ISSN: 2633-4828 Vol. 5 No.2, June, 2023

International Journal of Applied Engineering & Technology

A COMPREHENSIVE SURVEY AND ANALYSIS OF IMAGE ENCRYPTION TECHNIQUES FOR SECURE DATA TRANSMISSION

Mohan Manju[1*] and Dr. Rajesh Kumar Pathak[2]

[1]Research Scholar, Department of Computer Science, Shri Rawatpura Sarkar University, Raipur, Chhattisgarh, India

[2]Vice Chancellor, Department of Computer Science, Om Parkash Jogender Singh University, Rajasthan, India

ABSTRACT

This paper presents an extensive literature survey and comparative study of encryption techniques to derive the most secure force algorithm. Due to the paramount importance of encryption in cyber security, it is vital to know and identify the most robust method of encryption available. This paper systematically reviews different encryption methods through an extensive literature study followed by empirical analysis of each method. Study of strengths, weaknesses and applicability of different encryption methods based on factors like computational efficiency, crack ability and cryptographic attacks and overall effectiveness would help to better understand the choice of using the most robust algorithms for encrypting data. In summarizing the information provided in this research, paper aim to present valuable insights for the reader with regard to identification of the best encryption technique for preserving confidentiality and integrity of data while transmitting data in modern computing environments.

Keywords: *Encryption techniques, Cryptography, Cryptographic attacks, Cybersecurity.*

1. INTRODUCTION

In the contemporary digital world where hundreds of millions of data breaches and cyber-attacks occur, encryption is one key to ensuring cybersecurity. With data security being a pivotal concern for both the private and public sector in our modern digital age, encryption techniques serve to reinforce cybersecurity to keep a range of sensitive data safe from unauthorized access and data compromise, including data processed via personal devices or enterprise networks. It remains critical in this ever-changing string of cybersecurity threats to have a proper encryption method in place to protect the integrity of systems and the confidentiality and security of data. Modern cryptographic protocols form the fundamental basis of secure communications and information security in cyberspace (Kataria, Lopes, Niravil, & Keshav, 2021). These protocols harness a wide range of cryptographic insights and algorithms to enable secure communications and protect digital information from various forms of infiltration, espionage, attack and intervention. Given the computing power available today, the various problems that plagued classical encryption haven't disappeared – they've just become mostly invisible. This forces us to consider modern cryptographic procedures as almost entirely different from their classical forebears (Gong, Qiu, Deng, & Zhou, 2019). While classical encryption appeared to have only one solution – symmetric algorithms in a one-time-pad, for example – modern cryptographic procedures are much more flexible. Cryptographic protocols based on modern primitives can utilize symmetric and asymmetric encryption, hash functions and digital signatures; they can prop up almost any traditional code, and can be designed to offer security guarantees way beyond what cryptography alone could ever promise.

Asymmetric encryption, or public-key cryptography, is the other pillar of modern cryptographic protocols. Such protocols allow us to compute one-time messages on insecure channels to exchange keys for longer communications or decryption. Modern cryptography mostly employs two types of public-key cryptography: the Rivest-Shamir-Adleman (RSA) algorithm, invented by the French cryptographers Robert Rivest, Adi Shamir, and Leonard Adleman in the late 1970s, and Elliptic Curve Cryptography (ECC) (Jaryal & Marwaha, 2017).

Furthermore, a vast number of modern cryptographic protocols combine symmetric and asymmetric techniques in hybrid encryption schemes: such schemes rely on asymmetric encryption for secure key exchange and distribution, while utilizing the speed of symmetric encryption for actually encrypting and decrypting the bulk data. Real-world cryptography requires striking the right balance between the two opposing forces of security and

performance. Modern cryptographic protocols also rely on cryptographic hash functions to ensure data integrity and authentication (Ge, Chen, Chen, & Shen, 2021). A hash function takes arbitrary-length input data and outputs a fixed-size hash value. This hash value can be used to verify the integrity of the transmitted or stored data and detect any alterations. Since it was invented, modern cryptography has been upgraded to reflect newly emerging threats – the latest example to represent this trend is the case of post-quantum cryptography; the study and design of new cryptographic algorithms that immune to attacks by quantum computers, which today is one of the most important research approaches in cryptographic protocols.

This paper provides a quality review about the field of encryption techniques, and compares them in a comparative manner so that the best technique for force can be figured out. Without encryption and without the security culture we are living in the world would be in a different stage as compared to today. This is what this research is aiming to accomplish. This paper will analyze the strengths and the weakness of these techniques so that the built company can adjust the best approach for the network they make.

We will conduct a systematic review of the literature – including empirical evaluations – on an extremely wide range of encryption techniques, from classical through to modern cryptographic protocols, to determine pros and cons: under which side-channel attack, what computational resource requirement, and what application does this encryption algorithm perform best for?

Their results should give us insight into the complex world of encryption schemes, letting the world decide how to best keep their cyberspace secure. In an age where privacy and security are paramount, knowing which adversarial force algorithm is the securest can prevent sensitive data from being infiltrated by cyber attacks. With this study, we hope to provide our insight on securing cyberspace and keeping it clean from attacks to the world at large during transmitting over network.

2. OBJECTIVES

The study aims to investigate several encryption techniques, and pick the most secure force algorithm. In this digital era in which new threats such information breaches are emerging across the Internet on a daily basis urging people to take preventive measures to secure their data against modern hacking techniques. The researcher, goes across limited understanding about the security aspect of their information, and this may make them the victim of the cyber-crime. In this study, I intend to look into several encryption techniques, summarize their strengths and weaknesses, categories them, differentiate between them in addition to finding out the most secure force algorithm.

