INNOVATIVE TECHNOLOGICA
METHODICAL RESEARCH JOURNAL
ISSN: 2776-0987 Volume 3, Issue 12 Dec. 2022

OPTIMIZATION ENERGY EFFICIENT OF CRYPTOGRAPHY AS ENCRYPTION AND DECRYPTION IMAGE USING ECC FOR APPLY IN SECURE ONE-WAY COOPERATIVE IMAGE TRANSMISSION

Firas Saadallah Raheem
Education College Ibn Rushd for Humanities,
University of Baghdad. Baghdad, Iraq
firas.saadallah@ircoedu.uobaghdad.edu.iq

Abstract

The paper an image compression structure the adaptive JPEG2000 image compression technique using the wavelet image transform is designed. The use of CS for periodic data transmissions is proven as an effective solution for WSNs as observed in CS-based sensor communications reduce data transmissions and improve energy efficiency significantly. But another challenge while using the compression is data loss due to different security threats during the transmission. The image is compressed data is more vulnerable to the different wireless channel threats. This paper addresses the security issues for compressed data by using the modified ECC-based cryptography method. The key problem of the conventional ECC method is the complicated and time-consuming task of scalar multiplication which may consume the extra energy of sensor nodes, so energy consumption is optimized by elaborating the steps of ECC-based encryption and decryption in the proposed ECC-based model. The main aim of improving the image quality with minimum processing time and error rates. However, for WMSNs, force aptitude is also an essential research challenge as the high-dimensional digital images consume more processing capabilities of sensor nodes. In WMSN, the image is transmitted through a large number of relays; thus the larger the transmissions the more the energy consumption.

The compressed data at the receiver end is decompressed with poor quality, hence securing the compressed data by using the lightweight security method is important while planning the helpful picture transmission model. In this chapter, we propose our next research contribution to alleviate the challenges of security and energy efficiency for cooperative digital image transmission.

Keywords: Optimized JPEG 2000, introduced , digital image compressed, ECC-based encryption and decryption

1. Introduction

Wavelet transform realizes the JPEG 2000 is the consistent picture weight standard reliant on the wavelet change and was created by the Joint Photographic Specialists Get-together advisory gathering in 2000, replacing their DCT-based JPEG standard. The JPEG 2000 is a picture weight estimation in which, after picture tiling, the tiles are changed using the Cohen-*Daubechies*-Feauveau CDF 9/7 wavelet change for lossy weight and CDF 5/3 wavelet change for lossless weight. This procedure brings about a gathering of sub-groups on different levels. The quantized sub-bands are a piece of code squares. These code squares are encoded, starting from the most fundamental piece plane to the lower bit planes using the Embedded block coding with optimal truncation EBCOT [1] count. Encoding of each piece plane incorporates three passes: importance spread [2- 4], centrality refinement, and cleanup pass. Centrality expansion pass encodes bits and signs of immaterial coefficients with a critical coefficient as neighbors. At that point, size refinement encodes refinement bits of coefficients discovered fundamentally before bit planes. Taking everything into account, in cleanup pass coefficients without any coefficients found in basic bit planes are encoded [5].
Finally, the bits conveyed in the engineering pass are then encoded by a setting-based twofold calculating coder. The resultant bitstream is then parted into packets containing bits of a social occasion of code squares. Bundles containing less necessary bits might be discarded. Packets from all sub-groups are then assembled in „layers", so that the image quality increases with interpreting of each layer, supporting novel transmission along these lines [7-8]. The JPEG 2000 encoding count is amazing and has numerous appealing highlights. Be that as it may, it is complicated and computationally strange and has limited embeddedness [9-10].

1.1 B. SPIHT

SPIHT [11] was proposed by A Said and Pearlman in 1996. The SPIHT coding is a reasonable and improved kind of EZW computation that achieves higher weight and perfect execution over EZW. The figuring relies upon a sensible referencing of the coefficients by degree and bit plane, with transmission

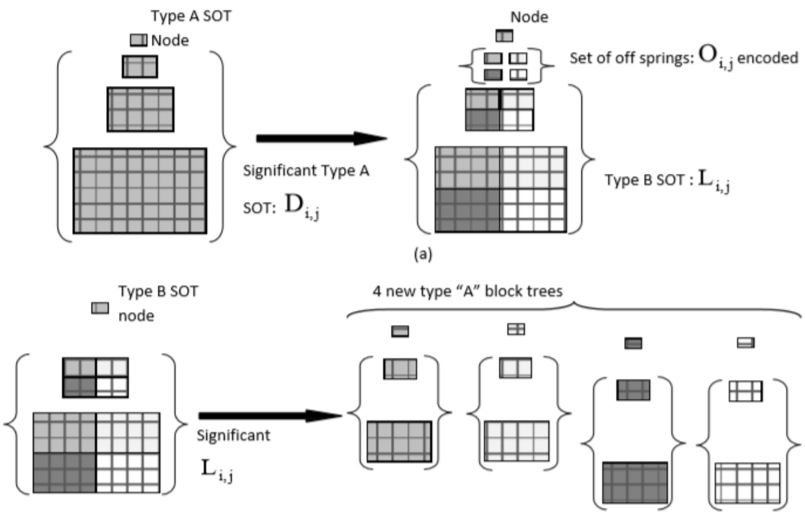
INNOVATIVE TECHNOLOGICA
METHODICAL RESEARCH JOURNAL
ISSN: 2776-0987 Volume 3, Issue 12 Dec. 2022

