IMAGE ENCRYPTION USING A VARIETY OF PERMUTATION TECHNIQUES AT NUMEROUS LEVELS

Sowmya R [1], Asmath A [2], Asma Banu S [3]

[1] Department of Electronics and Communication Engineering, Government Polytechnic for Women Hassan, Karnataka, India.
[2] Department of Electronics and Communication Engineering, Government Polytechnic Kushalnagar, Karnataka, India.
[3] Department of Electronics and Communication Engineering, Government polytechnic Bagepalli, Karnataka, India.

ABSTRACT :

The expansion of online communication is happening at a dizzying pace. 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. You may ask for advice from experts by video chat, voicemail, or email. 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. The increasing need for fast data transmission and storage has put multimedia apps in a precarious position, since they use a lot of bandwidth. Encryption and compression of data are essential for data security, safeguarding data resources during transmission and storage, especially on networks. Encrypting images before compression is necessary for high-level security. Arnold Transform, Combinatorial Random Permutations, and Cyclic Permutation of Prediction Errors are the three techniques that we provide for grayscale photo encryption. By repeatedly applying linear transformations and mod functions to different pixel places, Arnold Transform is able to encrypt data. When iterations are performed several times, the relationship between adjacent pixels is completely broken. To make data encryption as foolproof as possible, the Combinational Random Permutation method mixes bits, pixels, and blocks. By encrypting the prediction error domain rather than the actual image, the Cyclic Permutation of Clusters of Prediction Errors technique achieves excellent security.

Keywords: Image encryption, Permutation techniques, Numerous level, Multimedia, Encryption.

1. INTRODUCTION

One of the most crucial things that has to be done when information is being sent across a network is to make sure the network is secure. Applications for picture or video encryption may be found in many different fields. Cryptography is one technique that may be used to guarantee the secrecy of data transfers. By using this technique, the information that will be shared will be converted into an unintelligible format, guaranteeing that only those with the proper authorization may precisely recover it. The encryption procedure may be carried out using either of the two encryption techniques—symmetric key cryptography or asymmetric key cryptography. When a single key is used for both encryption and decryption, the phrase

"symmetric key cryptography" describes the result. In contrast, "asymmetric key cryptography" describes the situation in which a separate key is used for both encryption and decryption.

The foundation of individual privacy, corporate effectiveness, and public safety is secure communication. It is crucial in a number of situations, including safeguarding private data, promoting confidence in electronic systems, and stopping cybercrime.Secure communication is essential for the following main reasons.

Secure communication prevents people' personal data (such as financial information and medical records) from being intercepted or stolen. Businesses depend on secure communication to keep trade secrets, customer data, and strategic plans safe from rivals or unscrupulous actors. Governments need secure routes to protect confidential information and ensure national security. Cybercriminals often use unprotected connections to exploit data for financial gain, identity theft, or other harmful goals. Encrypted communication protects against eavesdropping, phishing, and man-in-the-middle attacks, decreasing vulnerabilities. Secure communication protocols (such as HTTPS and TLS) build confidence between users and systems, assuring authenticity and dependability. Encryption ensures that consumers' information is secure, boosting trust in online services such as banking, e-commerce, and social networking. Many businesses are controlled by stringent data protection standards (such as GDPR and HIPAA), which need secure communication procedures. Organizations that fail to safeguard communications risk facing legal consequences, reputational harm, and a loss of customer confidence. Confidentiality guarantees that information is only available to authorized individuals. Integrity guarantees that data is not changed during transmission, hence preserving its correctness and dependability. As technologies such as IoT, AI, and 5G advance, secure communication is critical for preventing vulnerabilities in networked systems.

Blockchain and cryptography protocols are crucial for safeguarding communications in decentralized networks.