Furthermore, this research aims to address the following specific objectives:

a. To review the existing literature on encryption methods, including both classical algorithms and modern cryptographic protocols, to establish a comprehensive understanding of the landscape.

b. To classify encryption techniques based on their underlying principles and mechanisms, facilitating a structured comparative analysis.

c. To evaluate the performance, computational efficiency, and security strengths of various encryption techniques through empirical testing and benchmarking.

d. To identify key factors influencing the selection of encryption methods, such as computational overhead, resistance to cryptographic attacks, and compatibility with different applications.

e. To synthesize the findings of the comparative analysis and provide recommendations for selecting the most suitable encryption method based on specific use case requirements and security considerations.

f. To explore real-world applications and case studies showcasing the practical implementation and deployment of encryption techniques across different domains.

g. To highlight current challenges in encryption and propose future research directions to address emerging threats and advance the state-of-the-art in cryptographic security.

By fulfilling these objectives, this study endeavors to contribute to the broader discourse on cybersecurity and encryption, empowering organizations and individuals with the knowledge needed to make informed decisions about protecting their digital assets in an increasingly interconnected world.

3. CRYPTOGRAPHY

Cryptography is the practice and study of techniques for securing communication and data from adversaries. It involves encoding information in such a way that only authorized parties can access and understand it, while preventing unauthorized access or tampering (Jiao, Ye, Dong, Huang, & He, 2020). Cryptography encompasses a wide range of methods and algorithms, including encryption, decryption, hashing, and digital signatures. Encryption involves converting plaintext into cipher text using an algorithm and a key, making it unintelligible to anyone without the corresponding decryption key. Decryption, on the other hand, is the process of converting cipher text back into plaintext using the correct decryption key. Hashing is a cryptographic technique used to generate a fixed-size hash value from input data, which is commonly used for data integrity verification and password storage. Digital signatures are cryptographic mechanisms used to verify the authenticity and integrity of digital messages or documents (Song, et al., 2023). Cryptography plays a crucial role in various applications, including securing online transactions, protecting sensitive data, and ensuring the privacy of communication over networks. With the increasing prevalence of digital threats and cyber attacks, cryptography continues to evolve to address emerging security challenges and safeguard information in an increasingly interconnected world.

Types of Attack

1) ***Security Threats:*** There are a number of security threats as the first step of network security attack. The most important security threats are denying of service, disrobe deny of service attack, the viruses, Trojan horses, spywares, malwares, illegal access, randomly, erasing the recodes, the unauthorized internet access [1].

2) ***Unapproved Access:*** Access to network resources and records should have been allowed only to the approved persons. Every common file and resources in your network should be accessed only by the sanctioned persons and ought to be scanned and checked regularly [1].

3) ***Data sniffing attack and issues related to cryptography:*** Another possible attack on the network would be theft of main information, and theft of information can be blocked if you are using proper encryption technique such as 128 encryptions specify or 256 encrypt security scale. This will help in such a way when you send or receive data over FTP programs the data would not be clear and when any other gar gets have it will be useless as it won't be able to state any purpose or use of t [12].

4) ***Unauthorized installation of programs:*** In addition to the above-discussed virus and security attack prevention measures, it's helpful to limit authorized programs to install on to your set of connections, i.e., your server and all client computers. Nobody must be allowed to install any kind of program with a possibility of causing security breaches, like download any music or video programs, gaming software or any other additional internet applications.

5) ***Application-Level Attacks:*** The attacker exploits a limitation in the application layer, such as security weakness in the web server, or a control weakness in the filtering of server-side input. [13]

3.2 Image cryptography

Image cryptography – often referred to as visual cryptography – is a subfield of cryptography specifically targeted at encrypting and decrypting digital images to allow for the secure storage and transmission of digital images and photo information. Unlike text cryptography, which operates on computer character strings, the main interest of image cryptography is on the integrity, authenticity and confidentiality of digital images (one of the most

frequently encountered streams of digital data) that must be protected from tampering and misuse, as well as from unauthorized access, exposure or disclosure.

There are several techniques and approaches used in image cryptography:

a) ***Pixel-based Encryption:*** The pixels of the image are individually altered or processed according to cryptographic algorithms and keys. For example, the visual content can be obscured by substitution, permutation or XOR operations.

b) ***Visual cryptography:*** Visual cryptography is an encryption method where an image is encoded and divided into several shares or blocks; each share contributes partially to the whole picture. The different shares are distributed to authorized subsets, and, by putting together a minimum set of shares and using cryptographic functions, the original image is reconstructed(Gamido, Sison, & Medina, 2018). This cryptosystem protects the users' privacy by ensuring that each separate share of an image cannot be decoded without knowing all the other shares. Only when the predetermined threshold of shares is met can the original image be reconstructed.

c) ***Steganography:*** Secret information can be hidden inside the pixels of an image in a way that would remain hidden to even a human observer. This could be accomplished by embedding the secret data bits in the least significant bits of the image pixels, or else by exploiting the redundancies of image data.

d) ***Watermarking:*** Watermarking is a method of encoding digital watermark (a 'signature') into an image for copyright protection or for providing other authentications. Binary consensus methods become imperative for independent watermarks. It is perceptually invisible or semi-transparent, and the image can be visually unchanged. Furthermore, it can store watermarking.

Image cryptography has applications in secure image transmission across networks, digital rights management (DRM), medical image encryption to safeguard patient privacy, and verification of digital photographs to prevent falsification by malicious parties. With ever more images created and consumed every day, cryptography will play a key part in assuring the safety and integrity of visual information in our increasingly digital and connected world.

3.1.1 Process of Image Encryption

Image encryption refers to a set of computational methods to secure digital images by converting them into cipher text, as a sequence of bits, based on certain transformation policies/functions dictated by the underlying cryptographic algorithms and keys (Chaudhary, Shahi, & Neupane, 2022). As a general concept, the ultimate goal of image encryption is to preserve the confidentiality and integrity of images, to be sure that no unauthorized entity can gain the capability to view and comprehend the original image though having access to the encrypted copy of it. This is particularly important given that organizations today need to transmit or store lots of sensitive or confidential images, e.g. medical images, satellite images, confidential documents, and so forth.