requesting compelled by a set circulating computation (SPIHT). SPIHT achieves weight by totaling countless immaterial coefficients in spatial orientation trees (SOT) spatial direction trees (Alcoholic), moreover called zero trees. A zero tree is based on the premise that if a coefficient is inconsequential, its relatives in higher recurrence sub-groups are bound to be unimportant. SPIHT tries between band connections among change coefficients and achieves an incredible rate-mutilation execution and gives an installed bitstream that licenses definite piece-rate versatility, for example, progressiveness. Criticalness data in the SPIHT calculation puts away in three information subordinate orchestrated records a list of insignificant pixels (LIP), a list of insignificant sets (LIS), and a list of significant pixels (LSP). The calculation instates by fusing the coefficients in the most negligible repeat sub-band (LL-band) in LIP, and those with relatives are added to LIS as a sort of 'A' region. The LSP begins as an unfilled once-finished. a list of insignificant pixels (LIP), a list of insignificant sets (LIS), and a list of significant pixels (LSP). The algorithm initializes by adding the coefficients in the lowest frequency sub band (LL- band) in LIP [13] , a The SPIHT coding of wavelet coefficients fuses a collective issue of masterminding and refinement passes related to decreasing edges. In the orchestrating pass, the immensity decision of a large number of coefficients concerning the current limit is coded. A vital coefficient is found because the signed piece is promptly transmitted [14- 15]. After the orchestrating pass, the refinements pass adds to the coefficients that were found to be enormous before with a present limit.

The calculation begins with the largest plane and proceeds toward the best targets. At each piece plane, the orchestrating pass encounters the LIP sought after by LIS, and after that refinement, the pass goes to LSP. For every coefficient in LIP, one piece is used to depict its noteworthiness for the present edge. If the coefficient isn't huge, it stays in LIP; generally, the signed piece is transmitted and the coefficient is moved to LSP. After LIP, sets of LIS are checked. Each set (spatial course tree) of LIS endeavors against edge and vitality is encoded. A colossal 'A' set will be allotted into four successor coefficients and a type 'B' set (awesome relatives), if the stunning relative set exists.The type 'B' set is added to the arrangement, four coefficients are sought after their centrality against current most distant point, and added to LIP and LSP as per the requirement. A huge type 'B' set is apportioned into four type 'A' sets and is added to the game plan. The apportioning of type 'A' and type 'B' set

ISSN: 2776-0987 Volume 3, Issue 12 Dec. 2022

of SPIHT. Eventually in refinement pass, each coefficient of LSP (apart from the additional ones in the present piece plan) is refined with one piece. At that point, the utmost is secluded by two, and the algorithm at that point repeats the strategy [16] . A significant type "A" set will be partitioned into four offspring coefficients and a type "B" set (grand descendants), if the grand descendant set exists; the type "B" set is added to the end of LIS, while four coefficients are tested for their significance against current threshold and added to LIP and LSP accordingly. Significant types "B" set is partitioned into four type "A" sets (with offspring coefficients as corresponding nodes) and are added to the end of LIS [17] . The partitioning of type "A" set and type "B" set of SPIHT is shown in figure 1. Finally, in refinement pass, each coefficient of LSP, except those added in current bit plane, is refined with one bit [18]. Then the threshold is divided by two, and the algorithm then repeats the above procedure. Effectiveness of the algorithm can be further enhanced by entropy coding its output, but at the cost of a larger encoding/decoding time [19].



Fiure.1 the apportioning of type 'A' and type 'B' set of SPIHT is shown in Figure 2.10. Eventually in refinement pass, each coefficient of LSP.

A fundamental issue of the SPIHT coder is that the calculation utilizes subordinate information records to screen sets and coefficients to be tested for significance against threshold. The utilization of records in SPIHT causes a unique memory basically and includes multifaceted computational nature for including/organizing of memory. The unusual slow execution of SPIHT has been represented in research papers that use state memory to screen sets/coefficients for criticalness testing. NLS [20] proposed by Wheeler and Pearlman utilizes 4 bits for every coefficient state memory, while use in [21] requires 3 bits for every coefficient state memory to empower coding WSNs with imaging abilities are highly constrained as far as memory, handling capacity, and battery power go as they have to transmit images on remote systems that suffer due to high probability and busyness of clamor. It is additionally significant that the computational cost of weight isn't the related cost of transmission precisely to upgrade energy proficiency and stretch the existence of system. In this way, a quick and productive image pressure calculation with low memory need and bit rate adaptability (embeddedness) is apt for execution on these frameworks [23-24].

The characteristics of the unmistakable picture weight calculations are exhibited in [25-26]. Even though JPEG 2000 gives the most astounding coding proficiency, its weight is very time- and vitality-consuming and is thus not reasonable for usage in constrained conditions.

2. Problem Statement

- Image coding strategies Optimized JPEG 2000 introduced for the digital image compressed after the denoising to improve the image transmission performance as well as computational efficiency.
- The optimized ECC technique further encrypts the compressed data. The novelty of this method is that it achieves the trade-off between minimum energy consumption and strong security by modifying the optimized scalar multiplication tasks using a special random number as a scalar. This approach limiting the computational endeavors accomplishes higher security for compressed data.
- The complete wireless communication model designed using the BPSK modulation and Rayleigh fading channel for cooperative image transmission.
- Investigated image compression algorithms using image quality analysis element like PSNR, MSE, etc.
- Performance evaluation of cooperative image transmission with best-in-class techniques exhibited as far as BER, MSE, energy efficiency, etc. are concerned.

Before presenting the proposed methodology design and algorithms, we first discuss the different types of digital data and file types that are transmitted over the WMSNs.

3. Related Work

There are different types of image cryptography/encryption methods.

