International Research Journal of Advanced Engineering and Science

ISSN (Online): 2455-9024

A Novel Compression-Encryption Scheme Based on DWT and ECC for Securing the Transmission of Multimedia Data in IoT Environment

Khadija El Kinani[1], Salma Bendaoud[2], Fatima Amounas[3]

[1]RO.AL&I, PHD student, Faculty of Sciences and Technics, Moulay Ismail University of meknes, Errachidia, Morocco

[2]PHD, RO.AL&I Group, Faculty of Sciences and Technics, Moulay Ismail University of meknes, Errachidia, Morocco

[3]RO.AL&I, Computer Sciences Department, Faculty of Sciences and Technics, Moulay Ismail University of Meknes, Errachidia, Morocco

Abstract— *The Internet of things (IoT) is a kind of advanced information technology that has attracted much attention in today's world. The security of multimedia data and its applications has become a building block of any digital communication technology. Video encryption is commonly used as a technique for providing security for digital video among the Internet of Things applications. The transmission of video is a susceptible issue due to the large volume and the significant information of these data. So, it is necessary to reduce the volume and save images in high quality by lossless compression. The joint image compression and encryption method is a promising solution due to its better security. In this paper, a new compression-encryption scheme for secure multimedia data based on the merging of AES and ECC cryptosystems. The compression is performed by using the Wavelet Transform technique. Pre-compression encryption is applied in order to make the algorithm robust. For the evaluation purpose, we evaluate its performance by comparing the PSNR and SSIM values of the original and encrypted image. The simulation results using Matlab show that the suggested algorithm achieves high security feature and it is efficient for encrypting media data content. Practical implementation proved that the proposed encryption algorithm is suitable for multimedia encryption applications.*

Keywords— *Internet of Things, Compression, Image encryption, Discrete Wavelet Transform, ECC, Hybrid System.*

I. INTRODUCTION

The Internet of Things (IoT) is a promising technology of the future that is expected to connect billions of devices. The increased number of communications is predicted to generate mountains of data, and data security can be a threat. IoT technology, involving the use of embedded devices, differs from computers, laptops, and mobile devices [1]. This technology is used in many different sectors, including domestic, healthcare, telecommunications, the environment, industry, construction, water management, and energy. With the fast growth of IoT, digital technology IoT-based becomes an integral part of human life. It makes multimedia data easy to share with various users for specific purposes. A large amount of image information can be stored and transmitted as quickly as possible. Security and privacy issues have emerged as critical challenges that can potentially compromise their successful deployment in many data-sensitive applications. Cryptography is one of the dominant solutions to ensure the confidentiality of information. Due to the rapid application of multimedia technology, IoT requires lightweight encryption techniques. The design of architectures for multimedia security encryption algorithms needs a great deal of effort to be suitable for embedded and mobile objects with low computational resource constraints. Various IoT applications have been developed, requiring the transmission of a large amount of multimedia data such as images, audio files, or videos [2-3]. The existing standards provide encryption to text files, but they fail to provide the same security to multimedia data such as video, audio, images, etc. Recently, video encryption has received ever-increasing research interest from cryptographers in many IoT applications. Digital image or video encryption is an important issue and has been widely used in recent times to ensure security. Several encryption and decryption cryptosystems are available to secure images from unauthorized users. The asymmetric encryption approach is shown its imperative features comparing to its biggest competitors RSA by offering significantly lower computational workload, lower processing unit consumption, and lower memory usage. In the last few years, the application of elliptic curves in cryptography has been attracting the increased attention of many authors. They have opened a wealth of possibilities in terms of security. The security of elliptic curve cryptographic schemes is based on the difficulty to solve the Elliptic Curve Discrete Logarithmic Problem (ECDLP). Although several research works have been shown that this approach provide the best results, there is still need to improve the previous approaches. This paper focuses on protecting confidentiality and integrity of multimedia information, which is one of the crucial security features for many applications in the IoT. A joint compression and encryption scheme is a promising method for transmitting image data securely and efficiently over public networks [4]. By combining the compression and encryption operations, more uncertainty is achieved in the size of the encrypted image. There exist many image compression and encryption algorithms [5-8]. However, to achieve robust security and compression together is still a challenging task. In this context, the main motivation of this work is to propose a novel compression-encryption scheme based on hybrid approach, which is computationally faster and secure. The proposed model integrates the data reduction at the multimedia IoT devices by applying data compression using wavelet transform technique and data encryption with high security level based on the merging of AES and ECC for efficient encryption of video frames. The simulation results in MATLAB show that the whole scheme is suitable for secure IoT multimedia communication.