The process of image encryption typically involves the following steps:

a) ***Pre-processing:*** The digital image can be normalized, resized or converted to a different color space in advance of encryption in order to achieve uniformity and compatibility with the algorithm.

b) ***Encryption:*** While encrypting, the pixel information of the photo is changed by applying cryptographic techniques, for example by substituting, permuting, confusing-diffusing, transforming and/or disarranging the data in some way, so that the image is transformed into an obfuscated state with its content irrecoverable without the decryption key.

c) ***Key Generation:*** It is necessary for encryption to have cryptographic keys which determine how image data is transformed. These can be symmetric (the same key used to both encrypt and decrypt) or asymmetric (a different key is used to encrypt and decrypt). The harder it is to predict and generate the cryptographic key, the stronger the level of encryption.

d) ***Generation of Cipher text:*** The cipher text is generated by applying the encryption algorithm and keys to the original image data. The cipher text is an image consisting of the same pixels as the original image, but in a random and scrambled order, making it unintelligible to any eye other than that of the intended recipient.

e) ***Transmission or Storage:*** The cipher text containing the encrypted image can be transmitted over unprotected communication channels or stored in registries and insecure devices without information about the sensitive visual content possibly leaking out. Only those intended legitimate recipients having the secret key to decrypt this signal are capable of recovering the original image from the ciphertext.

The protection of visual information from potential threats is of utmost importance in a wide array of applications where images are processed and shared (Gamido, Sison, & Medina, 2018). Image encryption, specifically applied to safeguard those sensitive digital files, is a viable approach to achieve socially sensitive secure digital imaging and communications. In fact, the increasing number of applications (from personal to classified), which heavily rely on visual data, calls for advanced security measures against their unlawful access and exploitation in digital communications and storing systems, as the visual and audio information nowadays are a key source of stolen information in peer-to-peer file-sharing and copyright-infringing networks.

4. IMAGE ENCRYPTION METHODS

Image encryption methods are cryptographic techniques specifically designed to protect digital image data from being viewed, tampered with, or stolen. They perform encryption on the pixel data of an image and convert it to cipher text, which is unreadable by anyone except those possessing an appropriate decryption key (Jaryal & Marwaha, 2017). There is a number of image encryption methods used in cryptography with their own distinct features, and intended for different use cases. Some of the most popular image encryption methods include:

4.1 AES (Advanced Encryption Standard)

AES can be used for image encryption by applying the AES algorithm to the pixel data of an image and then using this cipher text to secure the image from unauthorized access(Gaur, 2021). AES is a symmetric encryption algorithm used for encrypting and decrypting data blocks of fixed sizes (such as, 128 bits).

Each block is processed with

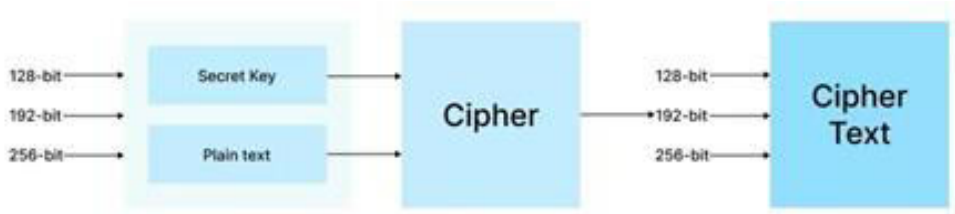

Figure 1: *AES encryption algorithm*

a symmetric key for encryption and decryption. Firstly, the digital image has to be pre-processed so that it can be adapted for the AES algorithm Secondly; the user has to generate a secure encryption key for cryptographic security. Finally, the AES algorithm is applied to the pixel data of the image using the encryption key (Kamal, Hosny, Elgindy, Darwish, & Fouda, 2021). Then, the resulting encryption of the pixel data into cipher text image where human-eye is not able to understand what the original data is.

This means if the algorithm is used correctly, an original licensed image cannot be moved to a counterfeit channel and vice versa. It also protects from potential viewing before sending to the authorized receiver, and also from getting hacked before arriving its destination.

If we want to decrypt the AES-encrypted image (i.e.: 1481411220202225158 to 11479312), the AES algorithm can be applied again by using the decryption key to provide the plaintext image data. AES for image encryption is

a method of communicating information securely, ensuring no one can view or read the information even if it is intercepted or taken.

AES can be a high-level security and eminent entity of the licensed steps to ensure that no one is able to get the original image data without an authorized decryption key, even though it is encrypted.

Because of all the advantages it provides, AES is considered as a possible way to encrypt images. Besides those advantages, there are some weaknesses to contest. One of the main advantages to use AES to encrypt images is because it has a strong cryptographic security. Proof about this is due to the fact that this encryption algorithm is considered as a robust one and it can resist to several attacks such as the brute-force attacks. AES is a widespread adopted algorithm and also standardized. Therefore, it's easy to find software and hardware developed to encrypt and decrypt images with this kind of algorithm. Moreover, AES has a strong efficiency related to the time it takes to encrypt or decrypt data, making it suitable for real-time applications, such encrypting images. Last but not least, the key length is 128, 192 and 256 bits. You can choose between 128, 192 or 256 depending on your needs for security.

However, there are some important drawbacks with using AES for image encryption. One limitation is that, because it is symmetric, both sender and recipient need to possess the same secret cryptographic key in order to communicate securely. As such, key distribution in AES can significantly complicate its use in certain applications where secure key exchange is difficult or simply not practical. Moreover, while AES is a fast and relatively efficient cipher, encrypting even moderately-sized images or processing many images at high speed can quickly lead to computational bottlenecks in resource-constrained environments. A key disadvantage with using AES as a stream cipher is that cryptographic authentication and integrity are not offered out-of-the-box, meaning that attackers could potentially tamper with, or alter, the cipher text (eg, by inserting false data) if additional mechanisms to prevent this weren't implemented.