- **Image Encryption Based on Chaos Theory and Chaotic Map:** A confusion-based picture encryption plot is commonly composed of two procedures: (i) stage and (ii) dissemination. The change is accomplished by scrambling every one of the pixels, in general, utilizing a 2D turbulent guide, (for example, Pastry specialist map, Arnold feline guide, and so on). During dispersion, the pixel esteems are adjusted successively; the change made to a particular pixel relies on the amassed impact of all the past pixel esteems. Be that as it may, the same number of rounds of stage and dissemination or cycles ought to be taken. The general encryption speed is moderate.
- **Chaos-based Random Number Generator:** For an arbitrary generator, the number of ones and zeros in the yield are equivalent. It is conceivable to detail numerous other factual properties that depict the keystream generated by an arbitrary source. Different test suites are accessible in writing. These accurate tests are designed to assess the arbitrariness properties of a limited grouping. The unruly circle generated by a non-linear framework is sporadic, intermittent, unpredictable, and has a tricky reliance on the underlying conditions. These qualities concur with the disarray and dissemination properties in cryptography. Hence, as of late, the turbulent framework has been read for security in both digital and straightforward forms [6].
- **Stream Encryption Scheme:** Stream encryptions depend on delivering a constant cryptographic keystream and are used to scramble one piece or byte at once. Stream ciphers have relatively low memory requirements. Various image encryption schemes under this category have been proposed in the last decade [27-28].
- **Block Encryption Scheme:** Square encryption is an encryption plot in which the plain substance is isolated into squares of fixed length and blended one square on the double. Square ciphers can provide integrity protection and confidentiality. Chaotic block ciphers transform blocks by directly applying the chaotic maps. Various image encryption schemes under this category have been offered in the last decade [29-30].

INNOVATIVE TECHNOLOGICA
METHODICAL RESEARCH JOURNAL
ISSN: 2776-0987 Volume 3, Issue 12 Dec. 2022

4. Methodology

This section presents the novel framework of energy-efficient and secure digital image cooperative image transmission system. System model designed for one-way cooperative image transmission is shown in Figure 2. The nodes *S* and *D* represent the transmitter and receiver, respectively. The node *S* transmits an image to the node *D* through Rayleigh fading channel and the node *D* sends the *ACK* message to the *S* through the DF-based cooperative communication algorithms. The *ACK* message is transmitted by node *D* to *S* for the confirmation of successful image information received over the Rayleigh blurring channel as per the standards of wireless communication technologies such as 802.11.

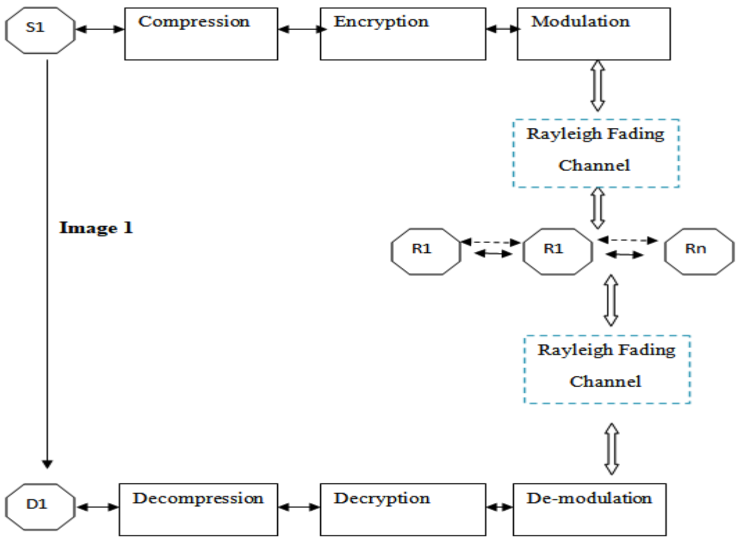


Figure 2 Image compression with encryption and transmission

Let R is the set of all relay nodes:

$$R = \{R_1, R_2, \ldots, R_N\}, \quad N \geq 2$$

The input image is transmitted in various squares through the agreeable relay nodes. In cooperative image transmission, every relay node plays two roles, such as relaying role (*RR*) and monitoring role (*MR*). Relay node performs the process of image blocks transmission. Each transfer nodes ought to have two parameters referenced in equations.

Let R be the set of all relay nodes:

The input image is transmitted in various squares through the agreeable relay nodes. In cooperative image transmission, every relay node plays two roles, such as RR and MR. Relay node performs the process of image blocks transmission. Each transfer hub ought to have two parameters referenced in Equations

Where R_i is the i^{th} relay node, R_j is the j^{th} relay node, M_j is total transmitter, recipient hubs associated with the ith relay node, and d_{ij} is the distance among i^{th} and j^{th} relay hub and

Where N_j (x, y) is the j^{th} MR, R_i is i^{th} relay node associated with the j^{th} MR center point, and d_{ij} is the separation between the i^{th} MR center point and the j^{th} RR hub.

The role of MR is to detect and transmit the current squares to the closest transfer hub. Hand-off hub at that point recognizes the got data, applies the DF technique, and after that sends it towards the following moderate or proposed sink hub. The correlation among the relay nodes helps to efficiently deliver the multimedia data over the wireless channel towards the intended recipient. The cooperative communication among relay nodes decodes and forwards the current image data towards the next relay node selected through correlations among all available relay nodes*.* Novel algorithms for image compression are implemented based on JPEG 2000 and ECC-based cryptography and contribute to the functionality in the next sub-sections.