Existing Compression-Then-Encryption [CTE] system

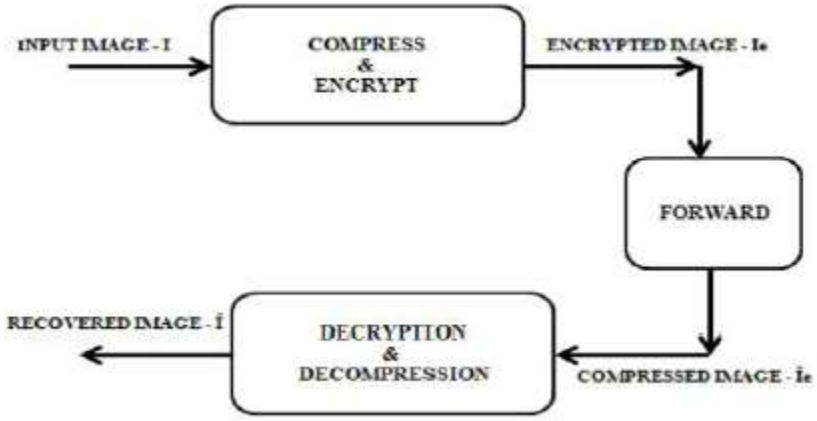

Fig. 1 shows block diagram of CTE system.

The block diagram of the current CTE system is depicted in Figure 1. In this system, a transmitter sends an image 'I' to a receiver in a way that is both secure and efficient. The transmission takes place through an untrusted channel provider. Before encrypting the information into Ie, the transmitter first compresses the information into Ie using an encryption function called $E_K(.)$, where 'K' represents the secret key. The data

that has been encrypted is then sent to the channel so that it may be transmitted to the recipient. The receiver will execute decryption and decompression of the image Ie in a sequential manner in order to get a rebuilt picture Ie. In many different circumstances involving secure transmission, the Compression-then-Encryption (CTE) paradigm is able to fulfill the requirements. When a transmitter is constantly concerned in maintaining the privacy of the picture data by encryption, however, the sequence in which compression and encryption are applied may need to be reversed in some circumstances. Despite this, the transmitter does not have any reason to compress the data or execute a compression method prior to encrypting the data. Following that, the channel provider compresses all of the network traffic in order to maximize the use of the network. As a result, compression took place at the channel, which is referred to as an ETC system.

2. LITERATURE SURVEY

A review of significant research on picture encryption and compression algorithms that we have used for comparative performance evaluations. The picture encryption approach uses natural features of pictures, such as high redundancy and strong spatial correlation, as well as diffusion characteristics, to create an encrypted image. An image encryption approach that employs Arnold's Transform, as described in [1,] investigates the properties of Arnold's cat map. Arnold's cat map is a basic discrete system that distorts and convolutes pathways in phase space. The scrambling effect is most successful in Arnold's Cat Map, hence the proposed method works well for image encryption. The Arnold Cat Map uses linear algebra to change the location of pixel values in the original image, resulting in an encrypted image. In [2], the author used the exclusive OR operation in combination with the Arnold Transform to produce scrambled images, hence improving the cryptosystem's security and resilience via many diffusions in the encryption method. In [3], the author used the Logistic map to improve the security of the Arnold transform technique. The logistic map is a general representation of the chaotic map. The word "chaos" refers to unpredictability and is defined as the study of nonlinear dynamic systems. Chaotic maps are simple, unstable dynamic systems that are very sensitive to their initial conditions. Chaos-based encryption provides very secure image encryption. The basic idea behind this research [3] is to turn the image on a pixel-by-pixel basis into chaotic map variables by iterating a chaotic map with certain starting circumstances. Traditional Arnold transform-based approaches in [1-3] have a common constraint in that the image height and width must be similar. To overcome the Arnold transform's shortcomings, the author of [4] develops a picture encryption approach by combining the Arnold transform with three stochastic strategies: random division, iterative number generation, and encryption order construction. The security of this approach is based on random procedures. This Arnold transform-based technique may be used to encrypt images of any size. As a result, compared to the classic Arnold transform, the proposed approach is more secure and applicable.Encryption and decryption operations are often regulated by specific keys, which may be identical or may be acquired simply from the other. These cryptographic algorithms are referred to as private key cryptography. The research in [5] focuses on the development of improved private key cryptographic techniques for security, notably the invention of private key cryptographic strategies using permutation methods. In [6], the author proposes the use of pseudo-random sequence generators to generate binary sequences for cryptography

