Quest Journals
Journal of Electronics and Communication Engineering Research
Volume 4 ~ Issue 1 (2018) pp: 24-29
ISSN(Online) : 2321-5941
www.questjournals.org

Research Paper

Examining Encryption Algorithms in Encrypted Images: Multiple Approaches

Chanbasappa Patil [1], Arunkumar [2], Bharati [3]
[1, 2, 3] *Lecturer, Department of Electronics and Communication Engineering, Government Polytechnic Bidar, Karnataka, India.*

Abstract:
Trends in online communication are evolving at a dizzying rate. The internet has made it possible to establish an international "Virtual Community" that is unconstrained by space and time. Anyone may now easily connect with experts all across the globe thanks to the internet. Electronic mail, phone, or video mail may be used to seek the advice of experts. With no longer any assurance of privacy whether using wired or wireless ways, the Internet has evolved into a hostile environment. The challenge with transmitting multimedia material online is keeping it secure and private. As the need for fast data transmission and storage continues to rise, multimedia applications are confronted with the challenge of excessive bandwidth usage. Information security, data transmission, storage, and protection, especially on networks, need data compression and encryption. Images should be encrypted prior to compression in order to provide maximum security. Our three techniques for grayscale photo encryption are Arnold Transform, Combinatorial Random Permutations, and Cyclic Permutation of Prediction Errors. Arnold Transform use linear transformation and mod function iteration to reposition pixels, therefore encrypting the image. The link between nearby pixels is completely broken after many repetitions. To make data encryption as foolproof as possible, the Combinational Random Permutation method mixes bits, pixels, and blocks. The Cyclic Permutation of Clusters of Prediction Errors method encrypts the region of prediction errors rather than the actual image, which results in high security.

Keywords: *Encryption, Algorithm, Encrypted Image, Information Security, online communication.*

I. Introduction

The process of guaranteeing the security of the network is one of the most critical activities that must be completed throughout the process of information transmission over the network. Applications of the encryption of photos or videos may be found in a broad range of fields of study. The use of cryptography is one way that may be applied in order to guarantee the secrecy of data transfers. When this approach is used, the information that is going to be conveyed will be converted into a format that is unreadable. This will guarantee that only authorized persons will be able to recover the information in an accurate manner. There are two different approaches to encryption: symmetric key cryptography and asymmetric key cryptography. Both of these approaches may be applied to successfully complete the encryption process. "Symmetric key cryptography" is a word that describes the situation that arises when the same key is used for both the encryption and decryption processes. On the other hand, another kind of cryptography known as "asymmetric key cryptography" describes the situation that arises when a separate key is used for both the encryption and decryption processes.

Communication that is encrypted is essential to the protection of personal privacy, the effectiveness of organizations, and the safety of society. There are many different circumstances in which its significance may be found, including the protection of sensitive information, the guarantee of confidence in digital systems, and the prevention of cybercrime. The following are some of the most important reasons why secure communication is so important:

1.1 **Protection of Sensitive Information**

- **Personal Privacy**: Secure communication protects individuals' personal data (e.g., financial details, medical records) from being intercepted or stolen.
- **Corporate Security**: Businesses rely on secure communication to protect trade secrets, customer data, and strategic plans from competitors or malicious actors.

- **National Security**: Governments require secure channels to safeguard classified information and maintain national security.

1.2. Prevention of Cybercrime

- Cybercriminals often target unsecured communications to exploit data for financial gain, identity theft, or other malicious purposes.
- Encrypted communication prevents eavesdropping, phishing, and man-in-the-middle attacks, reducing vulnerabilities.

1.3. Ensuring Trust in Digital Interactions

- Secure communication protocols (e.g., HTTPS, TLS) establish trust between users and systems, ensuring authenticity and reliability.
- Encryption assures users that their information is safe, fostering confidence in online services like banking, e-commerce, and social networking.

1.4. Legal and Regulatory Compliance

- Many industries are governed by strict data protection laws (e.g., GDPR, HIPAA) that mandate secure communication practices.
- Organizations that fail to secure communications risk legal penalties, reputational damage, and loss of consumer trust.