4.1 Image compression / decompression

In this contribution, mainly, there are two reasons for the superior performance of JPEG 2000: the embedded block coding and wavelet transform with the use of the optimal truncation (EBCOT). Thus the JPEG 2000 provides a complete novel way of interacting with image compression in an efficient and scalable manner. As the sensor nodes have limited battery capabilities, the reduction of transmitted data will lead to a network lifetime enhancement The adaptive JPEG 2000 image compression technique using the wavelet image transform is designed as shown in Figure 3.

The adaptive JPEG2000 image compression technique using the wavelet image transform is designed. Figure 3. shows the working of JPEG2000 image compression (at the transmitter side).

INNOVATIVE TECHNOLOGICA
METHODICAL RESEARCH JOURNAL
ISSN: 2776-0987 Volume 3, Issue 12 Dec. 2022

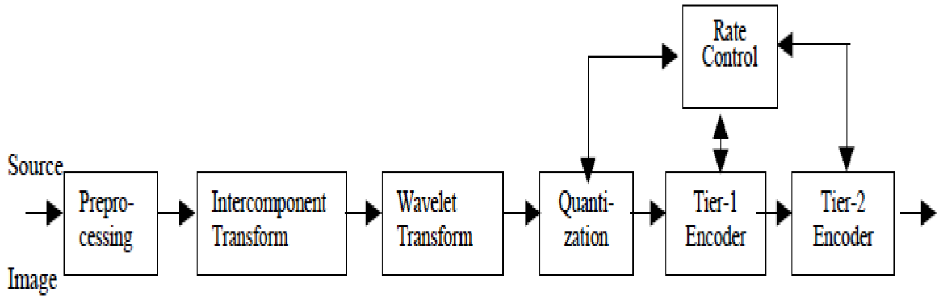


Figure 3 Structure of adaptive JPEG2000 compression.

Figure 3 results into the compressed image, which is fed to the ECC based encryption, then modulation and transmission over the remote channel. At the got end, after the demodulation and decryption, the decompression step is performed.

Figure 3 results into the compressed image, which is fed to the ECC-based encryption before the modulation and transmission over the remote channel. At the got end, after the demodulation and decryption, the decompression step is performed.

- **Pre-processing:** Inside the primary development, the encoder changes the test information to an excellent clear range with the objective that it is roughly engaged around zero. In case the test data is set apart, by then acknowledge they are locked in at zero.

- **Inter-component transform**: JPEG 2000, of course, contemplates a between-segment part to be connected with the image after it has been level-moved. This change empowers the elaborate topic to relate the particular segments for multisegment pictures. Such transform occurrence changes over the RGB data to Cyber Data.

- **Wavelet transform:** It is a widely used technique in the image-processing domain. In DWT, each square is distinguished to be separated into the wavelet sub-packs over the various levels. The compression method JPEG 2000 exploited the lifting-based DWT. The wavelet transform is an essential task in order to generate the resolution-scalable bitstreams as well as the spatial correlation decomposition. The vector of transformed coefficient is the outcome of the wavelet transform.

ISSN: 2776-0987 Volume 3, Issue 12 Dec. 2022

- **Quantization:** The process of quantization is mainly used in lossy compression. In every sub-band, the wavelet coefficients are scalar quantized. The constant values are defined and a dynamic range of sub-band values are used to join the step size of quantization. The quantization step is used to minimize the precision of the sub-band coefficients; thus fewer bits are required to encode the changed coefficients.

- **Tier-1 coder:** The code blocks are delivered from every sub-band. The code squares are freely entropy-coded. The JPEG 2000 method uses the EBCOT entropy coding system which comprises two levels. The coefficient bit context modeling as well as the bit-plane data arithmetic coding are executed over the block samples which then produce the embedded block bitstreams in the main working of a tier-1 coder.

- **Tier-2 coder:** In Tier-2 coder, the compacted data is used in each quality layer called the packetization procedure. Such a process of data ordering is essential in creating the SNR and resolution scalable compressed bitstream.

- **Rate Control:** The rate control phase used to manage the quantizer step sizes in order to achieve the target bit-rate constraints in lossy compression. Each block bitstream is truncated to different sizes in order to render the best rate-contortion picture.

4.2 Encryption/Decryption

After the image is compressed, the compressed data is more vulnerable to the different wireless channel threats. This paper addresses the security issues for compressed data by using the modified ECC-based cryptography method. The key problem of the conventional ECC method is the complicated and time-consuming task of scalar multiplication which may consume the extra energy of sensor nodes, so energy consumption is optimized by elaborating the steps of ECC-based encryption and decryption in the proposed ECC-based model.

- Key Generation: Inside the key generation process, you have to pick an immense whole number d, and search the T = dG where d is a private key. It is fundamental to guarantee the success of the private key and an agreeable relationship with the security of the ECC encryption and decoding.

ISSN: 2776-0987 Volume 3, Issue 12 Dec. 2022

- Encryption: The transmitter can encode the message with an open key or other keys. During the encryption procedure, the plain text should be mapped to a prime field section m, discretionarily picking a vital whole number k, processing x_1y_1 $(x_1y_1) = kG$, $(x_2y_2) = kT$ and calculating $C = m*x_2$, (x_1y_1, C) to get the encrypted data.
- Decryption: In the data decryption process, the receiver needs to do the calculation $(x_2y_2) = d\ (x_1y_1)$ with the private key d. The recipient can get the first plain text by computing= Cx_2^{-1}.