The main contributions of this work are:

- To suggest a new compression and encryption scheme for improving the security in the IoT environment.
- To perform the compression by using discrete wavelet transform.
- To adopt the hybrid AES-ECC approach to provide the required security features such as confidentiality, integrity of multimedia information.
- To evaluate the performance of the proposed scheme by comparing the PSNR and SSIM values of the original and encrypted image.

The remainder of this paper is arranged as follows: Section 2 describes a review of some previous and related works. Section 3 investigates the basic theory on elliptic curve 3 and compression technique. Section 4 explains the proposed compression-encryption scheme. Section 5 is devoted to the experimental simulation and security analysis. Finally, the last section draws the conclusion of this paper.

II. Related Works

Due to the sensitive information that can be exchanged over IoT technology, the security of these networks is critical. Recently, a considerable amount of attention has been devoted to research about how to ensure the confidentiality and integrity of multimedia data in the IoT environment [9-11]. Encryption is one of the best way to make IoT networks secure since so much data is being transferred. Image compression is a method of reducing the image size without compromising its quality to a large extent. Image security is a major challenge for protecting images against unauthorized access. One of the most important approaches is a joint compression and encryption scheme [12-13]. Due to the recent growth of compression-encryption strategies in various applications, many researchers have been inspired to adopt compression and encryption schemes to ensure the security of multimedia data. For instance, Ponmani E. et al. [14] proposed an ECC encryption scheme to secure the compressed images transmitted via the wireless network. They performed the compression by using DWT, which provides a high compression ratio and robustness for protecting the digital image integrity. DWT avoids blocking artifacts that cause the loss of valuable information. It produces an image with better quality. Next, Tsai et. al. [15] proposed a chaos-based joint compression and encryption schemes. The authors used the auxiliary data structures to effectively improve an existing chaos-based scheme. Then, they solve the issues of large multidimensional lookup table overheads. This improves the accuracy of frequency distribution estimations. Another work was carried out by Wang et al. [16]. The authors proposed an image compression scheme with personal identity information based on CS and Secret Image Sharing. Their scheme can complete compression and encryption, but cannot resist the man-in-the-middle attack. So any-one can disguise himself as a legal person to access the information. After that, Chaudhary, Pratibha et al. [17] suggested a joint image compression and encryption scheme that works for different image dimensions and different image sizes. The compression and encryption is done simultaneously which makes computations faster and secure at the same time. Their scheme takes just a few seconds as computational time for compressing larger images. This simultaneous compression and encryption scheme had interested many researchers. In [18], Bergeron, Cyril et al. present some works in the field of video crypto-compression with a particular focus on selective encryption adapted to video compression standards. Further, Karthick Panneerselvam, et al.[19] proposed an approach to include the encryption/decryption into the video embedding process. The authors disclosed a way for embedding a secret video inside a cover video in their previous works. They attempt to improve this approach by combining compression, encryption, decryption, and secret information embedding to provide a more secure data transfer. Another work most recently proposed by H. Dweik et al. [20] to maintain data security over the networks. The authors suggested an enhanced algorithm of the AES-ECC hybrid encryption system, which has good flexibility and versatility, and optimized the design of the ECC function according to the characteristics of wireless sensor networks. Another work most recently proposed by Bilal S.A. Al-hayani et al. [21] with the rise of the optimized Video Internet of Things. The authors suggested an hybrid approach employing the wavelet image transform for the compression combined with Elliptic Curve Cryptography for video encryption. Their method attempt to increase image quality while minimizing processing time and error rates. But still there is a need to reduce the computational costs in order to overcome the major security issues. In this context, we introduce a novel compression-encryption scheme with improved security level by using the robustness of ECDLP and DWT.