4.2 Rivest-Shamir-Adleman (RSA)

The Rivest-Shamir-Adleman (RSA) algorithm is an asymmetric encryption algorithm. RSA provides advantages, as for any asymmetric encryption algorithm, and disadvantages too, as for any RSA encryption in absolute (Gandhi & Gor, 2022). One of the most significant advantages of RSA is the robust security that comes from the computational intractability of factorizing large composite numbers into their prime factors, which poses a formidable protection against both brute force (an exhausting search procedure of all possible keys to find the correct key) and other forms of known cryptographic attacks. In the best case, where it is correctly implemented and one makes good RSA choices, RSA encryption leads to the confidentiality, integrity and authenticity of encrypted image dataset.

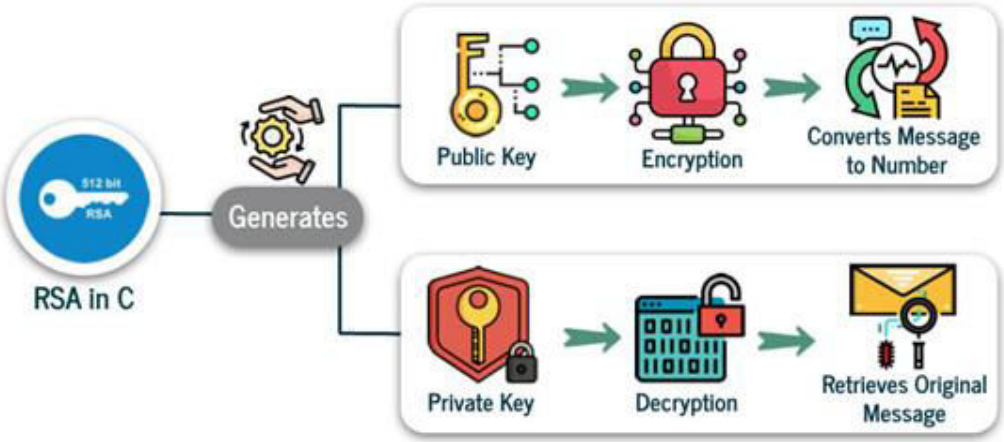

Figure 2: *Rivest-Shamir-Adleman (RSA)algorithm*

In addition to confidentiality, RSA allows for secure key exchange between users, as well as the provision of digital signatures (Sahoo, Mohanty, & Sethi, 2022). Digital signatures can add authentication and integrity to data before transmission, but it is important to note that to ensure the authenticity of the sender, signatures need to be created at the sending end and verified at the receiving end. RSA encryption not always provides real-time services. It tends to be slower than symmetric encryption algorithms like AES which can be a problem when a large image file is to be encrypted or if we have a large number of images that are to be processed in real time AND encrypted at once. RSA also requires rigorous key management to ensure that the private keys remain secure and confidential; otherwise there lies the risk that an attacker can gain access to these keys which can lead to undesirable security breaches. Despite all these drawbacks, RSA is an algorithm that is widely used and trusted. There can be no doubt in saying that RSA algorithm is widely used to secure digital images in various applications.

4.3 BLOWFISH

Blowfish encryption is a method to encrypt images by using the symmetric encryption abilities for protection of digital images from unauthorized access or tampering. Blowfish is a symmetric block cipher algorithm designed to provide high cryptographic security with good efficiency and speed (Devi, Sharma, & Rangra, 2015).

Generally speaking, there are a few steps to encrypt images using Blowfish:

Key Generation: The symmetric key created in the first step is used for Blowfish encryption. Thanks to Eric Verdin for creating this awesome image. The second step is to generate a long and random key for Blowfish encryption, which is the core to virtually all image-encryption algorithms that I know of (just ask Bill Tunstall-Pearce). That key is shown at the top of the box.

Encryption: Applying the Blowfish encryption algorithm to (block of) pixel data obtained from the image using an encryption key, Blowfish is a symmetric encryption algorithm (Singh & Singh, 2013). It works on a fixed size block of data at a time (usually 64 bits long) and it performs multiple encryptions on a single block of data. The technique involves a series of substitution and permutations of characters in a plain text block leading to an encoded text block.

Transmission or Storage: The outcome of the ciphering process is the cipher text, in which the pixel data now resides in an obscured form that's only accessible to somebody who also has the proper key. Encrypted images can be transmitted across unsecure channels, or stored inside an unreliable domain.

Decryption: With the symmetric key used in encryption, the receiver is able to decode the cipher text image. The inverse of the used Blowfish algorithm is applied, transforming the cipher text blocks to the plain text blocks and recovering the original pixels of the image.

Image encryption with Blowfish has some advantages, first of all, it is a strong crypto security, Blowfish is not vulnerable to brute-force attack and other software attacks and attacks to software as long as the protocol of implementation. Secondly, compared with other algorithms, Blowfish is fast, it is appropriate for real-time image decryption application. Last but not least, it has variable key-length, Blowfish allow user custom the level of crypto security according to requirements.

There are also certain limitations to the use of Blowfish for image encryption: Blowfish has symmetric encryption nature, use of same encryption key by sender and receiver will allows secure communication. However, for secure key exchange becomes hectic and impractical sometimes. Blowfish is fast to a certain limit whereas sending a large size image file to receiver and processing large numbers of images in real time might be a resource intensive process, which may degrade performance in the environment where are limited resources available to process the image file.