1.5. Facilitating Confidentiality and Integrity

- Confidentiality ensures that information is accessible only to authorized parties.
- Integrity ensures that data is not altered during transmission, maintaining its accuracy and reliability.

1.6. Mitigating Risks in Emerging Technologies

- As technologies like IoT, AI, and 5G grow, secure communication is essential to prevent vulnerabilities in interconnected systems.
- Blockchain and cryptographic protocols play a critical role in securing communications in decentralized systems.

Existing Compression-Then-Encryption [CTE] system

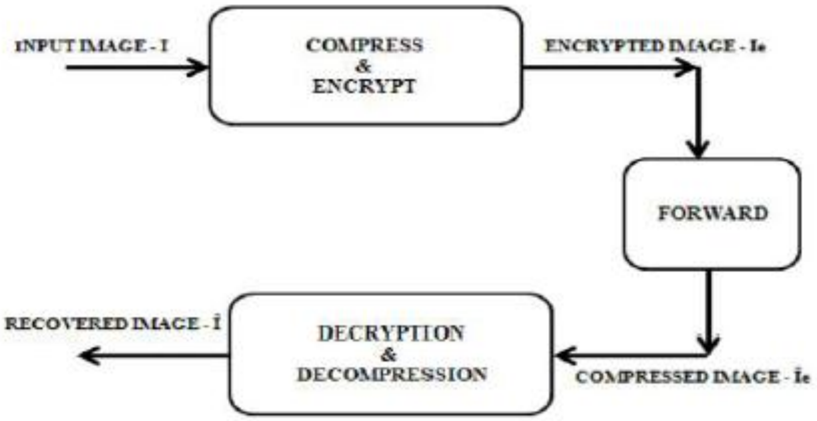


Fig. 1 a shows block diagram of CTE system.

Figure 1 is a representation of the block diagram of the existing CTE system. Within this framework, a transmitter is responsible for transmitting an image 'I' to a receiver in a manner that is not only safe but also effective. It is via a channel provider that cannot be trusted that the broadcast would take place. The information is first compressed into Ie by the transmitter using an encryption function known as EK(.), where 'K' stands for the secret key. This is done before the information is encrypted into Ie. Following this, the data that has been encrypted is transferred to the channel in order for it to be sent to the receiver. Decryption and decompression of the image Ie will be carried out in a sequential fashion by the receiver in order to get a reconstructed picture Ie. CTE, which stands for compression-then-encryption, is a paradigm that is capable of meeting the criteria in a wide variety of situations that include secure transmission. When a transmitter is continually concerned with safeguarding the privacy of the image data by encrypting it, however, the order in which compression and encryption are performed may need to be reversed in some cases. This is because encryption is always used to protect the data. However, the transmitter does not have any need to compress the data or carry out a compression procedure before encrypting the data. This is because the data is already encrypted. The next step is for the channel provider to compress all of the network traffic in order to make the most efficient use of the network. Because of this, compression was carried out at the channel, which is a system that is known as an ETC system.