Here, the private key d is used to ensure the basics of encryption and decryption process of the security technique. The number k has a moderate impact on data security. However, as we discussed, the complex scalar operations in k random number generation processes are proposed to minimize the computational efforts. The new methodology ECC, for the most part

5. Result and Discussion

This segment displays the re-enactment results and investigation of the model designed. The outcomes of PSNR, MSE, Compression Ratio (CR), Structural Similarity Index Measure (SSIM), etc. are estimated. The parameters PSNR and MSE The SSIM is another image quality evaluation parameter. It is is a technique for foreseeing the apparent nature of digital TV and true-to-life pictures as different sort of digital pictures and recordings. It is computed as:
Where x and y are two images. The variables l, c, and s stands for the functions of luminance, contrast, and structure, respectively.

1. The performance metrics CR is figured as the degree of full-scale bits required for taking care of the picture before compression (BC); furthermore, complete bits as are necessary for putting away the picture after compression (AC). Calculation process: according to the two-count methodology, the calculation process proposed, such as from right to left (R2L) (algorithm 2) and from left to right (L2R) (Algorithm 1). As a result of PP is left or the right piece of the B obtained the results of BB*B in that the computation of B*Z. Give the bit a chance to number of B be h, the bit number of k bee, at that point the bit number of PP is v=e%h. With the PP the accompanying part delivered toward the completion of k.

2. **Optimized scalar multiplication:** In the process of the proposed calculation (algorithm), the mix is utilized with other scalar duplication to enhance the effectiveness of calculation. For instance, in the progression of 2) in the proposed calculation, figuring F=B*D and O=PP*D, there is a path joining with NAF (Non-Adjacent Form) calculation The reinforcing with NAF computations leads the lower point expansion operation quantity during the expansion part of EP processing.

Algorithm : Optimization ECC Encryption
1. N: extended random binary string generation
2. Update N, according to NAF.
3. B: Extended part generation in NAF method
4. W=0;
5. c=0
6. Compute (according to NAF method):
7. F=B*D
8. I=PP*D
9. If Nc = 1 then W=W+F, if $L_c = -1$, then W=W-F
10. $W=2^hW$
11. c=c+1
12. Go to step 9, n times process repeated, at end of last iteration, the algorithm terminated at step 9.
13. $W=2^vW$
14. W=W+O
15. return W

Thus implementation method significantly reduced the computational efforts in the process of encryption and decryption using on compressed image and de-modulated image, respectively, in proposed one-way architecture this segment displays the re-enactment results and investigation of the model designed in this section. The outcomes are estimated regarding PSNR, MSE, Compression Ratio (CR), Structural Similarity Index Measure (SSIM), etc. The parameters PSNR and MSE The SSIM is another image quality evaluation parameter. The SSIM is a technique for foreseeing the apparent nature of digital TV and true to life pictures, just as different sorts of digital pictures and recordings. It is computed as:

$$SSIM = [l(x,y)]^2 * [c(x,y)]^2 * [s(x,y)]^2 \quad .$$

Where x and y are two images. The variables l, c, and s standards for the functions of luminance contrast and structure, respectively.

The performance metrics compression ratio (CR) is figured as the degree of full-scale bits required for taking care of the picture before compression (BC); furthermore, complete bits as are necessary for putting away the picture after compression (AC).

$$CR = \frac{BC}{AC} \quad .$$

Here BC is nothing but the original image size, and AC is compressed image size. Based on various performance metrics, the proposed approach is evaluated. The digital images are taken from the publically available research datasets such as man, Barbara, couple, Lena, boat, and cameraman. All experiments are evaluated on six images. We present the outcomes methods savvy to legitimize the viability of the proposed methods.

5.1 Evaluations of modulation methods

In this work, it is proposed to use BPSK modulation rather than other modulation methods such as quadrature phase-shift keying (QPSK) and quadrature amplitude modulation (QAM). The BPSK method for modulation suggested based on the experimental evaluation of BPSK with QPSK and 8-QAM modulation methods in terms of bit error rate (BER) and throughput. Figure 4 demonstrate the outcomes of BER and performance for each modulation method in the proposed one-way image transmission model respectively.

As observed in Figure 4 each modulation technique is evaluated on the proposed model using both additive white Gaussian noise (AWGN) also, Rayleigh fading channels. For both wireless channels, BPSK modulation method shows the minimum bit error rate performance with varying SNR. Similarly, BPSK achieved the highest throughput for image data transmission as demonstrated in Figure 4. The reasons for the superior performance of BPSK modulation over the QPSK and QAM in proposed cooperative image transmission model the simple encoding method. BSPK is the simplest method to encode data in the phase as compared to both QPSK and QAM and hence achieved the minimum BER performance with maximum throughput.

