Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 6, June : 2023

A NOVEL CHAOTIC SYSTEM-BASED ANALYSIS OF IMAGE SECURITY AND VIDEO WATERMARKING SYSTEM USING DCT

Dr. S. Swapna Rani
Associate Professor, Department of ECE, Maturi Venkata Subba Rao (MVSR) Engineering college, Hyderabad.
E-Mail: sswapnarani_ece@mvsrec.edu.in

ABSTRACT
With the ongoing advancement of multimedia technology, data security has emerged as a significant issue. In this work, the encryption and decryption processes will be chaotic. DCT is enabled with the cryptography of the key that will be used for hiding in the image, and once the Key that is set at DCT and IDCT is matched, the encryption and decryption processes will be completed. Information concealment was one of the most important issues in human cultures due to the development and urgent demand for data transmission through social networks. applied to the concealment of private information on various digital media, including email, audio, video, and pictures. Here, we embed the text message and extract it to create a picture and text message.
Keywords: DCT, Cryptography, encryption, decryption

INTRODUCTION

The art of steganography involves hiding a message. Steganography is used to hide communications from people you don't want to see them. Contrary to cryptography, it does not hide the fact that a secret communication is taking place; rather, it renders messages impossible to read.

There are many parallels between steganography and cryptography despite the fact that the two have different objectives. In fact, some authors classify steganography as a form of cryptography because hidden communication is a form of secret writing. In popular computer files (including images, sounds, text, and HTML), steganography swaps out ineffective or infrequently used data for new, hidden data. This confidential information may be presented as plain text, cypher text, or even visuals.

Steganography and watermarking are two fields linked to information concealment: Information hiding has three essential components: capacity, security, and resilience. Capacity is the maximum quantity of information that can be concealed, security is the inability of eavesdroppers to find the concealed data, and robustness is the maximum amount of modification the cover medium can withstand before the concealed data becomes tainted.

Steganography is a method of storing data that conceals their existence. Steganography was used to carry out covert transactions. For instance, governments are interested in two different sorts of concealed data communication: the one promotes national security, whereas the second does not. Both sorts are supported by steganography, and businesses also have comparable worries about trade secrets for new technology or product information. Of course, the chance of information leaking is much decreased when communicating through steganography. Businesses utilise watermarking, a different type of steganography.

Watermarking involves a hidden, distinctive piece of information that is used to identify a media without actually touching it. As an illustration, imagine that I have designed an image and added a watermark to it that identifies me as the author. If and when this image is shared with others, I will be able to verify my ownership of it and identify myself as its inventor. Companies frequently employ this strategy for copyrighted digital media in order to provide protection. Additionally, steganography improves privacy on an individual basis, however it does not replace encryption. Of course, this is only successful if the hidden embedded information is

not discovered.

In multimedia, there are three main watermarking strategies. The first is called spatial domain watermarking, and it basically involves embedding a PRN sequence or a visible logo into specific host image pixels. The second is watermarking that transforms domains, such as DCT, DWT, or DFT. The third option, compressed domain watermarking, is only available for audio or video files. The typical requirements for a video watermarking technique include transparency, robustness, (blind) oblivious detection, freedom from deadlock problems, public key detection, and others. All of the available watermarking techniques, however, only fully meet some of the requirements. As an illustration, certain methods are extremely robust (oblivious), but they are not sufficiently robust.

LITERATURE REVIEW

[1] Z. Wang and X. Zhang (#1) Current steganography cover selection techniques are unable to withstand pooled steganalysis. This study suggests a safe cover selection technique that can withstand both pooled and individual item steganography. When choosing a cover, the maximum mean discrepancy (MMD) distance between the stego set and a clear arbitrary image set is kept below a normal threshold, where the threshold is the MMD distance between two clear arbitrary image sets, in order to avoid pooled steganalysis. In order to resist single object steganalysis under this restriction, a searching approach is created to choose the least steganographically altered photos that fit within an acceptable computational complexity. The security of steganography is ensured with the chosen covers against both single object steganalysis and pooled steganalysis. The experimental results demonstrated the effectiveness of the proposed method.

