مجلة

كلية التـــراث الجامعة

مجلة علمية محكمة

متعددة التخصصات نصف سنوية

العدد السابع والثلاثون

15 حزيران 2023

ISSN 2074-5621

رئيس هيئة التحرير

أ.د. جعفر جابر جواد

مدير التحرير

أ. م. د. حيدر محمود سلمان

رقم الايداع في دار الكتب والوثائق 719 لسنة 2011

مجلة كلية التراث الجامعة معترف بها من قبل وزارة التعليم العالي والبحث العلمي بكتابها المرقم (ب 3059/4) والمؤرخ في (2014/ 4/7)

Video Encryption in Parallel Environment: A Survey

Sara Joda Al-Saeed **Ali Shakir Mahmood**

Department of Computer Science, Collage of Education,
Mustansiriyah University

Abstract— As networks continue to develop, more information is being transmitted online, including multimedia content like images, videos, and other visual media types. These details must be protected using encryption algorithms because they might be sensitive. Encryption procedures have grown more difficult and expensive as a result of the growth in data volume and complexity of visual information. Encryption methods can be applied in a parallel computing environment to increase encryption efficiency and shorten execution time. It is possible to encrypt different portions of a video at once by dividing the encryption process among a number of parallel operations. Parallel video encryption can offer quicker encryption speeds by utilizing the power of parallel processing, making it appropriate for real-time applications or scenarios involving large video collections. In areas like video surveillance, secure video streaming, or protecting video content, it enables the effective use of computational resources. In general, using parallel video encryption is a promising way to secure video data because it combines the power of parallel processing with encryption methods, improving encryption performance and increasing video security. This research paper presents a comparative analysis of innovative video encryption algorithms. These algorithms are judged according to standards like perceptual performance of encryption and decryption, error rates and quality, level of security, and compatibility with common video formats. Significant contributions have been made by earlier studies in the field. Incorporating a variety of innovative algorithms, researchers have created a number of techniques, including permutation-based pixel encryption, chaotic mapping, and partial video encryption. Peak signal-to-noise ratio, correlation coefficients, and error rates are a few examples of the measurements used to assess these algorithms' performance. Furthermore, some algorithms exhibit adaptability by observing the established video compression standards and preserving the size and format of the original data.

Keywords— Video Encryption, Parallel Environment, the Chaos Theory

الخلاصة— مع استمرار تطور الشبكات ، يتم نقل المزيد من المعلومات عبر الإنترنت ، بما في ذلك محتوى الوسائط المتعددة مثل الصور ومقاطع الفيديو وأنواع الوسائط المرئية الأخرى. يجب حماية هذه التفاصيل باستخدام خوارزميات التشفير لأنها قد تكون حساسة. أصبحت إجراءات التشفير أكثر صعوبة وتكلفة نتيجة للنمو في حجم البيانات وتعقيد المعلومات المرئية. يمكن تطبيق طرق التشفير في بيئة الحوسبة المتوازية لزيادة كفاءة التشفير وتقصير وقت التنفيذ. من الممكن تشفير أجزاء مختلفة من الفيديو دفعة واحدة بتقسيم عملية التشفير على عدد من العمليات المتوازية. يمكن أن يوفر تشفير الفيديو المتوازي سرعات تشفير أسرع من خلال الاستفادة من قوة المعالجة المتوازية ، مما يجعلها مناسبة لتطبيقات الوقت الفعلي أو السيناريوهات التي تتضمن مجموعات فيديو كبيرة. في مجالات مثل المراقبة بالفيديو ، دفق الفيديو الآمن ، أو حماية محتوى الفيديو ، فإنه يتيح الاستخدام الفعال للموارد الحسابية. بشكل عام ، يعد استخدام تشفير الفيديو المتوازي طريقة واعدة لتأمين بيانات الفيديو لأنه يجمع بين قوة المعالجة المتوازية وطرق التشفير ، وتحسين أداء التشفير وزيادة أمان الفيديو. تقدم هذه الورقة البحثية تحليل مقارن لخوارزميات تشفير الفيديو المبتكرة. يتم الحكم على هذه الخوارزميات وفقًا لمعايير مثل

الأداء الإدراكي للتشفير وفك التشفير ، ومعدلات الخطأ والجودة ، ومستوى الأمان ، والتوافق مع تنسيقات الفيديو الشائعة. تم تقديم مساهمات كبيرة من خلال الدراسات السابقة في هذا المجال. بدمج مجموعة متنوعة من الخوارزميات المبتكرة ، ابتكر الباحثون عددًا من التقنيات ، بما في ذلك تشفير البيكسل القائم على التقليب ، والتخطيط الفوضوي ، والتشفير الجزئي للفيديو. تعد نسبة ذروة الإشارة إلى الضوضاء ومعاملات الارتباط ومعدلات الخطأ أمثلة قليلة على القياسات المستخدمة لتقييم أداء هذه الخوارزميات. علاوة على ذلك ، تظهر بعض الخوارزميات قابلية التكيف من خلال مراقبة معايير ضغط الفيديو المعمول بها والحفاظ على حجم وشكل البيانات الأصلية.