III. Preliminaires

A. *Elliptic Curve Cryptography*

In this section, we introduce some basics notions connected with elliptic curves. Elliptic Curve Cryptography (ECC) was introduced as an alternative to other public key cryptosystem present such as RSA and ElGamal Cryptosystems. ECC provides greater security and better performance than other cryptosystems. The most used elliptic curves are defined on prime fields F_p or binary fields F_2^m. Here we begin with the definition of an elliptic curve over a finite field F_p. The elliptic curve E over F_p is denoted $E(F_p)$.

1) *Definition of Elliptic Curves*

An elliptic curve over a field F_p is the set of points satisfying the Weierstrass equation:

$$y^2 + a_1xy + a_3y = x^3 + a_2x2 + a_4x + a_6 \qquad (1)$$

where a_1, a_3, a_2, a_4, $a_6 \in F_p$, and also an element denoted Ω, called the point at infinity,

The equation (1) can be simplified according to the characteristic of the used finite field. In the prime field, the equation of the curve is given as follows:

$$E: y^2 = x^3 + ax + b; \text{ with } 4a^3 + 27b^2 \neq 0 \qquad (2)$$

By substituting different values for x and y in equation (2), the ECC points are generated. The set of all elliptic curve points is denoted by E_p (a, b). The point at infinity denoted by ‘Ω‘ is the additive identity for the abelian group. All the entities in the elliptic curve cryptosystem agree upon a, b, p, G, n which are called Domain parameters of ECC. The basic operations on elliptic curves are addition and doubling [22]. The elliptic curve E over a finite field $E(F_p)$ can be made into an abelian group by defining an additive operation on its points.

The Rules for Addition

For each three points $P(x_1, y_1)$;$Q(x_2, y_2)$ and $R(x_3, y_3)$ of the elliptic curves defined in Eq(2) such that R = P + Q. Then R is given by:

i) $R = \Omega$ for $x_1 = x_2$ and $y_2 = -y_1 - a_1x_1 - a_3$

ii) $x_3 = t^2+a_1t - a_2 - x_1 - x_2$ and $y_3 = -(t + a_1)x_3 - s - a_3$

with

$$t = \begin{cases} \frac{y_2-y_1}{x_2-x_1}, \text{if } P \neq Q \\ \frac{3x_1^2+2a_1x_1+a_4-a_1y_1}{2y_1+a_1x_1+a_3}, \text{if } P = Q \end{cases}$$

$$s = \begin{cases} \frac{y_1x_2-y_2x_1}{x_2-x_1}, \text{if } P \neq Q \\ \frac{-x_1^3+a_4x_1+2a_6-a_3y_1}{2y_1+a_1x_1+a_3}, \text{if } P = Q \end{cases}$$

The addition operation defined above turns $E(F_p)$ into an abelian group that has Ω as the identity element.

The Discrete Logarithm Problem

The elliptic curve cryptography (ECC) has recently received much attention since smaller ECC key sizes provide the same security level as RSA. The strength of Elliptic Curve Cryptography depends on the hard problem known as Elliptic Curve Discrete Logarithmic Problem. For two points on $E(F_p)$ such as Q=αP. Indeed, knowing P and α, it is relatively easy to calculate Q=αP for given α and P. However, only knowing P and Q, it is hard to determine α. It can be used not only as the public key cryptography to encrypt information [23-25], but also as a signature system [26].

B. *Compression-Encryption Technique*

With a growing need for data and information transmission in a safe and quick manner, research on image protection begins to take form [27]. There are two key issues related to the exchange of image data through public networks: the increasing size of image data and the weak security of image data during transmission. These problems can be overcome by combining compression and encryption techniques. To address this issue, the combination of these two methods may be classified into three categories: (i) a cryptographic technique followed by a compression technique [encryption-compression], (ii) a compression technique followed by a cryptographic method [compression-encryption], and (iii) both techniques employed in a single process [hybrid compression-encryption]. According to [28], the application of data compression before its encryption will reduce duplicate parts of data that are prone to cryptoanalytic exploitation. In this context, an effective and robust compression-encryption system must be implemented as a helpful way to address the security and protection issues in multimedia communication applications.