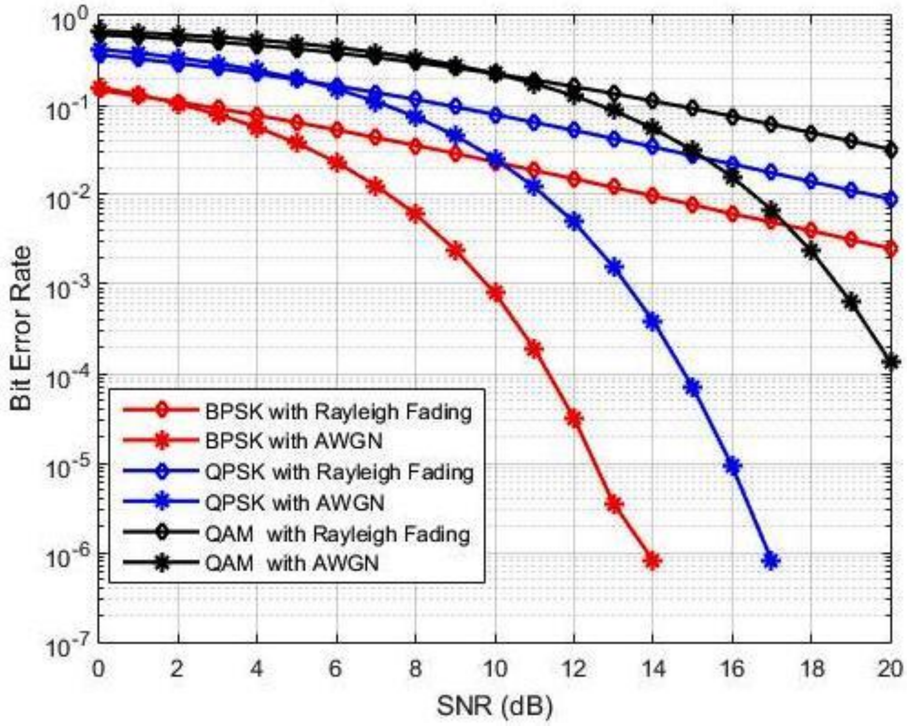


Figure 4 Bit error rate vs. SNR.

Note that these results demonstrated in Figure 4. Averaged outcomes after the evaluation of all six experimental images. Table1 (figure 4) shows the throughput performance of each evaluated image using all three modulation techniques.

Note that these results demonstrated in Figure 4 averaged outcomes after the evaluation of all six experimental images

5.2 Evaluations of image compression methods

The compression methods are evaluated in terms of many performance metrics for image mainly in two categories image quality parameters and compression quality parameter. The pressure procedure quality is assessed utilizing the CR parameter given in expression. In this section, the CR rate evaluations discussed. Table 1 (figure 4) demonstrates the performance of the compression ratio using different compression methods and proposed methods.

INNOVATIVE TECHNOLOGICA
METHODICAL RESEARCH JOURNAL
ISSN: 2776-0987 Volume 3, Issue 12 Dec. 2022

Table 1 Compression ratio evaluation.

	JPEG	Run length	JPEG2000	Proposed
Boat	1.888	4.426	11.231	13.234
Barbara	1.931	4.422	11.903	13.891
Cameraman	2.088	4.939	11.408	13.287
Couple	1.907	4.412	11.618	13.475
Lena	2.045	4.648	11.653	13.744
Man	1.870	4.461	11.435	13.598

As observed in Table 1, the adaptive JPEG2000 compression method presented in this paper shows the better CR as compared to all conventional methods. The performance is compared with JPEG, Runlenght Huffman coding . JPEG2000 methods. The JPEG method shows the worst performance for the CR. The advantage of DWT and EBCOT techniques in JPEG2000 leads the improved CR in the proposed cooperative image transmission model. Compression technique required to achieve the tradeoffs between the CR and image quality performance metrics especially for image compression.

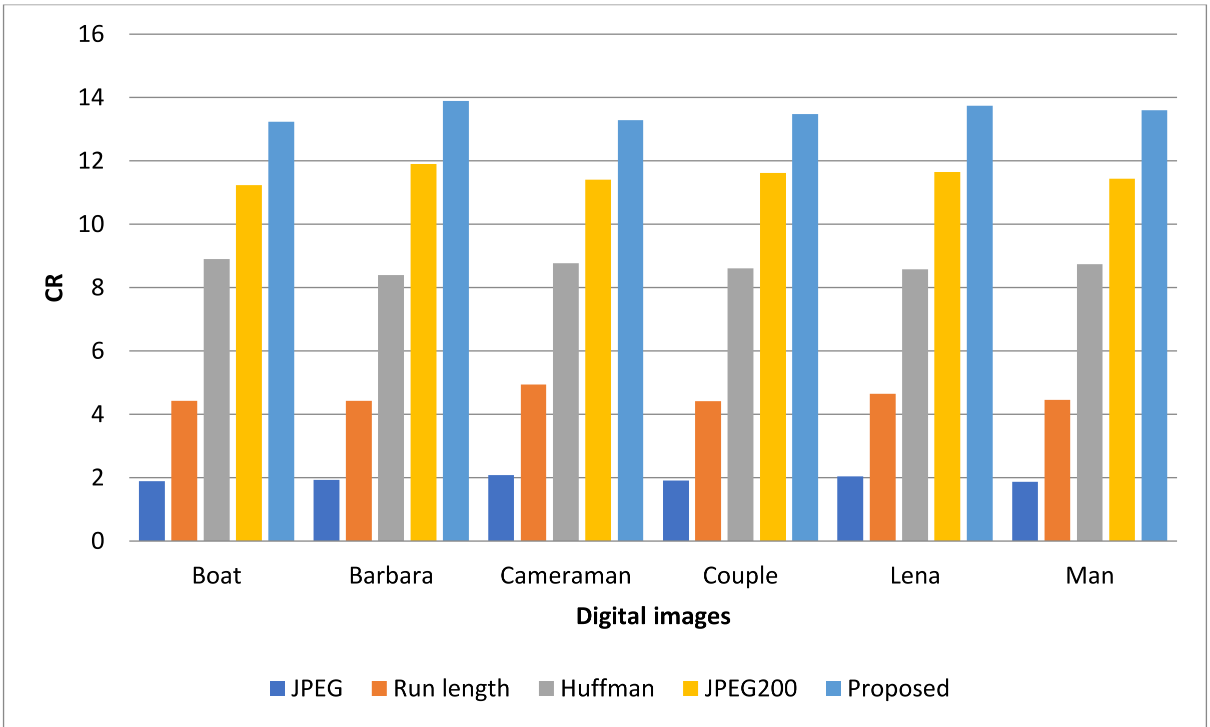


Figure 5 CR evaluations of different pictures.