Blowfish is widely used in conjunction with other strong encryption algorithms for encrypting images, but it isn't suitable for it by itself, for various reasons. One of the main limitations is that Blowfish only allows for a

maximum key length of 448 bits. While this makes the algorithm highly secure against brute-force attacks, it might still be insufficient to protect against other common cryptographic attacks in some instances where an extremely high level of protection is required. Also, using a symmetric encryption algorithm such as Blowfish makes it challenging to securely distribute and manage encryption keys, especially in scenarios where secure key exchange is difficult. Furthermore, even though Blowfish is an efficient algorithm, by itself it does not always provide sufficient mathematical security for fully protecting encrypted images with high-dimensional pixel values, when encrypting large images or processing images in large batches in certain real-time application scenarios, as it can require significant computing resources, which in turn might give rise to performance issues in fringe resource-constrained environments. Also, while Blowfish has remained mostly safe over the years and has been well-understood by the security community from the beginning, it's been shown to be vulnerable to several attacks over time, demonstrating the importance of performing regular reviews of older encryption algorithms and updating them to address the evolved threats we face today.

4.4 CHAOTIC MAP

Encrypting the image with chaotic maps means converting the image pixel values to a more diffused form by using iterations of sensitive dependence on their initial condition in a chaotic system to perform nonlinear operations on the data. Such operations, similar to those performed by random number generators, necessarily create a pseudo-random sequence with a very high degree of randomness. In chaotic maps such as the logistic map and the Henon map, each member of the sequence depends sensitively on the preceding member, mimicking random sequences computationally. An iterative application of encrypting the image with chaotic maps means transforming the binary digits from the pixel values into increasingly complex, disordered sequences, making it progressively more difficult to break the algorithm to determine what the data represents. The initial level of security achieved by selectively using the chaotic map can be improved by iterating the encryption operation on the single-value chaotic map output. The introduction of randomness at each iteration enables the process to help spread out or shuffle around the information leading to increasingly unpredictable and encrypted data. The encryption schemes of chaotic maps are also simple and lightweight, making them candidates for feedback functions in the real world of real-time requirements.

In aggregation with its promising features, beneath the surface, a chaotic map-based encryption scheme has limitations. For one, the security of the mapping parameters could become compromised if those parameters or their associated control are not secretive or render the encryption scheme more susceptible to attack. If the parameters of the chaotic map are predictable, perhaps maybe even because the dynamics governing that chaotic map are themselves less random, then it follows that security of the encryption scheme will also in some way become 'less random'. This predictability could then allow an attacker to launch a break-in that removes disguise from the encrypted image, rendering it viewable to whoever takes the time to peek. Furthermore, deforming an image, or reducing the visual quality of the image, could reduce image intelligibility for human end-users and, as a result, render the encrypted data less useful. Adding visual artifacts, or reducing visual quality, to the encrypted image is another limitation that prevents the use of chaotic maps for all image encryption cases. If the chaotic map is aggressive in deforming the image, then the remaining visible image upon encryption may not be so useful. If the chaotic map is not aggressive about image deformation, then the secret image may be revealed, or re-encrypted, to its original form.

4.5 ARNOLD TRANSFORM

The Arnold transform is a cryptography technique to obscure the structure of an image by repeated application of a permutation and rotation operation. This transform moves the pixel locations in the image around according to a chosen map, or function, which can be iteratively applied to the image. The data doesn't move, just the relative position of the pixels, i.e., the spatial structure of the image (Song, et al., 2023). The Arnold transform obscures the location of individual pixels within the image, making it unintelligible to an unauthorized user, unless they know the exact parameter used to shuffle the pixels around in the transformation (Mansouri & Wang, 2021). The Arnold transform is an iterative mapping function, which determines the new pixel position of the output image

with reference to a starting point. This starting point might have an offset of (x0, y0) from the origin (typically the top-left pixel of the image), and the new location of a pixel can be calculated using a formula – often involving a rotation angle theta and displacement offsets *dx* and *dy*. So, by using this mapping function iteratively, the pixels in the image can be shuffled repeatedly and scrambled according to the mapping parameters.

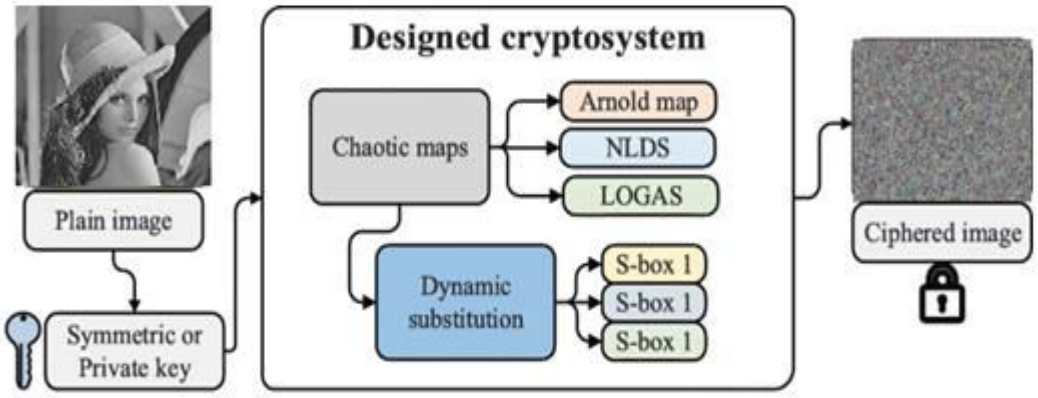

Figure 3: *Arnold transform mapping*

Figure illustrates repeated applications of the Arnold transform mapping, which successively scrambles the visual structure of the image. The output depends on the exact mapping function applied. It is interesting to note that the Arnold transform can be inverted to `unscramble' or undo the effect of the transform if the mapping parameters are known. The limitation of the Arnold transform for image encryption is that it's susceptible to a chosen-plaintext attack. In this attack, the attacker knows that the sender wants to send an image, and potentially even the type of image, such as a person's face or house (Ye, Deng, Zhang, & Yu, 2022). As the parameters needed to perform the Arnold transform, such as rotation angle and displacement offsets, need to be shared between the sender and recipient, the attacker can try shaking the image with different combinations of parameters to recover, or potentially guess, what they were. Furthermore, the Arnold transform might not apply well to modern cryptography primitives. This is due to recent attacks on image encryption, which can theoretically be applied to the Arnold transform, and progress in anti-cryptography, which could potentially reverse-engineer the parameter set used to encode an image. Furthermore, the Arnold transform can be computationally intensive, with performance depending on the quantity of image data and dimensions, and especially attacker-available computational power. This limitation can negatively affect its usability in information-sparse environments.

