Applied Physics Letters*, *118*(26), 264001.

6- Habek, M., Gene, Y., Aytas, N., Akkoc, A., Afacan, E., & Yazgan, E. (2022, June). Digital Image Encryption Using Elliptic Curve Cryptography: A Review. In *2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)* (pp. 1-8). IEEE.

7- William, P., Choubey, A., Chhabra, G. S., Bhattacharya, R., Vengatesan, K., & Choubey, S. (2022, March). Assessment of Hybrid Cryptographic Algorithm for Secure Sharing of Textual and Pictorial Content. In *2022 International Conference on Electronics and Renewable Systems (ICEARS)* (pp. 918-922). IEEE.

8- Hafsa, A., Sghaier, A., Malek, J., & Machhout, M. (2021). Image encryption method based on improved ECC and modified AES algorithm. *Multimedia Tools and Applications*, *80*(13), 19769-19801.

9- Forouzan, B. A. Introduction to Cryptography and Network Security. 2008. *New York*.

10- Koç, Ç. K. (Ed.). (2014). *Open problems in mathematics and computational science*. Cham: Springer International Publishing.

11- Yu, F., Li, L., Tang, Q., Cai, S., Song, Y., & Xu, Q. (2019). A survey on true random number generators based on chaos. *Discrete Dynamics in Nature and Society*, *2019*.

12- Rezk, A. A., Madian, A. H., Radwan, A. G., & Soliman, A. M. (2019). Reconfigurable chaotic pseudo random number generator based on FPGA. *AEU-international Journal of Electronics and Communications*, *98*, 174-180.

13- Elmanfaloty, R. A., & Abou-Bakr, E. (2019). Random property enhancement of a 1D chaotic PRNG with finite precision implementation. *Chaos, Solitons & Fractals*, *118*, 134-144.

14- Wang, Y., Liu, Z., Ma, J., & He, H. (2016). A pseudorandom number generator based on piecewise logistic map. *Nonlinear Dynamics*, *83*(4), 2373-2391.

15- Chen, L., Chen, J., Zhao, G., & Wang, S. (2019). Cryptanalysis and improvement of a chaos-based watermarking scheme. *IEEE Access*, *7*, 97549-97565.

16- Khan, J. S., Kayhan, S. K., Ahmed, S. S., Ahmad, J., Siddiqa, H. A., Ahmed, F., ... & Al Dubai, A. (2022). Dynamic S-Box and PWLCM-Based Robust Watermarking Scheme. *Wireless Personal Communications*, 1-18.

17- Reddy, R. R. C., Vivekanand, U., & Kamath, C. Cryptography & watermarking using Chaos.

18- Chen, L., & Wang, S. (2015). Differential cryptanalysis of a medical image cryptosystem with multiple rounds. *Computers in biology and medicine*, *65*, 69-75.

19- Khaitan, S., Sagar, S., & Agarwal, R. (2021). Chaos based image encryption using 3-Dimension logistic map. *Materials Today: Proceedings*.

20- Mansouri, A., & Wang, X. (2021). A novel one-dimensional chaotic map generator and its application in a new index representation-based image encryption scheme. *Information Sciences*, *563*, 91-110.

21- Gu, Q., & Gao, T. (2013). A novel reversible robust watermarking algorithm based on chaotic system. *Digital Signal Processing*, *23*(1), 213-217.

22- Zhou, N., Yan, X., Liang, H., Tao, X., & Li, G. (2018). Multi-image encryption scheme based on quantum 3D Arnold transform and scaled Zhongtang chaotic system. *Quantum Information Processing*, *17*(12), 1-36.

23- Kang, X. B., Lin, G. F., Chen, Y. J., Zhao, F., Zhang, E. H., & Jing, C. N. (2020). Robust and secure zero-watermarking algorithm for color images based on majority voting pattern and hyper-chaotic encryption. *Multimedia Tools and Applications*, *79*(1), 1169-1202.

24- Tan, Y., Qin, J., Xiang, X., Ma, W., Pan, W., & Xiong, N. N. (2019). A robust watermarking scheme in YCbCr color space based on channel coding. *IEEE Access*, *7*, 25026-25036.

25- Su, Q., Zhang, X., & Wang, H. (2022). A blind color image watermarking algorithm combined spatial domain and SVD. *International Journal of Intelligent Systems*, *37*(8), 4747-4771.

26- Su, Q., Liu, D., Yuan, Z., Wang, G., Zhang, X., Chen, B., & Yao, T. (2019). New rapid and robust color image watermarking technique in spatial domain. *IEEE Access*, *7*, 30398-30409.

27- Yuan, Z., Su, Q., Liu, D., Zhang, X., & Yao, T. (2020). Fast and robust image watermarking method in the spatial domain. *IET Image Processing*, *14*(15), 3829-3838.

28- Cheema, A. M., Adnan, S. M., & Mehmood, Z. (2020). A novel optimized semi-blind scheme for color image watermarking. *IEEE Access*, *8*, 169525-169547.

29- Giri, K. J., & Bashir, R. (2018). A block based watermarking approach for color images using discrete wavelet transformation. *International Journal of Information Technology*, *10*(2), 139-146.

30- Roy, S., & Pal, A. K. (2019). A hybrid domain color image watermarking based on DWT–SVD. *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, *43*(2), 201-217.

31- Wang, R., Shaocheng, H., Zhang, P., Yue, M., Cheng, Z., & Zhang, Y. (2020). A novel zero-watermarking scheme based on variable parameter chaotic mapping in NSPD-DCT domain. *IEEE Access*, *8*, 182391-182411.

32- Dawei, Z., Guanrong, C., & Wenbo, L. (2004). A chaos-based robust wavelet-domain watermarking algorithm. *Chaos, Solitons & Fractals*, *22*(1), 47-54.

33- Thakur, S., Singh, A. K., Ghrera, S. P., & Elhoseny, M. (2019). Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications. *Multimedia tools and Applications*, *78*(3), 3457-3470.

34- Noori Ghanim, Z., & Raheem Khoja, S. A. (2022). A partial image encryption scheme based on DWT and texture segmentation. *Cogent Engineering*, *9*(1), 2026555.

35- Loganathan, A., & Kaliyaperumal, G. (2016). An adaptive HVS based video watermarking scheme for multiple watermarks using BAM neural networks and fuzzy inference system. *Expert Systems with Applications*, *63*, 412-434.

36- Liu, S., & Kong, L. (2018, May). Local chaotic encryption based on privacy protection on video surveillance. In *2018 8th International Conference on Social science and Education Research (SSER 2018)* (pp. 390-393). Atlantis Press.

37- Fitwi, A., & Chen, Y. (2020, August). Privacy-preserving selective video surveillance. In *2020 29th International Conference on Computer Communications and Networks (ICCCN)* (pp. 1-10). IEEE.

38- Mohammed, S. Embedding biometric watermarking in video file based on chaotic principle. *technology*, *5*, 7.

39- Farri, E., & Ayubi, P. (2018). A blind and robust video watermarking based on IWT and new 3D generalized chaotic sine map. *Nonlinear Dynamics*, *93*(4), 1875-1897.
Eid, M. M., El-kenawy, E. S. M., & Ibrahim, A. A Fast Real-Time Video Encryption/Decryption Technique Based on Hybrid Chaotic Maps.