applications, which considerably improves information coding efficiency. The paper [7] provides a unique technique for photo encryption that combines numerous permutation algorithms. The core idea of this research is that intelligible information in an image results from correlations between the bits, pixels, and blocks in a certain arrangement. This identifiable information may be reduced by diminishing the connection utilizing certain permutation tactics. A random combination strategy that incorporates all three procedures has been proved to be useful for security applications. As a result, [7] examines the design of private key cryptography systems, highlighting the importance of permutation methods, together with pseudo-random sequence generators, in selecting a certain permutation key from a specified range of valid keys. [8] proposes a context-based adaptive lossless image coding (CALIC). CALIC's distinguishing feature is the use of several modeling contexts to condition a nonlinear predictor, which improves its flexibility to variable source statistics. CALIC employs a unique gradient-based non-linear predictor [GAP], which updates prediction coefficients depending on local gradient estimates. The work in [9] shown that stream cipher encrypted data may be compressed utilizing coding with side information principles while retaining compression performance. Furthermore, the technology introduced in [9] was applied to the prediction error domain, resulting in higher lossless compression performance for encrypted grayscale and color images, as described in [10].

3. ALGORITHMS FOR THE ENCRYPTION OF IMAGES

Image encryption algorithms are designed to protect the confidentiality of image data by transforming it into an unreadable format, ensuring that unauthorized access or interception does not reveal the original content. These algorithms leverage various cryptographic techniques and are often tailored for the specific properties of image data, such as high redundancy and large sizes.

3.1 Commonly Used Image Encryption Algorithms

3.1.1. Classical Cryptography-Based Methods

- **AES (Advanced Encryption Standard):**
  - Symmetric encryption algorithm.
  - Can be applied to images directly or in blocks (e.g., pixel matrices).
  - Ensures high security but may not be efficient for large images due to its computational intensity.
- **DES (Data Encryption Standard) and Triple DES:**
  - Older symmetric encryption algorithms.
  - Limited use due to vulnerabilities in DES, though Triple DES offers better security.

3.1.2. Chaotic-Based Encryption

- Utilizes chaotic maps (e.g., Logistic map, Henon map) to generate pseudorandom sequences.
- Examples:
  - **Arnold Cat Map:** Shuffles pixel positions based on a chaotic pattern.
  - **Logistic Map-Based Encryption:** Alters pixel values and positions using chaotic sequences.
- Highly efficient for image-specific properties and suitable for real-time applications.

3.1.3. Selective Image Encryption

- Only a portion of the image (e.g., significant regions or specific layers) is encrypted.
- Reduces computational load while maintaining adequate security.

3.1.4. Bit-Plane Encryption

- Encrypts individual bit planes of the image, typically focusing on higher-order bits.
- Allows control over the trade-off between security and complexity.

3.1.5. Compression and Encryption

- Combines image compression (e.g., JPEG, Wavelet) with encryption.
- Example: Encrypting wavelet coefficients after compression for efficient storage and transmission.

3.1.6. DNA-Based Encryption

- Encodes image pixels into DNA sequences.
- Leverages biological encoding schemes and operations like DNA addition and substitution.

3.1.7. Transform Domain Encryption

- Encrypts images in their frequency domain rather than the spatial domain.
- Techniques:
  - **Discrete Fourier Transform (DFT):** Encrypts frequency coefficients.
  - **Discrete Wavelet Transform (DWT):** Combines encryption with compression for efficient representation.
  - **Discrete Cosine Transform (DCT):** Often used in JPEG compression and encryption.