[2] [2] C.-M. Wang and K.-C. Wu: A unique steganography method involving reversible texture creation was suggested by the author. Re-sampling a reduced texture image allows a texture synthesis method to create a new texture image of arbitrary size and equivalent local appearance. To hide hidden messages, we incorporate the texture generation process into steganography. Our approach hides the source texture image and embeds hidden messages through the process of texture synthesis, as opposed to using an existing cover image to hide information. This enables us to retrieve the source texture from a stego synthetic texture as well as hidden messages. Our strategy has three clear benefits. First, our system provides embedding capacity proportional to stego texture image size. Second, our steganographic strategy is unlikely to be compromised by a steganalysis programme. Third, the functionality that allows recovery of the source texture is provided by the reversible ability inherited from our scheme. Our suggested approach can provide a range of embedding capacities, create visually appealing texture images, and recover the source texture, according to experimental results.

[3] [3] Z. Qu, Z. Cheng, and X. Wang: One of the important research areas in quantum secure communication is embedding secret information into quantum carrier images for covert transmission. This work suggests a unique matrix coding-based quantum steganography approach for quantum colour images that has strong imperceptibility and great embedding efficiency. Two distinct embedding techniques are suggested in order to properly use matrix coding in real-world requirements. SPE (1, 3, 2) coding, also known as single pixel embedded (1, 3, 2) coding, is one embedding technique. This technique would change no more than one LSQb while embedding two qubits of secret information into three least significant qubits (LSQbs) of a single quantum carrier picture pixel. The other embedding technique uses three LSQbs of multiple carrier pixels and is known as MPsE (1, 3, 2) coding. It uses two secret qubits to be hidden within each of the three LSQbs.

[4] [4] J. Fridrich and T. Denemark: Incorporating side-information at the sender is widely acknowledged to considerably increase steganographic security in actual use. The majority of side-informed techniques used today start with a high quality "precover" image, which is then processed, jointly quantized, and embedded with a secret. For use cases where the sender does not have access to a precover, we study an alternate type of side-information in this paper—a collection of several JPEG photographs of the same scenario.

In order to control the costs of changing particular DCT coefficients in an existing embedding scheme, the additional JPEG images are used to decide on the preferred polarity of embedding changes. In comparison to steganography using a single JPEG image, tests on actual images with synthetic acquisition noise and on genuine multiple acquisitions taken with a tripod-mounted and hand-held digital camera demonstrate a very large improvement in empirical security. Using Monte Carlo simulations, it is demonstrated that the proposed empirically determined modulation of embedding costs qualitatively minimises the Bhattacharyya distance between a quantized generalised Gaussian model of cover and stego DCT coefficients tainted by AWG acquisition noise.

EXISTING SYSTEM

To incorporate the watermark, we will pick the middle and high components that are over the JND threshold. In the DCT domain for H.264/AVC, there are primarily two types of watermark embedding methods. One type of algorithm, which is typically utilised in the low and middle component of the DCT coefficient, modifies the parity of the DCT coefficients in accordance with the watermark information. Though its resilience is low, this type of method has little effect on video quality. A different approach either raises the DCT coefficient or sets it to zero based on the watermark data. This kind of technique has superior robustness and is typically utilised for high frequency components. In order to incorporate the watermark into the medium and high components, we thus use two different types of methods. The procedure flow diagram for embedding a watermark is displayed. The embedding of the watermark is demonstrated as follows: in order to create safe sensitive data. All of these algorithms for creating secret keys are based on a single chaotic map. The process of encrypting and decrypting uses the key.

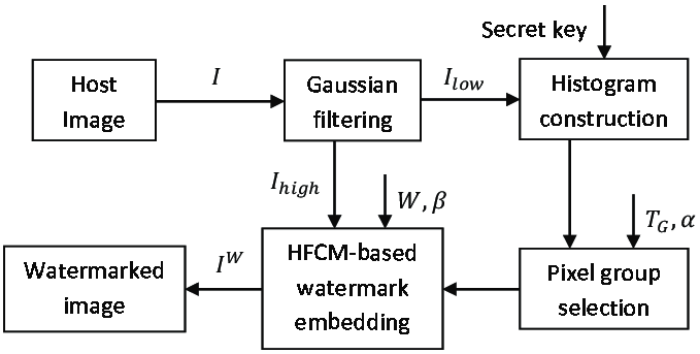

Fig. 1: watermark embedding process

The watermark embedding process is shownas follows:

step 1: Divide the current I-frame of video into 4×4 blocks, and implement integer DCT each block. Then calculate every JND threshold value of the integer DCT coefficient.

step 2: Analyze whether the JND threshold is larger than the quantized value. Since embedding watermarks in non-zero DCT coefficients will not significantly increase the bit rate, therefore, we analyze whether coefficient is greater than zero. If both of these two conditions are met, we embed the watermark. Then we set the watermark embedding position as a secret key.