ISSN: 2776-0987 Volume 3, Issue 12 Dec. 2022

5.3 Evaluation of Security Algorithm

After the compression, security is ensured by using the modified ECC method for the proposed image transmission model. The proposed ECC method designed to achieve computational efficiency so that the energy consumption of sensor nodes reduced significantly.The ECC method composed of three main tasks, such as key generation, encryption, and decryption. The computation efforts (time) required for key generation, encryption, and decryption and compared with existing ECC approach are measured. Table 2 shows the average computation times needed for each phase. Note that the experiments were conducted on I3 processor and 4 GB RAM configurations.

Table 2 Computation time analysis.

	ECC (Sec.)	Modified ECC (Sec.)
Key generation	1.09	0.98
Encryption	1.98	1.47
Decryption	2.11	1.52

As observed, the proposed modified ECC method achieved the computation efficiency with strong or equivalent security conditions for compressed image data. The most critical and time-consuming task of the ECC technique is scalar multiplication; therefore modified and simplified the process of scalar number generation is used to reduce the computational efforts required. Thus proposed approach takes less time for all tasks of cryptography as compared to the conventional ECC technique. Image quality evaluation. The image quality evaluation is done using performance metrics for the proposed model designed. The performance for picture quality assessed regarding PSNR, MSE, RMSE (Root MSE), SSIM, and correlation for each tested image for a one-way DF based cooperative image communication model. All performance metrics required two inputs, such as original image (at transmitter side) and received image (at received side). Table 3. shows all outcomes for proposed image transmission model over the sensor network.

Table 3 Image quality investigation

	MSE	RMSE	PSNR	SSIM	SNR
boat.png	0.1289	0.3591	57.058	0.999873	28.863
barbara.png	0.1636	0.4045	56.025	0.999678	28.851
cameraman.png	0.1828	0.4276	55.543	0.999916	28.872
couple.png	0.1280	0.3579	57.089	0.999869	28.884
lena.png	0.0771	0.2777	59.292	0.999928	28.861
man.png	0.1042	0.3229	57.982	0.999866	28.872
Average	0.1443	0.3749	56.8	0.9998	28.852

All results show that the proposed model for cooperative image transmission achieved efficiency for the image quality also the quality all tested images are not comprised using the proposed methods at each phase of the communication model.

6. Conclusion

The efficient one-way cooperative image transmission model for remote sight and sound sensors arranged over Rayleigh blurring channels is the main research challenge because of the restricted capacities of sensor hubs, thus The proposed cooperative image transmission technique is assessed for three key performance metrics with new techniques, for example, PSNR and vitality productivity, The image is compressed, the compressed data is more vulnerable to the different wireless channel threats. This paper addresses the security issues for compressed data by using the modified ECC-based cryptography method. The key problem of the conventional ECC method is the complicated and time-consuming task of scalar multiplication which may consume the extra energy of sensor nodes,

References

1. Alhayani, B., & Ilhan, H. (2017). Hyper spectral image classification using dimensionality reduction techniques**.** International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering**,,** vol.5, pp.71-74.
2. Tong, X. M., Zhang, L., Yi, Z., & Hu, P. (2017). MBVCNN: Joint convolutional neural networks method for image recognition. *AIP Conference Proceedings*, 4982456.] H. Yang, K. W. Wong, X. Liao, W. Zhang and P. Wei, "A Fast Image Encryption and Authentication Scheme based on Chaotic

ISSN: 2776-0987 Volume 3, Issue 12 Dec. 2022

Maps," *Communications in Nonlinear Science and Numerical Simulation,* Volume 15,Issue 11, PP. 3507 – 3517, 2010. Vol. 15, no. 11, pp. 3507- 3517, 2010

3. X. Y. Wang, F. Chen and T. Wang, "A New Compound Mode Of Confusion And Diffusion For Block Encryption Of Image Based On Chaos," *Communications in Nonlinear Science and Numerical Simulation,* Volume 15, Issue 9, PP. 2479 – 2485, 2010.
4. Y. Wang, K. Wong, X. Liao and T. Xiang, "A Block Cipher with Dynamic S-Boxes Based on Tent Map," *Communications in Nonlinear Science and Numerical Simulation,* Volume 14, Issue 7, PP. 3089 – 3099, 2009.
5. Y. Wang, K. W. Wong, X. Liao and G. Chen, "A New Chaos-Based Fast Image Encryption Algorithm," *Applied Soft Computing,* Volume 11, Issue 1, PP. 514 – 522, 2011.
6. D. Chai andA. Bouzerdoum, "JPEG2000 image compression: an overview," *The Seventh Australian and New Zealand Intelligent Information Systems Conference,* 2001.
7. A. Skodras, C. Christopoulos, and T. Ebrahimi, "The JPEG 2000 still image compression standard," *IEEE Signal Processing Magazine,* vol. 18, pp. 36-58, 2001.
8. R. K. Kodali, "An efficient scalar multiplication algorithm for ECC in WSNs," International Conference on Control, *Instrumentation, Communication and Computational Technologies (ICCICCT),* 2014.
9. S. Xu, C. Li, F. Li, and S. Zhang, "An improved sliding window algorithm for ECC multiplication," *World Automation Congress,* 2012.
10. R.P. Jasmi, B. Perumal, and M.P. Rajasekaran, "Comparison of image compression techniques using Huffman coding, *DWT and fractal algorithm," International Conference on Computer Communication and Informatics (ICCCI),* 2015.
11. A. K. Singh, "Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images," *Multimedia Tools and Applications*, 76(6) (2017) 8881-8900. vol. 76,no. 6, pp. 8881-8900,2017.
12. BSA. Al Hayani and H. Ilhan,"Visual Sensor Intelligent Module Based Image Transmission in Industrial Manufacturing for Monitoring and Manipulation problems," Journal of Intelligent Manufacturing, vol.4,pp.1-14.2020.