II. LITERATURE SURVEY

The following is a summary of the pertinent research that have been undertaken on picture encryption and compression algorithms that we have deployed for the purpose of comparative performance analysis. In order to generate an encrypted image, the picture encryption approach makes use of the intrinsic features of pictures, such as high redundancy and strong spatial correlation, in conjunction with diffusion characteristics. The properties of Arnold's cat map are investigated by means of an image encryption method that makes use of Arnold's Transform, as described in [1]. Arnold's cat map is a basic discrete system that convolutes and distorts pathways in phase space. It is also known as the "cat map." As a result of the fact that Arnold's Cat Map is the one in which the scrambling effect is most successful, the approach that has been described is useful for encrypting pictures. Using the concepts of linear algebra, the Arnold Cat Map is able to modify the placements of pixel values in the original picture, so generating an encrypted image. The author of [2] used the exclusive OR operation in combination with the Arnold Transform to produce scrambled images. As a result, the author was able to improve the security and resilience of the cryptosystem by including numerous diffusions into the encryption scheme. Within the context of [3], the author made use of the Logistic map in order to improve the safety of the Arnold transformer technique. There is a general form of the chaotic map that is represented by the logistic map. Unpredictability is what the word "chaos" refers to, and the study of nonlinear dynamic systems is what gives the term its definition. A chaotic map is a simple, unstable dynamic system that is characterized by a high sensitivity to the conditions that were present at the beginning of the process. The chaos-based encryption method provides an extremely safe method of encrypting pictures. This research [3] is based on the core principle of transforming the image into chaotic map variables on a pixel-by-pixel basis. This is accomplished by iterating a chaotic map with certain initial conditions. The traditional Arnold transform-based approaches described in [1-3] all have a common restriction, which is that the height and width of the image must be the same. A strategy for encrypting images is developed by the author in [4] by combining the Arnold transform with three stochastic strategies: random division, iterative number generation, and encryption order construction. This is done in order to solve the constraints of the Arnold transform. Random techniques are the foundation upon which this method's security is built. This method, which has its origins in the Arnold transform, may be used for the encryption of photographs of any dimensions. As a consequence of this, the recommended approach is more secure and has a wider range of applications as compared to the conventional Arnold transform.The processes of encryption and decryption are often guided by specific keys, which may be the same or may be derived from one another in a straightforward manner. The cryptographic methods that are being discussed here fall under the category of private key cryptography. The research presented in [5] focuses on the development of improved private key cryptography techniques for the purpose of ensuring security. More specifically, the study focuses on the fabrication of private key cryptographic strategies that make use of permutation approaches. The author of [6] proposes the development of pseudo-random sequence generators for the purpose of synthesizing binary sequences for cryptographic reasons. This would result in a major improvement in the performance of information coding. A innovative technique for encrypting images is presented in the research paper [7], which utilizes a combination of multiple different permutation strategies. The fundamental idea that underpins this investigation is that the information that can be understood in an image is derived from the correlations that exist between the bits, pixels, and blocks that are arranged in a certain arrangement. By decreasing the link between these two variables via the use of certain permutation tactics, this discernable information may be reduced. For the purpose of security applications, it has been shown that a random combination strategy that makes use of all three strategies is beneficial. As a consequence of this, the design of private key cryptography systems is investigated in [7], with an emphasis placed on the relevance of permutation methods as crucial components alongside pseudo-random sequence generators for the selection of a particular permutation key from a preset range of valid keys. CALIC, which stands for context-based adaptive lossless image coding, is a concept that is suggested in [8]. One of the distinguishing features of CALIC is that it makes use of many modeling contexts in order to condition a non-linear predictor. This, in turn, makes it more adaptable to changing source data. CALIC makes use of a unique gradient-based non-linear predictor known as GAP. This predictor alters prediction coefficients in accordance with local gradient estimates. According to the findings of the research presented in [9], stream cipher encrypted data may be compressed by using coding with side information principles, without compromising the efficiency of the compression process. Furthermore, the approach that was published in [9] was employed in the prediction error domain, which eventually led to higher lossless compression performance for encrypted grayscale and color photos, as described in [10].

III. PARAMETERS FOR THE EVALUATION OF AN ENCRYPTION ALGORITHM

3.1. Security

- **Key Length**: A longer key generally provides greater security by increasing the difficulty of brute-force attacks. For example, AES allows 128, 192, and 256-bit keys.

- **Resistance to Cryptanalysis**: The algorithm must withstand various types of cryptanalysis (e.g., linear, differential, and algebraic attacks).
- **Randomness and Entropy**: The algorithm should produce outputs with high randomness, making patterns difficult to detect.
- **Forward and Backward Secrecy**: If part of the encrypted data or key is compromised, it should not compromise past or future messages.
- **Resilience to Side-Channel Attacks**: Protection against attacks that exploit timing, power consumption, or electromagnetic leakage.

3.2. Performance

- **Computational Efficiency**: The time complexity of encryption and decryption operations must be low enough for practical use, especially in resource-constrained environments (e.g., IoT devices).
- **Memory Requirements**: The algorithm's demand for RAM and storage should be evaluated, particularly for devices with limited resources.
- **Throughput**: The amount of data processed per unit time, especially for real-time applications like video streaming or secure web browsing.