C. *Discrete Wavelet Transform*

The wavelet transform (WT) represents an image as the sum of wavelet functions (wavelets) with different locations and scales. The wavelet transform can be broadly classified into two types: (i) continuous wavelet transform and (ii) discrete wavelet transform. For long signals, a continuous wavelet transform can be time-consuming since it needs to integrate at all times. To overcome the time complexity, the discrete wavelet transform was introduced. Discrete Wavelet Transform (DWT) has been used more frequently in many image processing applications like image compression, image encryption, fusion, etc. DWT has localized in time and frequency domains, simultaneously revealing spatial and frequency views [29]. It decomposes the image at a multi-resolution level, which helps analyze it at different resolutions. Due to the multi-resolution property of DWT, information that is unnoticed at one level may become noticeable at another level. DWT is a crucial compression technique that is used to compress the image effectively [30].

IV. Proposed Methodology

In this section, we will present our investigations that aim to increase the security of exchanges over unsecured channel. Currently, multimedia data, such as images, audio, and video, are growing rapidly as an essential avenue for the sharing, and storage of data in our daily lives. In this context, the confidentiality and the integrity of multimedia data suffer from serious security issues. The main aim of this work is to develop a new compression-encryption scheme for the secure transmission of multimedia data in IoT applications. First, each image is compressed by using the wavelet transform technique. Then, to maintain the integrity of the transmitted data via our proposed cryptosystem, we adopted the hybrid approach based on AES and ECC.

The AES algorithm is employed to encrypt the extracted images, and then the generated key is encrypted by the ECC mechanism. Figure 1 illustrates the designer of the proposed approach.

V. Results and Disscussion

A. *Experimental Results*

Numerical simulations were performed using different security measures to show the security and efficiency of the proposed algorithm. Several frames taken at different times in the video are encrypted using the proposed algorithm. Figures 2, 3 and 4 show the clear images taken at different times in the video, with their encryption and decryption results respectively. Comparing the clear images and their encryption, we see that there is no visible information in the encrypted images from the clear images.

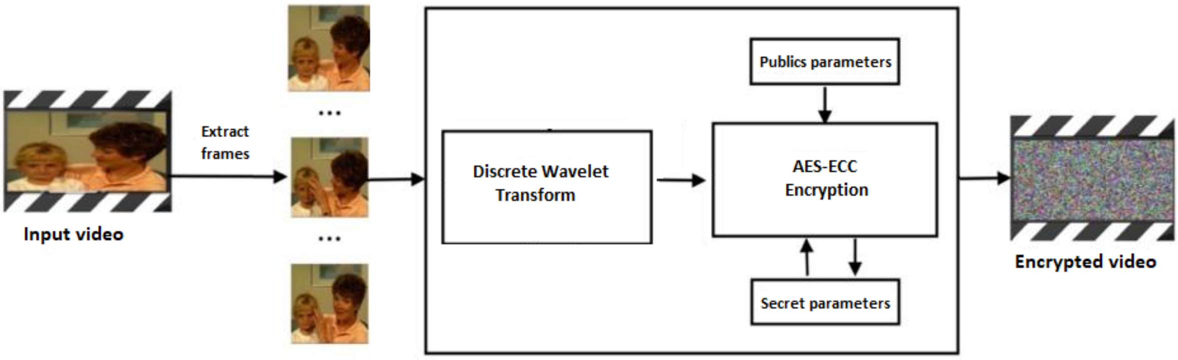

Fig. 1. The architecture of the proposed Approach.

First Plain image | Middle Plain image | Last Plain image

Fig. 2. Three frames of the video taken at different times.