4.6 SEQUENCE SECURE FORCE

The Sequence Secure Force Algorithm (SSFA) for image encryption provides a cryptographic solution that secures the confidentiality of digital images. SSFA is a sequence based cryptographic method in which the pixel values of the image are mapped based upon a series of cryptographic and dynamic mathematical operations that obscure the relationship between the plain text image and the cipher text. The SSFA is an encrypting algorithm that works based upon a sequence of intermediate pseudo-random numbers that are generated based upon a cryptographic key to securely determine the permutation, substitution, and diffusion and confusion operations to be performed upon the image data. For example, the transformation operations on the sequence may include permutation, substitution, diffusion and confusion operations which further confuse the connection between the plain text and the cipher text.

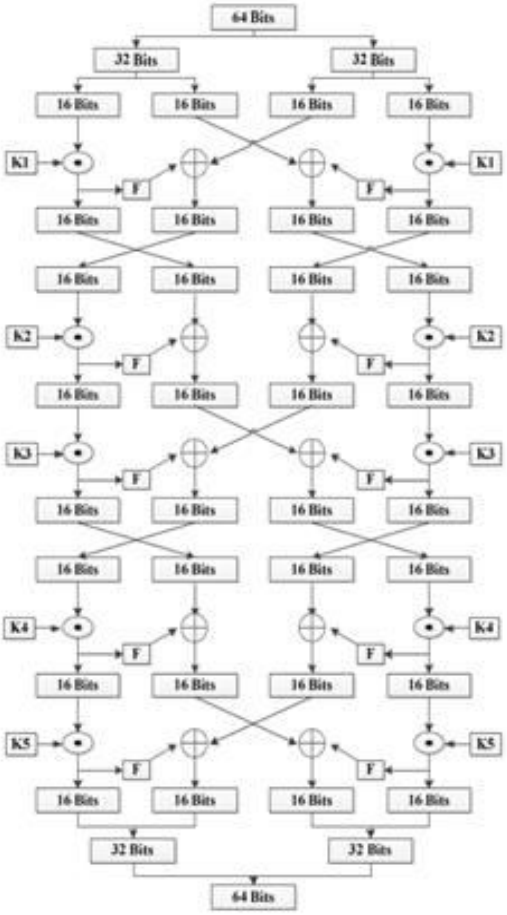

Figure 4: *Sequence secure force algorithm encryption process*

One of the major benefits of Sequence Secure Force Algorithm is achieving strong security and confidentiality of digital images. This is because SSFA encrypts the digital image using dynamic sequence and various levels of complicated computations, as well as abundant keys, all can greatly enhance the resistant level of encrypted image in cryptanalysis and brute force attacks. Meanwhile, SSFA is extensible and scalable in a wide range of operations, cipher and length. Therefore, users could freely change the cipher and the security levels when use SSFA. SSFA is both efficient and easy to be used by users, so that it can save computing time and integrate into the existing image processing systems.

However, as with most encryption algorithms, SSFA makes certain assumptions. For example, the computational overhead of performing such complicated math operations for encryption can become a bottleneck for high-resolution and large images. When we thought about the applicability of our method in a practical setting, we realized that it might not scale well. It also highlighted the importance of tamper-evident properties. We strongly advocate for security oversight of key management – for example, by suggesting that the cryptographic keys be hard-wired into the devices to ensure they cannot be accessed by malicious parties to view the encrypted images.

5. RESULTS

A comparative study of Image encryption which are AES, RSA, Blowfish, Chaotic Map, Arnold transform and Sequence Secure Force Algorithm(SSFA)the advantages and disadvantages of image encryption solutions.

Table 1: *Comparisons of existing cryptographic techniques in image*

Technique	Security Level	Computational Complexity	Key Length	Strengths	Weaknesses
Chaotic Map	Medium	Low	Variable	Non-linear, sensitive to initial conditions	Susceptible to chosen plaintext attacks
Arnold Transform	Low	Low	N/A	Simple, reversible transformation	Easily broken with sufficient computational power
AES	High	Medium	128, 192, 256	Widely adopted, strong encryption	Vulnerable to brute force attacks
RSA	High	High	1024, 2048, 4096	Public key encryption, strong security	Slower encryption and decryption compared to symmetric algorithms
Blowfish	Medium to High	Medium	32-448 bits	Fast encryption, widely used	Vulnerable to some cryptanalytic attacks
Secure Force	High	Low-Medium	256 bits	Low-complexity, energy-efficient, robust	Limited research and adoption, newer algorithm

AES is seen as a solution with robust cryptographic security and high efficiency, and therefore, suitable for real-time encryption. However, it seems that AES encryption are is going to have both key-management overhead issues and vulnerabilities if it is not implemented correctly.

This is great, because (among other things) RSA is an asymmetric encryption algorithm which is perfectly suited to the tasks of secure key exchange (e.g., HTTPS), and of digital signatures. But encryption and decryption using the RSA algorithm is nowhere near as fast as it is using a symmetric encryption algorithm (such AES or Blowfish), and if you're trying to encrypt a large image file, your RSA key is probably going to fall victim to practical limitations on the size of the key you can use: it is computationally pretty costly.