3.3. Flexibility

- **Scalability**: Support for varying key sizes and modes of operation to meet different security requirements.
- **Adaptability**: Compatibility with diverse platforms, such as hardware implementations (e.g., FPGAs, ASICs) and software environments.

3.4. Implementation Feasibility

- **Ease of Implementation**: Simplicity in design and coding minimizes bugs and vulnerabilities.
- **Standardization**: Adoption of international standards (e.g., NIST-approved algorithms like AES) ensures trust and interoperability.
- **Availability of Libraries**: Existence of well-tested, optimized libraries for developers.

3.5. Energy Efficiency

- For mobile devices or IoT systems, the algorithm should consume minimal power during encryption and decryption processes.

3.6. Scalability and Multi-Platform Support

- The algorithm should perform well on different devices and architectures, from low-power IoT devices to high-performance servers.

3.7. Interoperability

- The algorithm should integrate seamlessly with existing communication standards, protocols, and systems.

3.8. Cryptographic Functionality

- **Support for Modes of Operation**: Ability to work with CBC, CTR, GCM, etc., for different encryption needs (e.g., authenticated encryption).
- **Key Management**: Features for securely generating, storing, and exchanging keys.

3.9. Resistance to Future Threats

- **Post-Quantum Resistance**: Evaluation of whether the algorithm can withstand attacks from quantum computers, a growing area of concern.

3.10. Compliance and Certification

- Algorithms should comply with relevant standards like FIPS 140-2, ISO/IEC 18033, or NIST recommendations.

Practical Evaluation Steps:

- Conduct **theoretical analysis** to study resistance to known attacks.
- Perform **benchmarking** in different scenarios (e.g., on servers, mobile devices).
- Analyze real-world implementations for **side-channel vulnerabilities**.

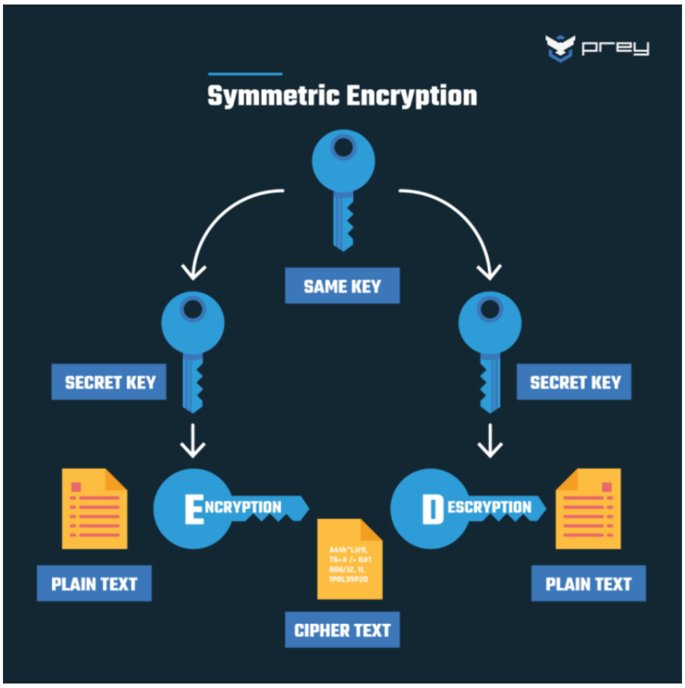


Fig. 2 Encryption choices.

By evaluating encryption algorithms against these parameters, developers and organizations can select the most suitable option for their security needs.

IV. SIMULATION RESULTS

The purpose of this chapter is to give the simulation results of parameters that were mentioned in the previous chapter for the Encryption-then-Compression Algorithms that were explained before. Additionally, this chapter draws conclusions about the efficiency of these algorithms with relation to the safety of a cryptosystem.

One of the most important things that must be done in order for a cryptosystem to operate well is to carry out statistical analysis on pictures that have been encrypted. What this means is that the ideal encrypted image should be resistant to any statistical attacks that may be launched against it. A number of statistical tests are carried out in order to establish that any Image Encryption Algorithm is, in fact, secure. Some of these tests are listed below.