PROPOSED SYSTEM

Many symmetric-key chaos-based picture and plaintext encryption techniques have been developed during the 1990s with the aim of achieving high diffusion and confusion in or A block cypher is used in the proposed chaos-based picture encryption technique. This block cypher uses several chaotic maps to create secret keys

with different lengths, such as 128, 256, and 512 bits. The suggested encryption and decryption procedure is broken down into the following steps: The beginning and output cypher pictures are divided into set length blocks for encryption and decoding. The following figure shows how a secret key is created: The two phases of encryption process are illustrated in the figure below:

Phase 1: secret key generation

Phase 2: image encryption

Secret Key Generation (Chaotic System):

The secret key is a prerequisite for encrypted data and is regarded as being more important than the encryption algorithm for a number of reasons. First, without the secret key, the encrypted data cannot be decrypted; second, the key space needs to be very large to prevent brute-force attacks; and third, if the secret key is weak, the encryption will fail. Since the secret key is independent of the plaintext by nature, multiple keys are utilised to encrypt different cipher-text from similar plaintext. A secret key is essential to the process of encrypting images because without one, attackers would be able to decipher the cypher image.

Therefore, supporters of successful encryption argue that the cypher keys must be vulnerable to the algorithm; as a result, the key space must be sufficiently large to ensure protection from all types of attacks. Secret keys also require a considerable amount of randomness, which can be produced using the chaos theory. The paper adopts a multi-chaotic system as follow

$$X_{n+1} = rX_n\,(1 - X_n)$$
$$X_{n+1} = exp\,(-\alpha X_n^2) + \beta$$
$$\begin{cases} X_{n+1} = 1 - \alpha X_n^2 + Y_n \\ Y_{n+1} = bX_n \end{cases}$$

Where X_n is the initial value. r, α, β and b are real constant parameters of system.

PROPOSED METHOD

First, a general residual chaotic system for picture encryption is developed based on RNS to address the flaw that classic chaotic systems typically require greater bit-width iterative calculations to alter the generation rate of chaotic systems. The following information is contained in the main principles of this encryption system: Utilising the Box-Muller technique and a normally distributed chaotic sequence as the key, iterate a one-variable polynomial function in GF to produce a generic chaotic sequence. Additionally, the system realises concurrent conversion calculation during R/B backward conversion, which significantly enhances the effectiveness of encryption and picture security. Secondly, a watermark embedding and extraction algorithm based on block selection is suggested with the goal of preventing the distortion drift of video watermarks.

First, five categories are established for the 4 4 brightness blocks based on the H.264 intra-frame prediction mode. When embedding, the suitable category of blocks is chosen based on conditional judgements, followed by additional processing of the encrypted pre-processed data, and ultimately, the watermark data and the chosen block are embedded in the DCT domain in accordance with a specific algorithm.