I. INTRODUCTION

Since the time of the ancient Romans, who employed comparable techniques to ensure protection of their important information and documents, encoding has been demonstrated to be one of the most effective methods for protecting information [1]. Information security could be referred to as information, a set of steps, methods, and policies, and the tactics accustomed to prevent and detect unauthorized accessibility to, troubleshooting of, disclosure of, disturbance of, and adjustment of computer network sources. Data encoding is the process of transforming data into particular symbols using meaningless codes. Identical key Cryptography is a technique for both encoding and decoding data. That only uses one key [1]. Cryptography, according to the Official Oxford Brief English Dictionary, is the art of writing or solving codes. Although historically correct, this does not adequately reflect the present scope of the field or its modern scientific underpinnings. Just the codes used for covert communication over the years are the subject of the definition. However, modern cryptography deals with much more than this, including methods for maintaining integrity, protocol strategies for sharing private keys, procedures for user authentication, electronic marketplaces and elections, electronic cash, and more. Without making an effort to offer a comprehensive classification, we could say that current cryptography is the study of mathematical techniques for protecting electronic information, systems, and devices from malicious attacks [2].

The advancement of information technology currently facilitates people's convenience, but it also creates prevalent security issues.". As more understandable information carriers, multi-media like image and video have found extensive use in the sectors of information transmission, medicine, military service, and other fields. Let's review what a digital video is before getting to the meat of the issue: A sort of information in digital form, mechanisms, and services operates by employing a video signal that is digital rather than an analog video signal [3], [4].To render the video unwatchable, opaque, or incomprehensible while encryption is used for storage or transmission. Priority number one is data security using cryptography to prevent illegal access by combatants. Data encryption addresses these problems and raises the level of digital world security [5], [6].

Most multimedia applications require video content to be secured, and the best way to secure videos is to encrypt them. For the purpose of protecting data, encryption involves transforming it from a format that can be read into an unreadable one. [7], [8].Video encryption is thought to be a very effective method for protecting video data. Video encryption deals with a significant amount of extra data from frame to frame. In order to be secure, the encryption technique must consequently offer a more complicated mechanism. A strong and quick encryption solution is required when the video is huge [11], [5]. The chaotic system is founded on nonlinear behaviors that respond incredibly poorly to their initial conditions. Given that chaotic systems are unpredictable over the long term due to their ergodicity and complicated dynamics, they appear to be a strong candidate [9], [10].

To create cryptographic systems with the highest level of entropy and resistance to attacks, these systems' equations produce unpredictable random values. The concept of "parallel processing" is emerging as a possible method for doing extensive engineering computations. Strong microprocessors can be used in parallel to produce high performance [9], [11].

The advancement of information technology currently facilitates people's convenience, but it also creates prevalent security issues.". As more understandable information carriers, multi-media like image and video have found extensive use in the sectors of information transmission, medicine, military service as well as the other field. Let's review what a digital video is before getting to the meat of the issue: a sort Information in digital form, mechanisms, and services operates to employing A video signal that is digital rather than an analog video signal [3], [4].

To render the video unwatchable, opaque, or incomprehensible while Encryption is used for storage or transmission. Priority the highest is Data security using cryptography prevents illegal access combatants. Data encryption addresses these problems and raises the level of digital world security [5], [6]. Most multimedia applications require video content to be secured, and the best way to secure videos is to encrypt them. For the purpose of protecting data, encryption involves transforming it from a format that can be read into an unreadable one. [7], [8].

Video encryption is thought to be a very effective method for protecting video data. Video encryption deals with a significant amount of extra data from frame to frame.In order to be secure, the encryption technique must consequently offer a more complicated mechanism. A strong and quick encryption solution is required when the video is huge [11], [5].

The Chaotic system is founded on nonlinear behaviors,that respond incredibly poorly to their initial conditions. Given that chaotic systems are unpredictable over the long term due to their ergodicity and complicated dynamics, they appear to be a strong candidate [9], [10].

To create cryptographic systems with the highest level of entropy and resistance to attacks, these systems' equations produce unpredictable random values. The concept of "parallel processing" is emerging as a possible method for doing extensive engineering computations. Strong microprocessors can be used in parallel to produce high performance [9], [11].

II. RELATED WORKS

Video encryption techniques aim to protect the confidentiality and integrity of video content by encoding it in a way that only authorized users can access and decode. Encryption methods have also been proposed for secure video data storage and transmission, ensuring that the content is only accessible to those who are authorized. Several studies have been conducted in recent years to investigate the use of chaotic systems in video coding, with a focus on the development of chaotic-based encoding schemes that improve the efficiency, security, and robustness of video transmission we will examine how video encryption techniques have performed in terms of security, complexity, and efficiency in previous research in this paper.

A. In 2006 [12], Wong, A., & Bishop, W. The author has disclosed an effective parallel video encryption technique designed for consumer devices. It is possible to accomplish an acceptable level of security while greatly reducing the computing burden associated with encryption by using partial video encryption techniques. That enhances security while preserving effectiveness and format compliance by using a variety of stream ciphers and a special multi-key technique. Experimental findings from the encoding of numerous check video sequences show the efficiency system for video encoding.