3.2 Characteristics of Good Image Encryption Algorithms

1. **High Security:** Resistance to attacks like brute force, statistical, and plaintext attacks.
2. **Efficiency:** Ability to handle large image sizes quickly.
3. **Sensitivity:** Small changes in the key should cause significant changes in the encrypted image.
4. **Robustness:** Resilience against noise or data loss.
5. **Compatibility:** Ability to work with other image processing operations like compression.

3.3 Popular Applications

- Secure image transmission in military and medical fields.
- Digital rights management (DRM) for images.
- Cloud storage of confidential image data.

4. PERMUTATION TECHNIQUES FOR ENCRYPTING IMAGES

Permutation techniques are commonly used in image encryption to scramble pixel positions while retaining their original values. These methods ensure that the encrypted image appears highly disordered, making it difficult for attackers to deduce the original image structure. Permutation is often used in conjunction with substitution or diffusion techniques for added security.

Types of Permutation Techniques for Image Encryption

4.1. Row and Column Shuffling

- Rearranges rows and columns of the image matrix based on a predefined or randomly generated key.
- Example:
  - Swap row 1 with row 3, column 2 with column 5, etc.
- Suitable for initial scrambling but vulnerable to known-plaintext attacks.

4.2. Block-Based Permutation

- Divides the image into smaller blocks and rearranges these blocks based on a key.
- Example:
  - An 8×8 image divided into 4×4 blocks and then shuffled.

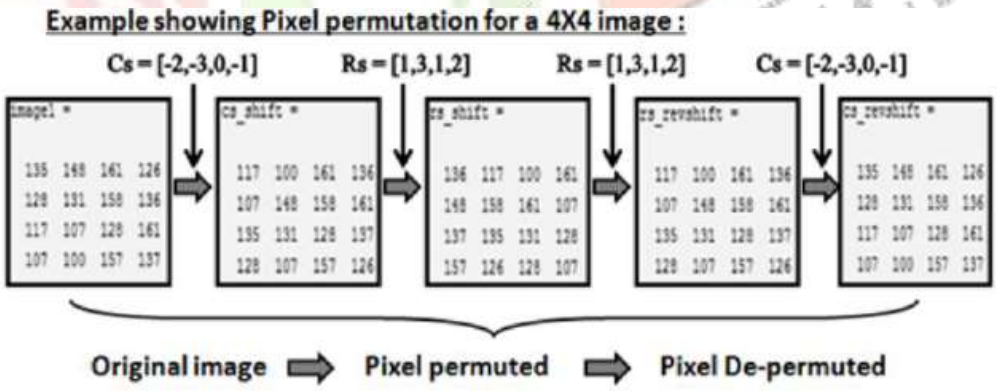

Fig 2 : shows an example for Pixel permutations for a 4X4 image

- Improves resistance to statistical attacks compared to pixel-level permutations.

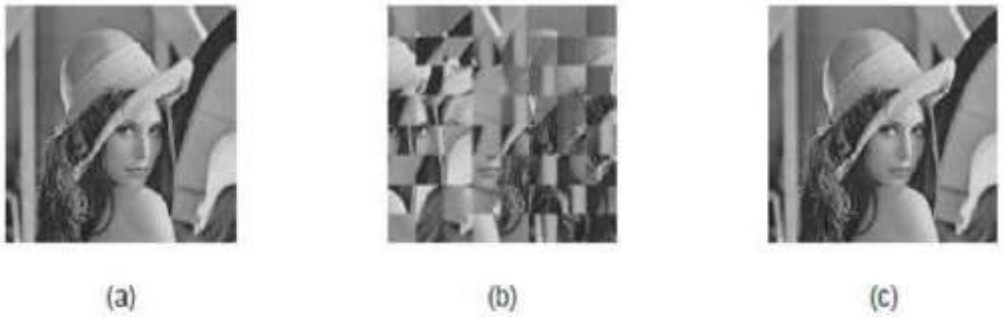

Fig 3 : BLOCK permutation (a) Original image (b) Encrypted image (c) Decrypted image