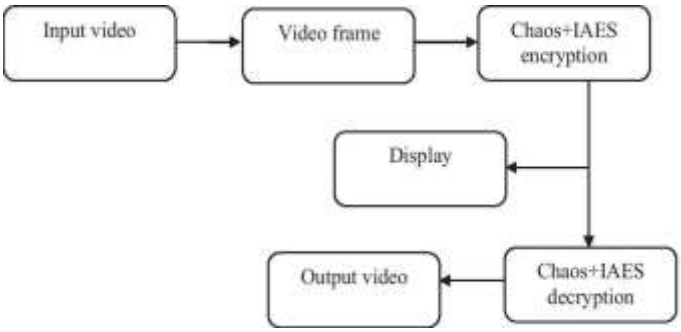

Fig. 2: Encryption and Decryption

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 6, June : 2023

SIMULATION RESULTS

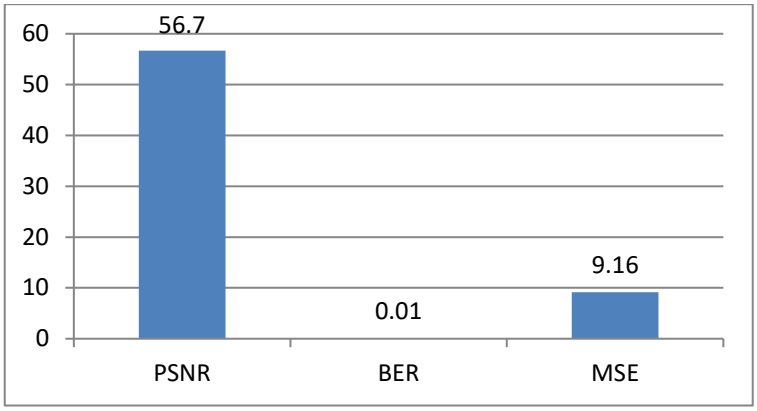

Fig. 3 : Input Image values

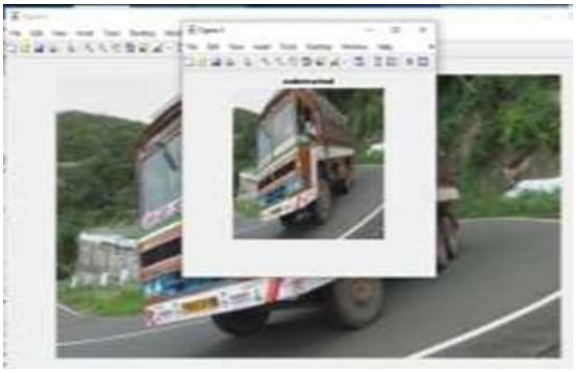

Fig. 4: Embedded a image in a video.

Fig. 5: Encrypted Image.

CONCLUSION

In this research, we suggested a novel chaotic system-based picture encryption technique. The repetitive computation of a big bit width can be divided into many calculations of a small bit width depending on the new method and block selection. The new intra-prediction mode keeps visual quality and capacity in balance. The encrypted version of the RCS we've presented is more secure, has a bigger key space, and performs better in terms of robustness and randomness. The cryptosystem we suggested is thus a suitable choice for picture encryption in watermark embedding technology. The experimental findings demonstrate the stronger robustness of the watermark embedding algorithm used in this paper.

REFERENCES

[1] Z. Wang and X. Zhang, "Secure cover selection for steganography," IEEE Access, vol. 7, pp. 57 857–57 867, 2019.

[2] K.-C. Wu and C.-M. Wang, "Steganography using reversible texture synthesis," IEEE Transactions on Image Processing, vol. 24, no. 1, pp. 130–139, 2015.

[3] Z. Qu, Z. Cheng, and X. Wang, "Matrix coding-based quantum image steganography algorithm," IEEE Access, vol. 7, pp. 35 684–35 698, 2019.

[4] T. Denemark and J. Fridrich, "Steganography with multiple JPEG images of the same scene," IEEE Transactions on Information Forensics and Security, vol. 12, no. 10, pp. 2308–2319, 2017

[5] Y. Zhang, X. Luo, Y. Guo, C. Qin, and F. Liu, "Zernike moment-based spatial image steganography resisting scaling atta Y. Wang, ''New Chinese remainder theorems,'' in Proc. 32nd Asilomar Conf. Signals, Syst., Comput., Pacific Grove, CA, USA, vol. 1, Nov. 1998, pp. 165–171, doi: 10.1109/ACSSC.1998.750847.

[6] W. Wang, M. N. S. Swamy, and M. O. Ahmad, ''Moduli selection in RNS for efficient VLSI implementation,'' in Proc. Int. Symp. Circuits Syst., vol. 4, 2003, pp. 512–515.

[7] H. Zhu, C. Zhao, and X. Zhang, ''A novel image encryption-compression scheme using hyper-chaos and Chinese remainder theorem,'' Signal Process. Image Commun., vol. 28, no. 6, pp. 670–680, Jul. 2013.

[8] N. Zhou, A. Zhang, J. Wu, D. Pei, and Y. Yang, ''Novel hybrid image compression–encryption algorithm based on compressive sensing,'' Optik, vol. 125, no. 18, pp. 5075–5080, Sep. 2014.

[9] Z. Yong, ''The unified image encryption algorithm based on chaos and cubic S-box,'' Inf. Sci., vol. 450, pp. 361–377, Jun. 2018. [13] B. Hu, Z.-H. Guan, N. Xiong, and H.-C. Chao, ''Intelligent impulsive synchronization of nonlinear interconnected neural networks for image protection,'' IEEE Trans. Ind. Informat., vol. 14, no. 8, pp. 3775–3787, Aug. 2018.

[10] Q. Zhang, C. Zhou, and Y. C. Tian, ''A fuzzy probability Bayesian network approach for dynamic cybersecurity risk assessment in industrial control systems,'' IEEE Trans. Ind. Informat., vol. 14, no. 6, pp. 2497–2506, Jun. 2018.

[11] M. Fallahpourckand statistic detection," IEEE Access, vol. 7,pp. 24 282–24 289, 2019.