B. In 2008[13], the authors Yang , S., & Sun, S presented a new and secure Using a chaotic map for the DCT domain as the basis for video encryption. They decide to use the video sequence's I-frames as encryption objects. Every original I-frame's DCT coefficients have been first scrambled using coupling chaotic maps, and then the scrambled I-frame is obtained. Second, they use another chaotic map to encrypt the scrambled I-DCT frame's coefficients. They employ five keys, a trio chaotic maps, double encryption of the I-frame, and throughout the procedure.

C. In 2008 [14], Shang, F., Sun, K., & Cai,.The author presented a powerful chaotic cipher-based MPEG video encoding system. The proposed chaotic stream cipher completes the initial phase of selective encryption by encrypting the Fixed Length Code word (FLC) to protect video content..Then, for each frame, chaos-based permutation is used to perform Shuffling of macro blocks in the video bit stream The idea for a chaotic encryption system uses two simplest chaotic maps and does not use floating-point arithmetic, resulting in fast encryption.
The suggested video encryption algorithm is well suited for MPEG video apps and could be modified to work alongside various compression standards because it has a number of desirable features like real-time processing, scalable security levels, strict size preservation, and full development compliance.In 2015[15], Bowade, J. S., khade, P., & Raghuwansh, M. M. They used multidimensional chaotic maps to encode videos and suggested image encryption methods based on low dimension chaotic functions. The video frames are shuffled together with the frame scrambling in order to maintain a balance between security and computing time. For the encryption of video frames and the creation of a 4D map, they employed the 3D Arnolds cat map. However, in order to make video encryption more resistant to selected assaults, a shuffling mechanism is provided here. Arnold's 4D cat is used to shuffle the cards. The original video cannot be cracked by any invader thanks to the movie's encryption, which also makes it more secure and sturdy.

D. In 2017 [16], Hamidouche, W., Farajallah, M., Ould-Sidaty, N., Assad, S. el, Déforges, O., Sidaty, N., & Deforges, They proposed an option for selective video encryption based on the chaotic system in the expandable HEVC extension. In terms of robustness and speed, the used chaos-based stream mechanism outperforms conventional stream ciphers. With minimal delay and complexity overheads, the suggested method encrypts an assortment of sensitive SHVC parameters.The encryption is done at the CABAC bin string level, and it meets both the requirements for constant bit rate and format compliant video encryption. It also keeps all SHVC features like the bit stream removal for mid-network adaptation and error resilience. The first scheme encrypts only the bottom SHVC layer, while the second encrypts all layers and the third only the top layer. The reliability of the proposed schemes is assessed using several kinds of video encryption standards, scalability arrangements, and High Definition (HD) sequences of video .The experiments showed that encrypting only the lowest or all of the various layer's results in a high level of security, whereas encrypting only the highest layer outcomes in a perceptual encryption water by slightly lowering the highest layer quality. Additionally, the proposed solution's complexity of processing is assessed within the context of a real-time SHVC decoder. The proposed solution's processing complexity is assessed in the context of a real-time SHVC decoder. The level of complexity overhead continues to be low, accounting for less than 6% of the total time involved within the actual time decoding SHVC video sequences.

E. In 2018 [8], Ibrahem, M. K., & Hamood A chaotic sequence created by combining two logistic maps and a cat map, according to a proposed method to video encryption, and a piecewise linear chaotic map—is used as the encryption key. This chaotic sequence is then used to scramble the frame's DCT coefficients before being encrypted using a specific formula. Conduct permutation on the macro block of each frame after picking encrypted to obtain the decrypted movie data from each frame. Using the inverse method, the video decrypted. First, a first logistic map is used to encrypt the video data, and the results of that encryption are then re-encrypted using a second sequence. The experiments with the created and used video encryption technology were successful.

F. In 2018 [17], Khorsheed, K. O., Abood, O. G., Guirguis, S., & Guirguis, S. K,. This research has addressed the function and importance of security for video transfer in depth. Encryption is crucial in sending the video core since it helps to ensure its confidentiality. In a nutshell, academic research has focused on a modern solution for pixel-based real-time video encryption. The idea behind pixel encryption is to move and change the values of the pixels. The position of pixel values is modified according to the unscrambled order that is formed. Overall, rearranging the pixel values first, then manipulating them in the opposite direction at the recipient side, would hold the decryption to edit the original video.

G. In 2019 [7], Abdalrdha, Z. K., Shawe, R. T., Hussein, S. A., Abbas, F. N., & Ridha, A. K. New video coding method has been devised for the purpose to avoid confusion among the chaotic system and the NTRU technique in digital video encoding. The video is encrypted with the NTRU method and decrypted with the chaotic algorithm to keep a high level of strength and security. The algorithm's strength is its usage of two keys (the public and private key) for the encryption process and the strength of the chaotic algorithm, which significantly raises the bar for video encryption safety requirements. In the outcome of the chaotic system's sensitivity to the starting situation. Common issues with video encryption systems were resolved via chaotic system decryption.

H. In 2021 [18], Elrefaey, A., Sarhan, A., & El-Shennawy, N. M. The author proposes leveraging GPUs to speed up an existing chaotic-based picture encryption technique. They want to make chaos-based encryption algorithms more efficient by introducing parallel implementations that use GPUs to perform the encryption and decryption process. The simulation results show a reduction in execution time of around 75 percent of encoding speed for the suggested algorithms on GPU utilizing CUDA-OpenGL.