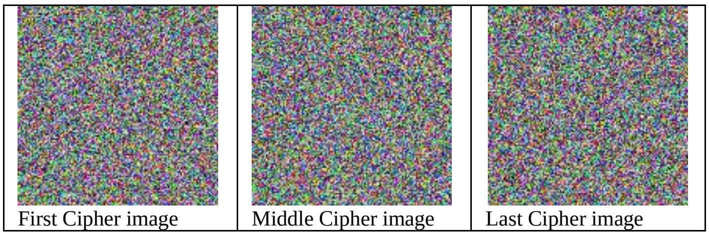
First Cipher image | Middle Cipher image | Last Cipher image

Fig. 3. Results of encryption process.

First Plain image *Middle Plain image* *Last Plain image*

Fig. 4. Results decryption process

From the Fig. 2 and Fig. 4, we can see that the image quality does not change during the process of compression/encryption. This indicates that our algorithm show a good compression performance without affecting image quality.

B. *Performance analysis*

In this section, numerical experiments and performance comparisons are given in detail under the Matlab R2015a platform in order to demonstrate the efficiency of the proposed scheme. Three test images (the first image, the middle image, and the last image) are used. This section includes aspects of the histogram analysis, the structural similarity index (SSIM), the peak signal-to-noise ratio (PSNR), the correlation analysis, and the entropy analysis.

1) *Histogram Analysis*

The histogram is one of the criteria in the cipher text to analyze the value distribution of an image, which is uniform and has random behavior in an ideal state. In this work, three test images taken at different times in the video (First Image, Middle Image, Last Image) were used in the analysis. The histogram plots of the plain images and the encrypted images are shown in Figures 5 and 6. The result shows that the histograms of the encrypted images are uniform after encryption. Subsequently, encryption prevents the adversary from extracting meaningful information using the histograms of the encrypted images.

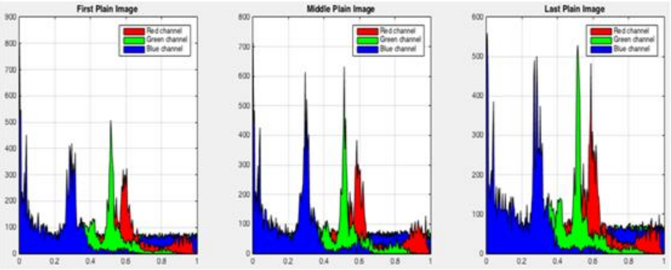

Fig. 5. Histograms of plain images.

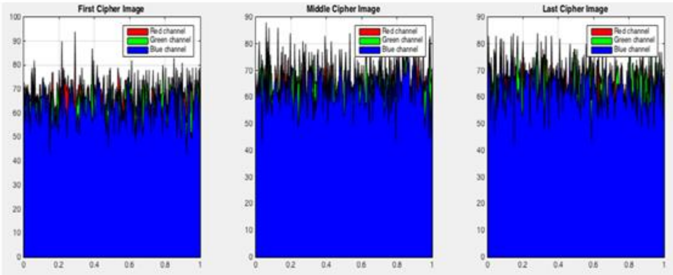

Fig. 6. Histograms of cipher images.

2) *Decryption Performance*

In this section, we will present the performance of the method in terms of calculated quality and evaluated quality by using two parameters: PSNR and SSIM.

- *Peak signal-to-noise ratio (PSNR)*

The peak signal-to-noise ratio (PSNR) is widely used to objectively evaluate video quality [31]. More precisely, PSNR is a widely used index to quantify the similarity between the plain image and the recovered image after processing to judge the effectiveness of compression. Here, PSNR is defined as the quality measurement between the original frames and encrypted one. It is calculated by using the mean square error (MSE) which should ideally be as low as possible for lossless decryption. Mathematically, It is computed as follows:

$$PSNR = 10log_{10}(\frac{M^2}{MSE})$$

Where M = maximum possible value of the image pixel.

Figure 7 shows the plot of PSNR values for the encrypted frames. For our approach the PSNR between the original video and the decrypted video remains high (33.3690) and the PSNR of 9.2636 between the original video and its encrypted version is low. This implies that the encryption process shows true randomness in each frame. Hence, the proposed method produced the highly distorted video. Thus, Our scheme can be considered for video protection in the Internet of Things.