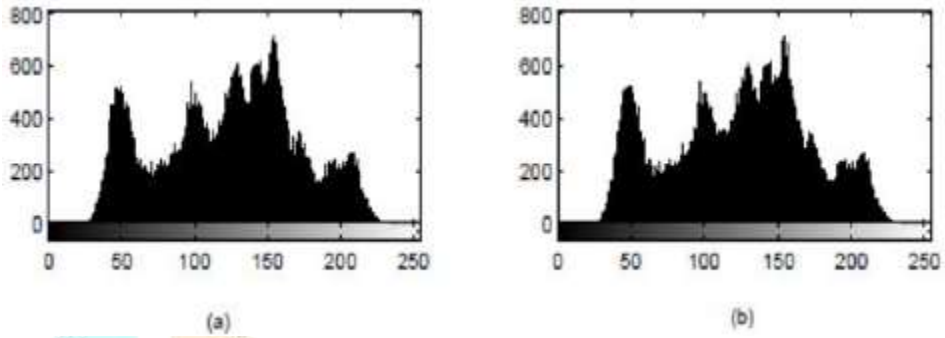

Fig 4 : Histograms of BLOCK permutation (a) Original image (b) Encrypted image

4.3. Pixel-Level Permutation

- Scrambles individual pixels throughout the image.
- Often guided by a key derived from a chaotic sequence or pseudorandom generator.
- Provides strong disorganization but can be computationally expensive.

Fig 5 : PIXEL permutation (a) Original image (b) Encrypted image (c) Decrypted image

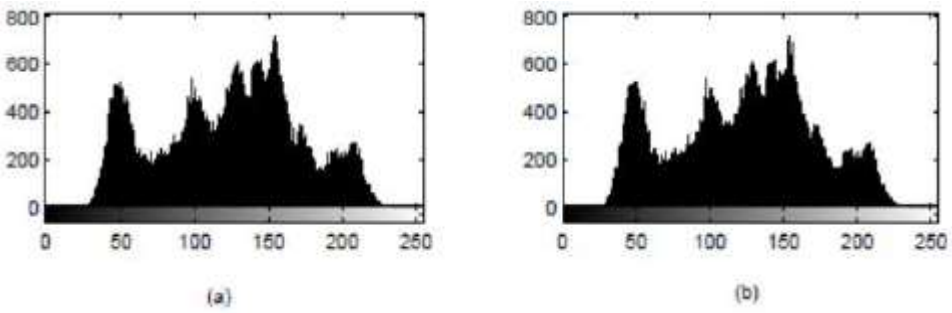

Fig 6 : Histograms of PIXEL permutation (a) Original image (b) Encrypted image

4.4. Arnold Cat Map

- A chaotic map that iteratively shuffles pixel positions based on a mathematical formula:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \mod N$$

- where N is the image dimension, and (x,y) are pixel coordinates.

Reversible: The original image can be recovered using the inverse map and the same number of iterations.

4.5. Bit-Plane Permutation

- Splits an image into its bit planes (binary representation layers of pixel values).
- Permutes these planes or shuffles bits within individual planes.
- Preserves image integrity but disrupts meaningful patterns.

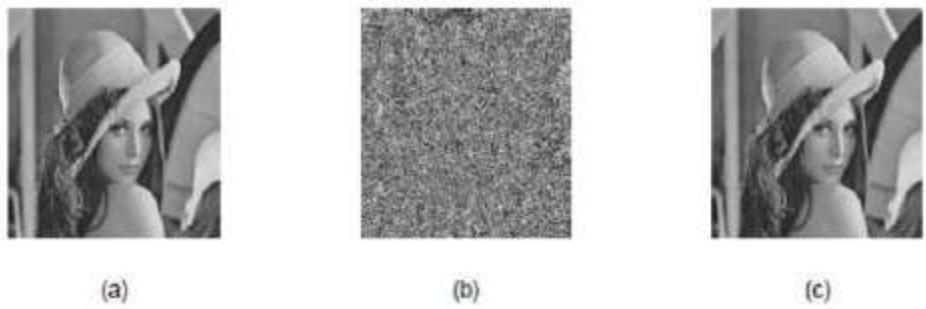

Fig 7 : BIT permutation (a) Original image (b) Encrypted image (c) Decrypted image