I. In 2021 [19], Eid, M. M., El-Kenawy, E.-S. M., & Ibrahim, A. The authors describe a video security method that uses the chaos system to cipher essential and vital data. They also suggest a reliable diffusion plan to address the effectiveness and security flaws of the conventional permutation-diffusion type of picture crypto systems. This method uses a chaotic map as a single necessary generator to produce the crucial data needed for the file encryption process. There is an image or video data encryption scheme depending on the spatiotemporal disorder system, and chaotic encryption has outstanding properties such as pseudo the randomness and sensitivity for initial difficulties. The chosen specs in each picture block are then encrypted using the series.

III. VIDEO ENCRYPTION

Since the time of the ancient Romans, who employed comparable techniques to ensure protection on their important information and documents, encoding has been demonstrated to be one of the most effective methods for protecting information [1] In order to avoid and detect unapproved entry, troubleshooting, the disclosure of, the disturbance of, and the configuration of computer network resources, information security can be defined as an assortment of steps, procedures, and tactics. Data encoding is the process of converting data into specific symbols by using meaningless codes.. Identical key Cryptography is a technique for both encoding and decoding data that only uses one key[1]. There are basically two types of encryption handling:

1. Symmetric cipher

In this type of encryption, it is evident that the key must be known by both the sender and the recipient; in fact, that is the secret. Of course, the distribution of the key presents the biggest challenge with this method [20]. Only one key is used for both decryption and encryption in encrypted data with a secret key. Before delivering the cipher text over to the recipient, the sender encrypts the plaintext with the key (or a set of rules). The receiver uses the same key (or rule set) to decode the message and obtain the plain text hidden key. A single key is used for both purposes, so cryptography is also known as symmetrical encryption. Prior to the invention of public-key encryption in the 1970s, the only application was Symmetric encryption is also known as traditional encryption or single-key encryption. Among the two encryption types, it is still by far the most commonly used. [21].

The Only key needs to be kept a secret; we don't need to keep the algorithm a secret. Symmetric encryption can be used widely because of this characteristic. Manufacturers have implemented encryption of data strategies in low-cost chips, as they do not need to keep the algorithm a secret. These easily obtainable chips are used in a variety of products.. The primary security issue with symmetric encryption is maintaining the key's secrecy [21] . Block cipher and stream cipher are two different types of symmetric ciphers [22].

2. **Asymmetric cipher**

Some consider the most important and recent development in cryptography in the last 300-400 years has been public-key cryptography [25]. Whitfield Diffie, a graduate student at Stanford University, and Martin Hellman, a professor, first publicly presented public key algorithms in 1976. The public key, which is accessible to everyone, and the private key, which is typically a confidential key that only the owner is aware of, are two the keys used in public key algorithms. The message is encrypted using the secret key, and it is decrypted using the public key. [23].

The Key pairs—one private key and one public key—are used in public or asymmetric key cryptography. To encrypt and decrypt a message or transmission, both are necessary. The private key is exactly that—private. It should not be confused with the key used in private key cryptography .That must not be disclosed to anyone. The key's owner is in charge of keeping it safely stored so that it cannot be misplaced or compromised .The public key, on the other hand, is exactly that—public. All users are supposed to be able to access public keys in public key cryptography. The system's strength comes from this very thing. Without the need for a prior key distribution agreement, two parties can interact securely and with little effort if they can easily obtain each other's public keys, typically through some sort of directory service[24].

An optimal video encryption method should meet certain criteria due to specific properties of digital video, which includes enormous, data, volumes, high redundancy, interactive processes, and real-time replies. Among them. Security is the most important criterion for video encryption. In today's multimedia environment, video encryption is becoming increasingly significant. In general, an encryption scheme is considered secure if the cost of decrypting it is equal to or more than the cost of obtaining video content permission. The two fundamental properties of a good cipher are confusion and diffusion, and both of these are significant features of chaotic systems as well [26].

IV. CHAOS THEORY

Edward Lorenz, a meteorologist and mathematician from MIT, made the initial discovery of chaos theory in the early 1960s while working on a weather forecast experiment. The hidden pattern in what appears to be random data is about to be explored by this hypothesis. It offers a practical method for resolving the non-linear issues of natural and artificial systems with unpredictable behaviors, such as traffic, stock markets, earthquakes, heartbeat rhythms, DNA coding sequences, weather, and climatic conditions [27].

Chaotic systems have recently substantially influenced strong cryptographic techniques. Systems have demonstrated their capacity to build very robust defenses against various threats. Systems also offer a strong blend of speed, efficiency, and security, which makes them the ideal choice for protecting digital photos. Chaotic systems have a number of intriguing properties, such as unpredictable behavior, boundedness , determinism, and great sensitivity to initial conditions [28].

Chaotic behavior in mathematics can be seen in chaotic maps, which are evolution functions. The parameterization of a map can be done with discrete-time or continuous-time parameters. Dynamical systems research typically makes use of Chaos maps, both separate and continuous. Chaotic cryptography possesses significant and profound properties that can be directly combined with traditional cryptography in order to offer a statistically attacks-resistant (i.e., secure enough) cipher. [29].