Blowfish's encryption and decryption speeds were high enough to accommodate real-time applications, while the maximum acceptable key length might not be sufficient to withstand world-class cryptographic attacks. Chaotic maps could add a degree of unpredictability and randomness to the unjumbling process, thus resisting cryptanalysis, but they could also introduce visual noise or artefacts into the encrypted image.

The Arnold transform was one of the earliest approaches for encrypting images, encrypting by reordering the pixel values in the spatial domain, or pixel positions. It still offers security against some kinds of attack (for example, against steganalysis), but it lacks security against chosen-plaintext attacks, and the repeated expansion and contraction makes for inefficient and relatively slow encryption.

Finally, image security could be improved by providing dynamic sequence-based encryption operations through Sequence Secure Force Algorithm (SSFA). However, this method also requires a computational overhead that might affect the security and scalability of the method for images of large size or high resolution.

6. CONCLUSION

Finally, in our conclusion, the comparison and contrast of several ciphers for drug imports of image encryption process such as AES, RSA, Blowfish, Chaotic map, Arnold transform, Sequence secure force algorithm is come up with here. Overall, in the battle of comparing already owned image encryption process, in accordance with the purpose. Each encryption method has own benefits and disadvantages To choose the most appropriate encryptions for their own purpose.AES is very secure and efficient for encryption purposes in real-time applications, RSA on the other hand is slower to encrypt data but it's very secure for exchange of keys and digital signatures, although

these same features can be accomplished with other encryption algorithms. Blowfish is fast to encrypt and decrypt but its maximum key length may not be long enough for using it against complex attacks. Chaotic maps add randomness and complexity to functions that help against cryptanalysis but would cause visual distortion when encrypting images. The Arnold transform performs encryption in a very different manner in space, while SSFA is provably very secure and scalable. Yet both might incur computational overheats and be impractical in certain situations, as can be seen in this comparative analysis. Overall, the comparative analysis underscores the importance of considering factors such as security, efficiency, scalability, and practical limitations when selecting an image encryption method.

Nonetheless, image crypto-systems still require extensive research and development for efficiency optimization and secret-key management in both theoretical and engineering aspects, such as the computational overhead on the sender and receiver, the practical storing and sharing of secret-key, and the security issues against new cryptographic attacks. Bridging the strengths of different encryption algorithms and reducing their weaknesses will be a promising trend for the development of more practical and secure image-encryption techniques to protect valuable images and videos in various applications.

7. ACKNOWLEDGEMENTS

Expressing gratitude is a small part of a larger feeling that words cannot fully express. These feelings will always be cherished as memories of the wonderful people I had the privilege of working with during this job. I would like to express my heartfelt gratitude to Shri Rawatpura Sarkar University, Raipur, Chhattisgarh, India for the environment which helped me in completing this work.

I express my deep and sincere appreciation to my supervisor Professor Dr. Rajesh Kumar Pathak. His extensive knowledge and systematic approach to problem solving was incredibly valuable to me. His understanding, encouragement and personal guidance laid a solid foundation for completing this project.

AUTHOR CONTRIBUTIONS

In this collaborative research endeavor, both authors played integral roles in exploring and analyzing various image encryption methods. Author 1 undertook the task of conducting an extensive literature review, delving into the intricacies of encryption techniques such as AES, RSA, Blowfish, Chaotic Map, Arnold transform, and the Sequence Secure Force Algorithm (SSFA). Meanwhile, Author 2 focused on hands-on experimentation, carrying out simulations to evaluate the performance and effectiveness of these methods. Together, they synthesized their findings, contributed to the development of comparative analyses, and collaborated on crafting clear and insightful conclusions. Through their combined efforts, this paper offers a comprehensive examination of image encryption methods, providing valuable insights for both academic researchers and industry practitioners alike.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

8. REFERENCES

Agarwal, S. (2023). Review of Image Encryption Techniques. *INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT, 07*(04). doi:10.55041/ijsrem21900

Alexan, W., Elkandoz, M., Mashaly, M., Azab, E., & Aboshousha, A. (2023). Color Image Encryption Through Chaos and KAA Map. *IEEE Access, 11*. doi:10.1109/ACCESS.2023.3242311

Castro, F., Impedovo, D., & Pirlo, G. (2023). A Medical Image Encryption Scheme for Secure Fingerprint-Based Authenticated Transmission. *Applied Sciences (Switzerland), 13*(10). doi:10.3390/app13106099

Chaudhary, N., Shahi, T. B., & Neupane, A. (2022). Secure Image Encryption Using Chaotic, Hybrid Chaotic and Block Cipher Approach. *Journal of Imaging, 8*(6). doi:10.3390/jimaging8060167

Devi, A., Sharma, A., & Rangra, A. (2015). A Review on DES, AES and Blowfish for Image Encryption & Decryption. *International Journal Of Engineering And Computer Science, 4*(6).

Elkandoz, M. T., & Alexan, W. (2022). Image encryption based on a combination of multiple chaotic maps. *Multimedia Tools and Applications, 81*(18). doi:10.1007/s11042-022-12595-8

Gamido, H. V., Sison, A. M., & Medina, R. P. (2018). Implementation of modified aes as image encryption scheme. *Indonesian Journal of Electrical Engineering and Informatics, 6*(3). doi:10.11591/ijeei.v6i3.490

Gandhi, S., & Gor, R. (2022). DIGITAL IMAGE ENCRYPTION USING RSA AND LFSR. *International Journal of Engineering Science Technologies, 6*(4). doi:10.29121/ijoest.v6.i4.2022.351

Gaur, P. (2021). AES Image Encryption (Advanced Encryption Standard). *International Journal for Research in Applied Science and Engineering Technology, 9*(12). doi:10.22214/ijraset.2021.39542