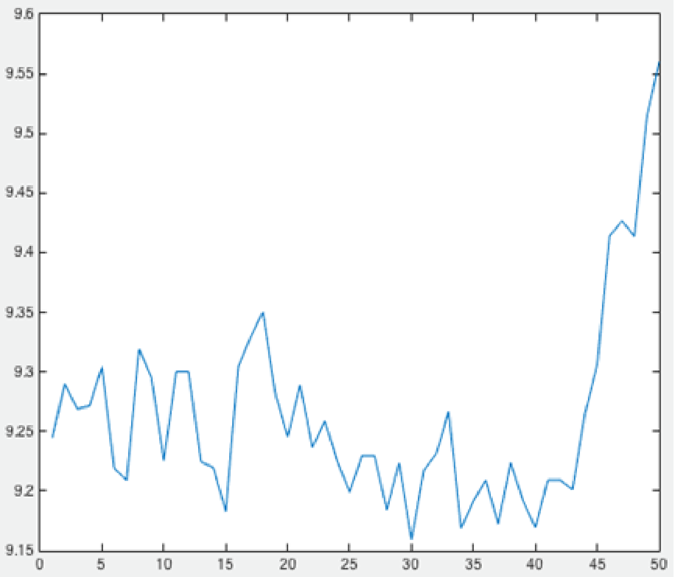

Fig. 7. PSNR for encrypted video frames.

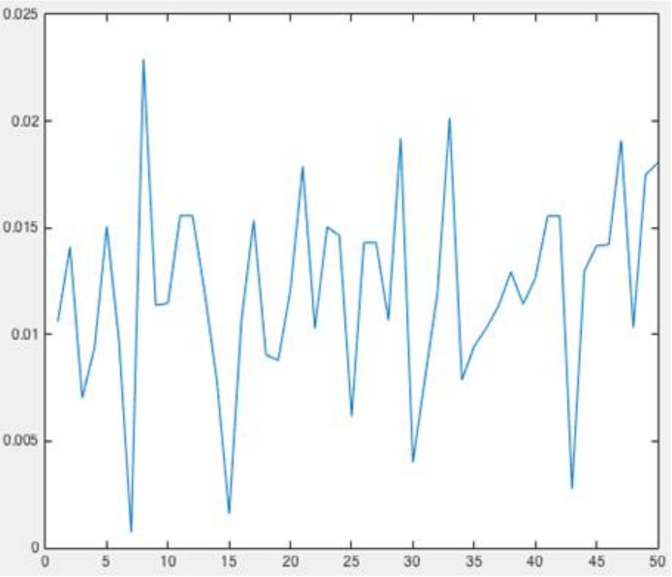

Fig. 8. SSIM for encrypted video frames.

- Structural similarity index (SSIM)

SSIM is designed to evaluate the degradation according to the local context of the defect; it is made a weighting of 3 parameters: Luminance, Contrast and Contours. SSIM ranges from 0 to 1, and SSIM is close to 1 when two images are similar. Figure 8 shows the results according to the proposed algorithm of SSIM. It can be seen that the SSIM value of the video sequence after encryption is almost zero. In other words, after encryption, the original video is far behind the encrypted video.

3) Coorelation Analysis

Correlation analysis is the relationships among pixels and their neighboring pixels for a natural image at horizontal, vertical and diagonal directions. The values of those relationships can be shown in TABLE 1. From the values, the correlation of adjacent pixels for plain image are all close to 1, while the produced the highly distorted video. Hence, this method can be a suitable solution while maintaining security of videos for most of the applications.