Chaotic systems are viewed as a collection of dynamical equations that change over time, where time may be discrete or continuous. Designing crypto systems can benefit from the special characteristics of chaotic systems, such as determinacy, ergodicity, and sensitivity to beginning conditions, because these characteristics are comparable to the confusion and diffusion aspects of a sound crypto system [30].

V. VIDEO ENCRYPTION WITH PARALLEL

With the continued rise in digital communications via the internet, multimedia data security is becoming more and more crucial. Various sorts of computer networks are used to transfer videos. Different encryption approaches are traditionally used to safeguard video transmission. As a result of the massive size of digital videos, they are typically transmitted in compressed form. Encryption technique algorithms have been proposed in this work[31].

Videos are simply a collection of frames. Each frame in a video is equivalent to a still image[6]. Encryption refers to The process of converting the initial information It is necessary to convert the encrypted data into a format that cannot be read by unauthorized users. There are many reliable, established encryption techniques. Exist, but the vast majority of them are unsuitable for direct video encryption. [8].

In recent years, chaos-based cryptography has grown in popularity as a means of providing effective, fast, and secure encryption. To improve security, chaos-based encryption employs repetitive steps of more than one chaotic map. However, this repetition, especially for videos, unfortunately increases processing time[18].

Parallel processing systems have been created to accelerate encryption algorithms. Particularly those with complex computations. This issue impairs the real-time use of these encryption algorithms for large image and video resolutions dividing images and videos into smaller parts that can be processed in parallel by multiple independent processing units substantially improves the encryption process [18].

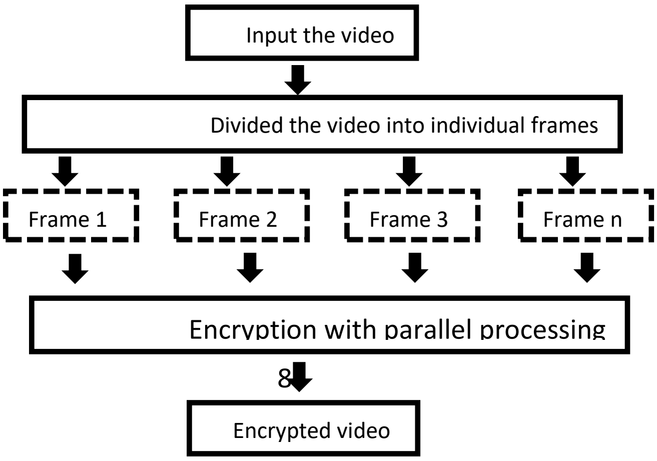
Input the video
Divided the video into individual frames
Frame 1
Frame 2
Frame 3
Frame n
Encryption with parallel processing
Encrypted video

Figure. 1 :video encryption in parallel

By using approaches for Parallel Programming. The hardware architecture, which can be shared memory, dictates the parallel processing paradigms. The idea of dividing work into discrete units and giving each core a single task to complete is present in both systems. In a shared memory architecture, each control unit (CU) and processor unit (PU) has access to a single memory. Another choice that works directly with hardware to provide the needed application with excellent speed and efficiency is parallel processing. In order to provide high-speed performance, parallel programming looks to be the best method to utilizing all of the available resources and processors [32].

In addition, to evaluate the crypto system effectiveness, speed, and security, we run a number of tests on it. All of the experiments showed that the suggested crypto system is protected against statistical and brute-force assaults. The results show that the suggested parallel crypto system sequence contains a large amount of unpredictability or uncertainty in addition to the qualities and advantages already discussed [32].

CUDA-OpenGL implementations use GPU processors to parallelize the functions of encryption and decryption on image and video frames. Parallel programming overcomes the limitations imposed by sequential computing, which governs both physical and practical factors and limits the development of faster sequential computers. Parallel programming has the advantage of scaling with problem size, allowing for the solution of larger problems. In general, parallel programming is a method of providing concurrency, specifically the simultaneous execution of multiple actions. Both substitution and diffusion methods in the video encryption method have been modified to support GPUs [18]

By using multiple stream ciphers in parallel and multi-key encryption, video encryption algorithm builds on the Video Encryption Algorithm (VEA) proposed in [12] to offer a quick, real-time encryption/decryption performance at a degree of security suitable for a number of consumer digital video applications. VEA security can be increased while maintaining encryption effectiveness using multi-key techniques [12].

A series of resynchronization groups form a resynchronization group, as depicted in Figure 2. That each use the exact same set of multi-keys, and a common-key group is a series of resynchronization groups that begin at one resynchronization point and end at the frame just before the next [12].

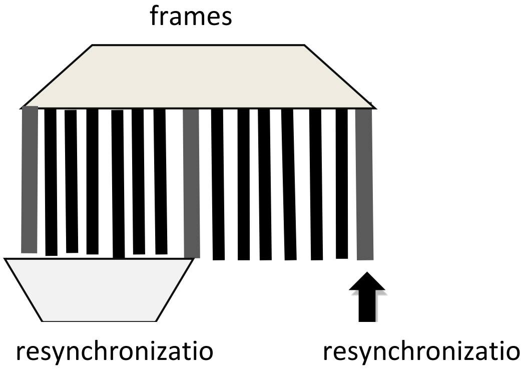

Figure 2. Depicts an example of a resynchronization group [12].