Sample IMAGES

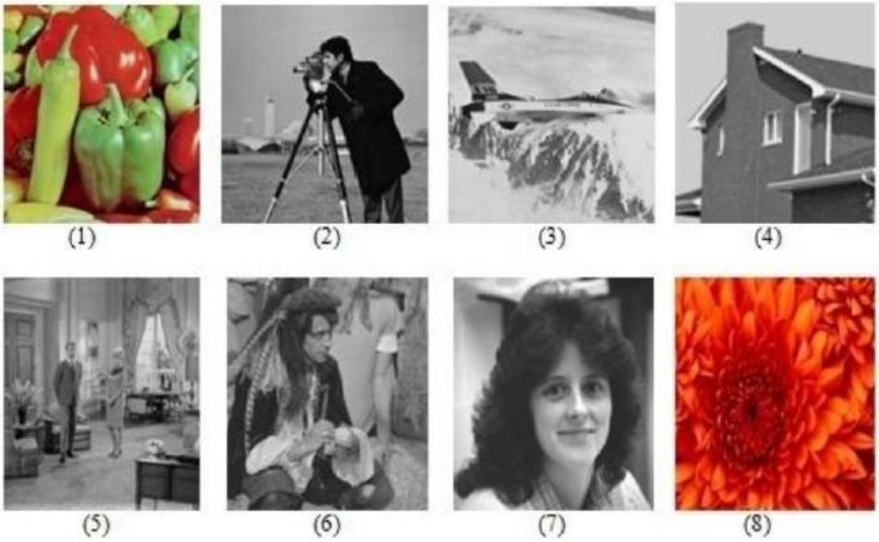
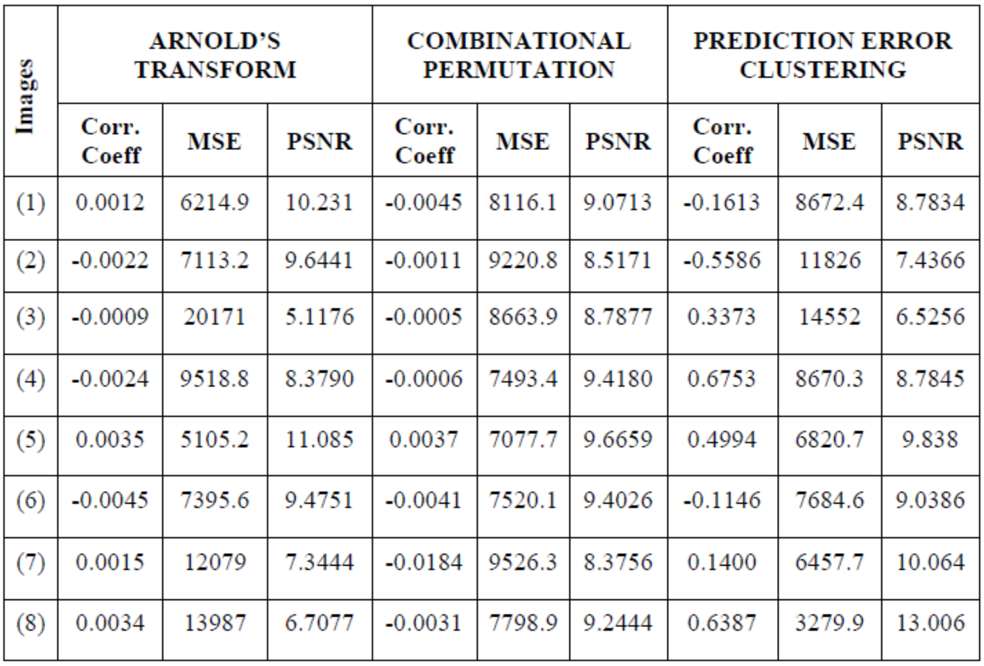


Fig. 3 shows sample images of size 256X256, (a) Pepper (b) Camera man (c) Jet plane (d) House (e) Living Room (f) Pirate (g) Women with dark hair (h) Flower.