Ge, B., Chen, X., Chen, G., & Shen, Z. (2021). Secure and Fast Image Encryption Algorithm Using Hyper-Chaos-Based Key Generator and Vector Operation. *IEEE Access, 9*. doi:10.1109/ACCESS.2021.3118377

Gong, L., Qiu, K., Deng, C., & Zhou, N. (2019). An optical image compression and encryption scheme based on compressive sensing and RSA algorithm. *Optics and Lasers in Engineering, 121*. doi:10.1016/j.optlaseng.2019.03.006

Jaryal, S., & Marwaha, C. (2017). Comparative Analysis of Various İmage Encryption Techniques. *International Journal of Computational Intelligence Research, 13*(2).

jasim, Z. M. (2020). Image Encryption Using Modification Blowfish Algorithm. *International Journal of Advances in Scientific Research and Engineering, 06*(03). doi:10.31695/ijasre.2020.33759

Jiao, K., Ye, G., Dong, Y., Huang, X., & He, J. (2020). Image Encryption Scheme Based on a Generalized Arnold Map and RSA Algorithm. *Security and Communication Networks, 2020*. doi:10.1155/2020/9721675

Kamal, S. T., Hosny, K. M., Elgindy, T. M., Darwish, M. M., & Fouda, M. M. (2021). A new image encryption algorithm for grey and color medical images. *IEEE Access, 9*. doi:10.1109/ACCESS.2021.3063237

Kataria, S., Lopes, E. J., Niravil, B. M., & Keshav, S. (2021). IMAGE ENCRYPTION TECHNIQUES AND COMPARATIVE ANALYSIS. *International Research Journal of Engineering and Technology*.

Khan, P. W., & Byun, Y. (2020). A blockchain-based secure image encryption scheme for the industrial internet of things. *Entropy, 22*(2). doi:10.3390/e22020175

Mansouri, A., & Wang, X. (2021). Image encryption using shuffled Arnold map and multiple values manipulations. *Visual Computer, 37*(1). doi:10.1007/s00371-020-01791-y

Patil, S. S. (2023). IMAGE ENCRYPTION AND DECRYPTION USING AES ALGORITHM. *INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT, 07*(04). doi:10.55041/ijsrem19004

Priyanka, & Singh, A. K. (2023). A survey of image encryption for healthcare applications. *Evolutionary Intelligence, 16*(3). doi:10.1007/s12065-021-00683-x

Sahoo, A., Mohanty, P., & Sethi, P. C. (2022). Image Encryption Using RSA Algorithm., *431*. doi:10.1007/978-981-19-0901-6_56

Sekar, J. G., & Arun, C. (2020). Comparative performance analysis of chaos based image encryption techniques. *Journal of Critical Reviews, 7*(9). doi:10.31838/jcr.07.09.209

Singh, P., & Singh, K. (2013). Image Encryption and Decryption Using Blowfish Algorithm in Matlab. *International Journal of Scientific & Engineering Research, 4*(7).

Song, W., Fu, C., Zheng, Y., Tie, M., Liu, J., & Chen, J. (2023). A parallel image encryption algorithm using intra bitplane scrambling. *Mathematics and Computers in Simulation, 204*. doi:10.1016/j.matcom.2022.07.029

Ye, J., Deng, X., Zhang, A., & Yu, H. (2022). A Novel Image Encryption Algorithm Based on Improved Arnold Transform and Chaotic Pulse-Coupled Neural Network. *Entropy, 24*(8). doi:10.3390/e24081103

Zhang, B., & Liu, L. (2023). Chaos-Based Image Encryption: Review, Application, and Challenges. *Chaos-Based Image Encryption: Review, Application, and Challenges, 11(11)*. doi:10.3390/math11112585

Zolfaghari, B., & Koshiba, T. (2022). Chaotic Image Encryption: State-of-the-Art, Ecosystem, and Future Roadmap. *Chaotic Image Encryption: State-of-the-Art, Ecosystem, and Future Roadmap, 5(3)*. doi:10.3390/asi5030057

ABOUT THE AUTHORS

Mrs. Mohan Manju is a Ph.D. Research Scholar, Department of Computer Science from Shri Rawatpura Sarkar University, Raipur, Chhattisgarh, India. She is working as an Assistant Professor, Department of Computer Science & IT, Kamla Nehru Mahavidyalaya, Korba, Chhattisgarh, India accredited by NAAC and affiliated to Atal Bihari Vajpayee Vishwavidyalaya, Bilaspur, Chhattisgarh, India. She has 13yrs of Teaching Experience and managing projects in academic level and giving sessions on different subjects like Computer Architecture, Operating System, Software Engineering, JAVA, Cryptography and Network Security, Oracle, Visual Basic, etc. and handling Projects. She holds Masters in Computer Application.

Dr. Rajesh Kumar Pathak is currently working as a Vice Chancellor in Om Parkash Jogender Singh University, Rajasthan, India. He worked as the Director in Greater Noida, Institute of Technology (GNIOT)and his key role was of administrator, researcher, academician and motivator and been worked as a Vice Chancellor at Shri Rawatpura Sarkar University, Raipur Chhattisgarh, India. He holds Doctorate in Computer Science with 20 years of experience in academic and administrative. Prior to this, gained experience as Pro Vice Chancellor and campus Director in Shri Venkateshwara University, Meerut campus and as an Advisor in Vishveshwarya Group of Institution.

He had been worked as Group Director (Vishveshwarya Group of Institution) and as a Professor and Head of Department of CSE, coordinator of M. Tech (CSE) and CEOSCA (center of excellence for open source computing and application at Greater Noida Institute of Technology, Gr. Noida. Also worked as a Dean and HOD (CSE) at SIET Pilkhwa Ghaziabad and A.P. in Department of CSE at ABES Engineering College Ghaziabad taught different subjects such as Operating System, data mining, etc. and other role to get involved to motivate students for their future career guidance.