The video stream can be easily partitioned for encryption and decryption. The data components of a video frame that must be encrypted can be divided into n partitions. A stream cipher with a different key can be used to encrypt all of the partitions. Utilizing n encryption keys with m bits. Because the proposed algorithm is designed to use multiple independent stream ciphers to encrypt information of roughly equal lengths, is ideal for parallel hardware implementation [12].

Because this algorithm can be parallelized with very little overhead, and parallelization linearly speeds up the algorithm. If a content stream is divided into n different partitions that are encrypted in parallel, the ideal speedup is n times that of serial video stream encryption. Although hardware costs for parallelization rise linearly, it should be noted that stream ciphers are relatively simple to build and thus easily replicated[12].

Table 1.Video Encryption Algorithms and Their Comparative Analysis

Year	Authors	Methodology	Key features	Measurements	Results
2006	Wong, A., & Bishop, W.	Partial video encryption using stream ciphers and multi-key technique	Reduced computing burden, format compliance, experimental validation	PSNR (Peak Signal-to-Noise Ratio) was employed as a metric to assess the performance of the suggested encryption technique.	During ten test trials, the suggested algorithm's average computational overhead was found to be 2.16% of the overall computing time necessary to decrypt a video stream.
2008	Yang, S., & Sun, S	Chaotic map-based encryption on I-frames using 5 keys and 3 chaotic maps	Scrambling of DCT coefficients, double encryption, high security	Distortion test correlation coefficients of two adjacent pixels	The distortion rate caused by encryption and decryption was discovered to be 0.1%, which is incredibly modest and scarcely perceptible. These experiments show that the suggested encryption technology is secure and has

					real-time capabilities.
2008	Shang, F., Sun, K., & Cai	Chaotic cipher	Efficient MPEG video encryption scheme using a chaotic cipher. Selective encryption of FLC with the proposed chaotic stream cipher. Chaos-based permutation used for macro block shuffling in the video bit stream. Two simplest chaotic maps used to avoid floating-point arithmetic, ensuring fast encryption.	They examine the security performance against cipher-text-only attacks and known plaintext attacks and conclude that the proposed scheme is resistant to both types of attacks. They evaluate the speed of the encryption/decryption operation and the impact on the video compression ratio, and concludes that the proposed scheme has little impact on the compression ratio and meets real-time processing requirements.	Real-time processing, scalable security levels, strict size preservation, and full formation compliance. Well-suited for MPEG video applications and could be extended to other compression standards.
2015	Bowade, J. S., khade, P., & Raghuwansh, M. M	Multidimensional chaotic map-based encryption using 4D Arnold's cat map.	Shuffling mechanism, balance between security and computing time.	They examined the quality of the encrypted video data using various measures such as Entropy correlation values.	The entropy values for the original and encrypted images are 7.77138 and 7.90009, respectively. This implies that the encryption method has increased the data's unpredictability. The correlation values for the original and encrypted images are 0.923 and 0.918,

					respectively. This implies that the encryption technique has reduced the correlation between the original and encrypted image data slightly.
2017	Hamidouche, W., Farajallah, M., Ould-Sidaty, N., Assad, S. el, Déforges, O., Sidaty, N., & Deforges	Chaotic system,	the chaotic system in the scalable HEVC extension is the basis for a selective video encryption solution. Traditional stream ciphers can't compete with the strength and speed of the chaos based stream system that is being used. Parameters of SHVC encrypted with the least amount of complexity and delay. Video encryption that complies with the requirements for constant bit rate and format compliance is done at the level of the CABAC bin string. Carries over all	This involves the evaluation of various High Definition (HD) video sequences, scalability configurations, and criteria for video encryption.	Encrypting all layers or just the lowest layer achieves a high level of security, while perceptual encryption solution can be obtained by slightly lowering the quality of the highest layer. The Proposed solution's processing complexity assessed in the context of a real-time SHVC decoder. Complexity overhead remains low, accounting for no more than 6% of the total time spent decoding SHVC video sequences in real time.

			SHVC features, such as bit stream extraction for mid-network adaptation and error resistance. Three encryption schemes are put forth: first that encrypts only the bottom SHVC layer, another that encrypts all layers, and a third that encrypts only the top layer. A real-time SHVC decoder's processing complexity was evaluated..		
2018	Ibrahem, M. K., & Hamood	Chaotic sequence-based encryption using logistic maps and piecewise linear chaotic map	Macro block permutation, two-stage encryption, successful experimental validation	The article examines the use of Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) as measurement techniques for assessing the quality of video encryption and decryption processes.	The results show that the proposed approaches are secure and can achieve when the MSE value is zero and the PSNR value is at its highest, the reconstruction is perfect., demonstrating good security characteristics.
2018	Khorsheed, K. O., Abood, O. G., Guirguis, S., &	Pixel-based video encryption through rearranging pixel values	High speed, confidentiality, successful experimental validation	They just discuss "the preferred algorithm" and compare its performance to that of other existing approaches.	For all video file sizes, the suggested approach showed faster encryption and