Table 1: Shows the statistical parameters measured for the sample images:



Images	ARNOLD'S TRANSFORM			COMBINATIONAL PERMUTATION			PREDICTION ERROR CLUSTERING		
	Corr. Coeff	MSE	PSNR	Corr. Coeff	MSE	PSNR	Corr. Coeff	MSE	PSNR
(1)	0.0012	6214.9	10.231	-0.0045	8116.1	9.0713	-0.1613	8672.4	8.7834
(2)	-0.0022	7113.2	9.6441	-0.0011	9220.8	8.5171	-0.5586	11826	7.4366
(3)	-0.0009	20171	5.1176	-0.0005	8663.9	8.7877	0.3373	14552	6.5256
(4)	-0.0024	9518.8	8.3790	-0.0006	7493.4	9.4180	0.6753	8670.3	8.7845
(5)	0.0035	5105.2	11.085	0.0037	7077.7	9.6659	0.4994	6820.7	9.838
(6)	-0.0045	7395.6	9.4751	-0.0041	7520.1	9.4026	-0.1146	7684.6	9.0386
(7)	0.0015	12079	7.3444	-0.0184	9526.3	8.3756	0.1400	6457.7	10.064
(8)	0.0034	13987	6.7077	-0.0031	7798.9	9.2444	0.6387	3279.9	13.006

V. CONCLUSIONS

The goal of this project is to encrypt grayscale images using three different techniques. The algorithm's robustness, flexibility, adaptability, and security are shown experimentally via the use of statistical evaluation parameters. Arnold's change approach exemplifies the qualities listed before, such as dependability, flexibility, and security. However, the apps can only handle images with the same size and processing speed.

The integration of many permutation algorithms was easy to implement. Bit permutation reduces correlation, while pixel and block permutation greatly improve security. As a result, the sensory data was decreased due to the random combination of all three variations. The findings show that the encrypted picture's histogram is uniformly distributed, which means that the proposed method is resistant to frequency analysis assaults. According to the results of the experiments, this approach is faster and more secure than the current methods.

It has concluded that the quality of image encryption is adequate when compared to method III, as the correlation coefficient in methods I and II is almost nil, according to the results of the statistical analysis displayed in table 1. This approach outperforms all others, despite a lower correlation coefficient. The encrypted picture's PSNR and MSE are calculated and compared to the original image. Table 1 shows that all three algorithms may be used for efficient encryption since their decibel levels are less than 15 dB.

References

[1]. Gabriel Peterson, "Arnold's Cat Map", Math 45 – Linear Algebra, Fall 1997.

[2]. L. Zhu, W. Li, L. Liao, and H. Li, "A novel algorithm for scrambling digital image based on cat chaotic mapping," In: Proc. of IIH-MSP '06, pp.601–604, 2006.

[3]. Z. Shang, H. Ren, and J. Zhang, "A block location scrambling algorithm of digital Image based on Arnold transformation," In: Proc. Of the 9th International Conference, pp. 2942–2947, 2008.

[4]. Zhenjun Tang, Xianquan Zhang, "Secure Image Encryption without Size Limitation using Arnold transform and Random Strategies," Journal of Multimedia, Vol. 6, No. 2, April 2011.

[5]. P.P. Dang and P. M. Chau, "Image Encryption for Secure Internet Multimedia applications," IEEE Trans. Consumer Electronics, vol. 46, no. 3, pp. 395-403, Aug. 2000.

[6]. A. Fuster and L. J. Garcia, "An efficient algorithm to generate binary sequences for cryptographic purposes," Theoretical Computer Science 259, pp. 679-688, 2001.

[7]. Mitra, Y.V. Subba Rao and S.R.M. Prasanna, "A New Image Encryption Approach using Combinational Permutation Techniques", International Journal of Electrical and Computer Engineering, 1:2 2006.

[8]. X. Wu and N. Memon, "Context based adaptive lossless image codec," IEEE Trans. Communication, vol. 45, no. 4, pp. 437– 444, Apr. 1997.

[9]. M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On Compressing encrypted data," IEEE Trans. Signal Process., vol. 52, no. 10, pp. 2992–3006, Oct. 2004.

[10]. A. Kumar and A. Makur, "Distributed source coding based encryption and lossless Compression of gray scale and color images," in Proc. MMSP, 2008, pp. 760–764.