ISSN: 2776-0987 Volume 3, Issue 12 Dec. 2022

13.B. Alhayani, A.A. Abdallah, "Manufacturing intelligent Corvus corone module for a secured two way image transmission under WSN", Engineering Computations, Vol. 37 No. 9, pp. 1-17. 2020.

14.Milind E. Rane, Umesh S Bhadade, "Comparative Study of ROI Extraction of Palmprint", IJCSN International Journal of Computer Science and Network, Volume 5, Issue 2, April 2016

15.Milind E. Rane, Umesh S Bhadade, "Multimodal System using Radon-Gabor Transform", International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS-2017) .(Scopus Published) K. A. MASCHER, H. STOGNER, A. UHL, "Comparison of Compression Algorithms: Impact on Fingerprint and Face Recognition Accuracy", *Proceedings of SPIE, Visual Communications and Image Processing*, Vol. 6508, 2007.

16.D. Lee, H. Kim, S. Tu, M. Rahimi, D. Estrin and J. D. Villasenor, "Energy-Optimized Image Communication on Resource-Constrained Sensor Platforms," *2007 6th International Symposium on Information Processing in Sensor Networks*, Cambridge, MA, 2007, pp. 216-225.

17.L.W. CHEW, W. C. CHIA, L. M. ANG, K. P. SENG, "Very Low Memory Wavelet Compression Architecture Using Strip Based Processing for Implementation in Wireless Sensor Networks", *Eurasip Journal on Embedded Systems,* Volume 2009, Number 1, Page 1. I. F. AKYILDIZ, T. MELODIA, and K. R. CHOWDHURY, "A Survey on Wireless Multimedia Sensor Networks," *Computer Networks, Elsevier*, Vol. 51, No. 4, pp. 921-960, 2007.

18.I. F. AKYILDIZ, T. MELODIA, and K. R. CHOWDHURY, "Wireless Multimedia Sensor Networks: A Survey,"*IEEE Wireless Communications Magazin*e, Vol. 14, No. 6, pp. 32-39, 2007.

19.I. F. Akyildiz, T. Melodia and K. R. Chowdhury, "Wireless Multimedia Sensor Networks: Applications and Testbeds," in *Proceedings of the IEEE*, vol. 96, no. 10, pp. 1588-1605, Oct. 2008.

20. S. Misra, M. Reisslein and G. Xue, "A survey of multimedia streaming in wireless sensor networks," in *IEEE Communications Surveys & Tutorials*, vol. 10, no. 4, pp. 18-39, Fourth Quarter 2008.

21.D. LEE, H. KIM, M. RAHIMI, D. ESTRIN, J.D. VILLASENOR, "'Energy-Efficient Image Compression for Resource-Constrained Platforms," *IEEE Transactions on Image Processing,* Vol. 18, No. 9, pp. 2100-2113, 2009.

22. M. NASRI, A. HELALI, H. SGHAIER, and H. MAAREF, "Energy-Efficient Wavelet Image Compression in Wireless Sensor Network", *International Conference on Communication in Wireless Environments and Ubiquitous Systems: New Challenges (ICWUS), TUNISIA.* pp. 1-7, 2010.
23. E. MAGLI, M. MANCIN, and L. MERELLO, "Low-Complexity Video Compression for Wireless Sensor Networks", *Proceedings of International Conference on Multimedia and Expo*. Vol. 3 no. 9, pp. 585-588, 2003.

24. A. MAMMERI, B. HADJOU, A. KHOUMSI, "A Survey of Image Compression Algorithms for Visual Sensor Networks", *ISRN Sensor Networks, Hindawi,* Vol. 2012, p.p 19 pages, 2012.
25. L. Ferrigno, S. Marano, V. Paciello and A. Pietrosanto, "Balancing computational and transmission power consumption in wireless image sensor networks," *IEEE Symposium on Virtual Environments, Human-Computer Interfaces and Measurement Systems, 2005.*, Messina, Italy, 2005, pp. 6 pp.-.
26. I. N. Laneman, "Cooperative diversity in wireless networks: algorithms and architectures," *Diss. Massachusetts Institute of Technology,* 2002.
27. J. Laneman, W. Gregory, "Distributed space-time coded protocols for exploiting cooperative diversity in wireless networks", *Global Telecommunications Conference*, GLOBECOM'02.IEEE.Vol. 1. IEEE, 2002.
28. E. Zimmermann, P. Herhold and G. Fettweis, "On the performance of cooperative diversity protocols in practical wireless systems," *2003 IEEE 58th Vehicular Technology Conference. VTC 2003-Fall (IEEE Cat. No.03CH37484)*, Orlando, FL, 2003, pp. 2212-2216 Vol.4.
29. J. N. Laneman, D. N. C. Tse and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," in *IEEE Transactions on Information Theory*, vol. 50, no. 12, pp. 3062-3080, Dec. 2004.
30. W. Wang, D. Peng, H. Wang, H. Sharif and H. Chen, "Energy-Constrained Distortion Reduction Optimization for Wavelet-Based Coded Image Transmission in Wireless Sensor Networks," in *IEEE Transactions on Multimedia*, vol. 10, no. 6, pp. 1169-1180, Oct. 2008.