	Guirguis, S. K			The encryption and decryption times (in seconds) for several video files of differing sizes using "MAES" and the suggested technique. The file sizes are in megabytes (MB).	decryption speeds than the MAES technique.
2019	Abdalrdha, Z. K., Shawe, R. T., Hussein, S. A., Abbas, F. N., & Ridha, A. K.	NTRU-based encryption with chaotic algorithm-based decryption	High strength, sensitivity to a starting situation, common issues resolved	They evaluated the performance of their suggested strategy using subjective evaluation as well as visual quality assessment by human observers	They also point out that their proposed technique is difficult to decode because it employs a pair separate video encoding algorithms.
2021	Elrefaey, A., Sarhan, A., & El-Shennawy, N. M.	Chaotic-based picture encryption technique using GPUs	Efficient, parallel implementation, reduction in execution time	They do not provide a specific measurement for video encryption quality. The experiments focused on encryption performance, specifically the encryption system's execution time and its applicability to both images and videos.	The experiments show that the proposed implementations perform significantly better than serial implementations of the same algorithms in their original form; results of the proposed algorithms on GPU show a 75% decrease in execution time for encryption speed
2021	Eid, M. M., El-Kenawy, E.-S. M., & Ibrahim, A	Chaotic map-based encryption with spatiotemporal disorder system	Pseudo randomness, sensitivity to initial difficulties, reliable diffusion plan	The performance of the plan is assessed based on the stream cipher's security, the affective safety of encrypted videos, and the impact on	The results show that the proposed stream cipher meets the requirement for secure encryption principles, and

				compression performance.	the encrypted photos or videos are perceived to be safe.

VI. CONCLUSIONS

Video encryption in a parallel environment holds great promise for ensuring the confidentiality and integrity of video data. This survey highlights the progress made in video encryption techniques in a parallel environment. The various encryption techniques for video encryption have been proposed, each with its own methodology and key features. PSNR, entropy, correlation values, MSE, and encryption and decryption speed were all used in studies to evaluate the performance of the encryption algorithms. The surveyed encryption techniques exhibit strong security characteristics, real-time processing capabilities, and improved encryption performance. Further research and development in this field will continue to enhance video encryption techniques, providing robust solutions for secure video transmission, storage, and playback in various domains. The findings contribute to the development of robust video encryption solutions and open avenues for further exploration in this field. By continually advancing video encryption techniques, we can ensure the confidentiality and protection of video data in various applications. The results pave the way for further research in this area and aid in the creation of reliable video encryption solutions. We can ensure the privacy and security of video data in a variety of applications by steadily improving video encryption techniques.

REFERENCES

[1] O. G. Abood and S. K. Guirguis, "A Survey on Cryptography Algorithms," in Proceedings of the International Journal of Scientific and Research Publications (IJSRP), vol. 8, no. 7, 2018, pp. 79-78, doi: 10.29322/ijsrp.8.7.2018.p7978.

[2] K. Jonathan and L. Yehuda, "Chapman & Hall/CRC Cryptography and Network Security," in Proceedings of the Chapman & Hall/CRC, n.d.

[3] X. Wang, C. L. D. J. P., "An Efficient Double-Image Encryption and Hiding Algorithm using a Newly Designed Chaotic System and Parallel Compressive Sensing," in Proceedings of the Information Sciences, Elsevier, 2022, doi: 10.1016/j.ins.2022.06.013.

[4] B. Ho Kang and B.-H. Kang, "A Review on Image and Video Processing," in Proceedings of the International Journal of Multimedia and Ubiquitous Engineering, vol. 2, no. 2, 2007, pp. 29-42, doi: 10.14257/ijmue.2007.2.2.04.

[5] M. Abomhara, O. Zakaria, and O. O. Khalifa, "An Overview of Video Encryption Techniques," in Proceedings of the International Journal of Computer Theory and Engineering, 2009, pp. 103-110, doi: 10.7763/ijcte.2010.v2.123.

[6] I. A. Baidaa Atya, A. S. Monem Rahma, and A. J. Abdul Mohsen Abdul Hossen, "Encryption of Video Images Using Arduino Card," in Proceedings of the International Journal of Scientific & Engineering Research, vol. 7, no. 7, 2016, pp. 51-56.

[7] Z. K. Abdalrdha, R. T. Shawe, S. A. Hussein, F. N. Abbas, and A. K. Ridha, "Encryption Video Using NTRU and Chaotic Algorithms," in Proceedings of the Xinan Jiaotong Daxue Xuebao/Journal of Southwest Jiaotong University, vol. 54, no. 6, 2019, pp. 22-31, doi: 10.35741/issn.0258-2724.54.6.22.

[8] M. K. Ibrahem and L. A. Hamood, "Video Encryption Based on Chaotic System and Stream Cipher," in Proceedings of the Iraqi Journal of Information and Communications Technology(IJICT), vol. 1, no. 2, 2018, pp. 12-17.