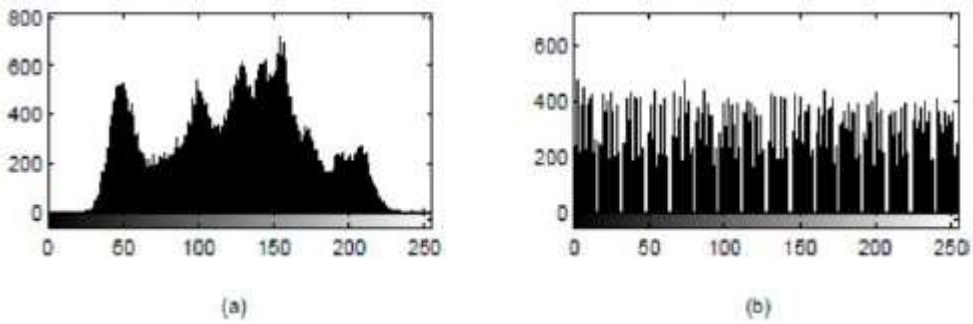

Fig 8 : Histograms of BIT permutation (a) Original image (b) Encrypted image

4.6. Zigzag Permutation

- Rearranges pixels in a zigzag order, commonly used in image compression (e.g., JPEG).
- Can be adapted for encryption by applying custom zigzag patterns.

4.7. Logistic Map Permutation

- Uses chaotic sequences generated by logistic maps for pixel position rearrangement:

$$x_{n+1} = r x_n (1 - x_n)$$

where r is a control parameter (commonly $3.9 < r < 4$), and x_n generates pseudo-random values.

- Provides high randomness and sensitivity to initial conditions.

4.8. Hilbert Curve-Based Permutation

- A space-filling curve that maps 2D image pixels into a 1D sequence.
- Reorganizes pixels based on their Hilbert curve order, ensuring locality and structure disruption.

Advantages of Permutation Techniques

1. **High Efficiency:** Most permutation methods are computationally lightweight and straightforward.
2. **Enhanced Security:** Breaks spatial correlation in the image, preventing statistical attacks.
3. **Reversibility:** Most techniques are inherently reversible when the key and permutation method are known.

Challenges

- **Weak Security When Used Alone:** Permutation techniques only rearrange pixel positions and do not alter their values, making them vulnerable to attacks without additional encryption layers.
- **Key Management:** Secure generation and transmission of keys are crucial to prevent unauthorized decryption.

Applications

- **Preprocessing for Substitution/Diffusion:** Enhances overall encryption when combined with other methods.
- **Lightweight Encryption:** Used in scenarios requiring moderate security and low computational overhead, such as IoT devices.

5. 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.These qualities, including dependability, flexibility, and security, are shown by Arnold's transform method. However, these applications are limited to images with the same size and computing speed.

Since bit permutation reduces correlation and pixel and block permutation greatly improve security, integrating many permutation approaches was easy to implement. As a result, the sensory data was decreased due to the random combination of all three variations. This technique is resistant to frequency analysis assaults, since the findings show that the encrypted picture's histogram is evenly distributed. According to the results of the experiments, this approach is faster and more secure than the current methods.

Considering the results as shown that there is almost no connection between techniques I and II, suggesting that the quality of image encryption is adequate when compared to method III. Despite the algorithm's superior performance, the correlation coefficient is rather low. It is necessary to calculate the PSNR and MSE for the encrypted image before comparing it to the original.

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.