[9] A. A. Khadhim and S. A. Mehdi, "A New Image Encryption Algorithm Using a Novel High Dimensional Hyper-Chaotic System," in Proceedings of the IEEE International Conference on

Computer Science and Automation Engineering (CSAE), 2012, pp. 669-673, doi: 10.1109/CSAE.2012.6272882.

[10] Z. M. Jasim, "Image Encryption Algorithm Based On Novel Chaotic System," in Proceedings of the IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), 2019, pp. 1-

[11] P. V. HOJJAT ADELI, "Parallel Processing," COMPUTER - AIDED CIVIL AND INFRASTRUCTURE ENGINEERING, vol. 2, no. 3, 1987, pp. 183-193.

[12] A. Wong and W. Bishop, "AN EFFICIENT, PARALLEL MULTI-KEY ENCRYPTION OF COMPRESSED VIDEO STREAMS," n.d.

[13] S. Yang and S. Sun, "Video encryption method based on chaotic maps in DCT domain," Progress in Natural Science, vol. 18, no. 10, 2008, pp. 1299-1304.

[14] F. Shang, K. Sun and Y. Cai, "An efficient MPEG video encryption scheme based on chaotic cipher," Proceedings - 1st International Congress on Image and Signal Processing, CISP 2008, vol. 3, pp. 12-16, 2008, doi: 10.1109/CISP.2008.462.

[15] J. S. Bowade, P. khade and M. M. Raghuwansh, "Technique of Video encryption/scrambling using chaotic functions and analysis (Vol. 2)," 2015.

[16] W. Hamidouche, M. Farajallah, N. Ould-Sidaty, S. el Assad, O. Déforges, N. Sidaty and O. Deforges, "Real-time selective video encryption based on the chaos system in scalable HEVC extension," Signal Processing: Image Communication, vol. 58, pp. 73-86, 2017, doi: 10.1016/j.image.2017.06.007.

[17] K. O. Khorsheed, O. G. Abood, S. Guirguis and S. K. Guirguis, "Enhancing the performance of video encryption used for security and privacy protection in secure multimedia transfer Survey of Denoising Techniques in Image Processing View project Using cloud computing services to reduce power consumption in android smart phones View project Enhancing the performance of video encryption used for security and privacy protection in secure multimedia transfer," International Journal of Engineering and Technology, vol. 7, no. 4, pp. 6167-6170, 2018, doi: 10.14419/ijet.v7i4.17936.

[18] A. Elrefaey, A. Sarhan and N. M. El-Shennawy, "Parallel approaches to improve the speed of chaotic-maps-based encryption using GPU," Journal of Real-Time Image Processing, vol. 18, no. 6, pp. 1897-1906, 2021, doi: 10.1007/s11554-020-01064-w.

[19] M. M. Eid, E.-S. M. El-Kenawy and A. Ibrahim, "A New Hybrid Video Encryption Technique Based on Chaos Cryptography," Journal of Computer Science and Information Systems, vol. 2, no. 2, 2021.

[20] Mk. Msit and A. Professor, "Overview of Modern Cryptography," www.ijcsit.com.

[21] W. Stallings, Cryptography and Network Security Principles and Practices, Fourth Edition.

[22] C.-J. Kuo, "Cryptography."

[23] T. Hameed Obaida, A. Salim Jamil and N. F. Hassan, "A Review: Video Encryption Techniques, Advantages And Disadvantages (Vol. 19, Issue 1)," 2018.

[24] Ayushi, "A Symmetric Key Cryptographic Algorithm," International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 15, Volume 1.

[25] Z. Su, S. Lian, G. Zhang and J. Jiang, "Chaos-Based Video Encryption Algorithms."

[26] Raman and Ashwin, "UC Irvine UC Irvine Electronic Theses and Dissertations Title Parallel processing of chaos-based image encryption algorithms," 2016.

27] A. Id, S. Shaukat Id, A. A. Id, A. E. Id, S. Aziz, S. Id, & J. Ahmad Id, "Chaos Theory and its Application: An Essential Framework for Image Encryption," n.d.

[28] S. F. Yousif, A. J. Abboud, & H. Y. Radhi, "Robust Image Encryption with Scanning Technology, the El-Gamal Algorithm and Chaos Theory," IEEE Access, vol. 8, pp. 155184-155209, 2020.

[29] O. M. Al-Hazaimeh, A. A. Abu-Ein, M. M. Al-Nawashi, & N. Y. Gharaibeh, "Chaotic based multimedia encryption: a survey for network and internet security," Bulletin of Electrical Engineering and Informatics, vol. 11, no. 4, pp. 2151-2159, 2022.

[30] U. Zia, M. McCartney, B. Scotney, J. Martinez, M. AbuTair, J. Memon, & A. Sajjad, "Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains," International Journal of Information Security, vol. 21, no. 4, pp. 917-935, 2022.

[31] J. Shah & V. Saxena, "Video Encryption: A Survey," IJCSI International Journal of Computer Science Issues, vol. 8, no. 2, 2011.

[32] M. Abutaha, I. Amar, & S. Alqahtani, "Parallel and Practical Approach of Efficient Image Chaotic Encryption Based on Message Passing Interface (MPI)," Entropy, vol. 24, no. 4, 2022