TABLE I. Correlation of two adjacent pixel of three frames of video

Image		Horizontal	Diagonal	Vertical
Plain image	First	0.9762	0.9498	0.9638
	Middle	0.9733	0.9463	0.9613
	Last	0.9736	0.9440	0.9601
Cipher image	First	0.0046	-0.0039	-0.0051
	Middle	3.8490e-04	0.0029	6.0006e-04
	Last	8.9783e-04	-0.0046	0.0098

4) Information Entropy

Information Information Entropy (IE) measures the uncertainty of the information occurrence per bit in an image and is widely used in the applications of image compression and encryption [32-34]. It can be defined as follows:

$$H(s) = \sum_{i=1}^{2^N-1} p(s_i)\, log_2 p(s_i)$$

where $s_1, s_2, \ldots, s_2^{N-1}$ are the sources, and $p(s_i)$ is the probability of s_i.

Accordingly, the entropy of cipher image with 256 gray levels in an effective algorithm should ideally be 8. To explain the information entropy of the original image and the cipher image, the original images and the cipher images are selected as the test images, and then corresponding values of entropy for different images can be obtained. Table II reveals that the entropy values of all cipher images are close to 8 and have the ideal values.

TABLE II. Information entropy

	Plain image	**Cipher image**
First image	7.6122	7.9961
Middle image	7.5892	7.9966
Last image	7.6159	7.9967

II. CONCLUSION

With the emergence of IoT, the multimedia contents are widely used in several applications nowadays. The widespread use of multimedia data makes media content security and protection increasingly urgent and necessary. In this paper, a joint compression and encryption algorithm based on the hybrid approach and wavelet transform is investigated. Firstly, the compression using a wavelet transform technique is performed. Secondly, an encryption approach based on the merging of ECC and AES is implemented. The simulation results indicated that the proposed scheme achieves protection, integrity, and security of the input video. The experimental results and performance analysis show that the proposed method not only can achieve good encryption and perfect hiding ability but also can resist any cryptanalytic attack. This proposed algorithm works easily for image or video files and provide satisfactory security. So, the proposed method can be used in IoT applications to achieve reliable security and robustness for the transmitted multimedia data. Therefore, it is very suitable for the security of IoT multimedia applications. In future work, there is a great interest in the detailed evaluation of performance and analysis of this scheme on real domains of IoT environment. Furthermore, the proposed protocol may be investigated and analyzed to be deployed in Healthcare systems and other similar fields.

REFERENCES

[1] Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M.“Internet of Things: A survey on enabling technologies, protocols, and applications”. IEEE Commun. Surv. Tutorials, vol. 17, no 4, pp.2347-2376, 2015.

[2] C. Tiken and R. Samlı , "A Comprehensive Review About Image Encryption Methods", Harran Üniversitesi Mühendislik Dergisi, vol. 7, no. 1, pp. 27-49, (2022).

[3] Rafik Hamza, Alzubair Hassan, Teng Huang, Lishan Ke, and Hongyang Yan, “An Efficient Cryptosystem for Video Surveillance in the Internet of Things Environment”, Hindawi, vol 2019, 2019. doi. 10.1155/2019/1625678

[4] A. Alfalou, C. Brosseau, N. Abdallah, “Simultaneous compression and encryption of color video images”, Optics Communications, vol. 338, Pages 371-379, 2015.

[5] Li, Peiya & Lo, Kwok-Tung. ”A Content-Adaptive Joint Image Compression and Encryption Scheme”, IEEE Transactions onMultimedia, vol. 20, no. 8, pp. 1960-1972, 2018.

[6] Zhe Nie, Zheng-Xin Liu, Xiang-Tao He, Li-Hua Gong, ”Image compression and encryption algorithm based on advanced encryption standard and hyper-chaotic system”, Optica Applicata, Vol. XLIX, No. 4, 2019.

[7] Nasrullah, Jun Sang, Muhammad Azeem Akbar, Bin Cai, Hong Xiang and Haibo Hu, ”Joint Image Compression and Encryption using IWT with SPIHT, Kd-Tree and Chaotic Maps”, Applied Sciences, vol. 8, no 10, 1963, 2018.

[8] Ijaz Ahmad, Seokjoo Shin,”A novel hybrid image encryption–compression scheme by combining chaos theory and number theory”, Signal Processing: Image Communication, vol. 98, 2021.

[9] M. K. Mishra and S. Mukhopadhyay, "Concurrent Video Encryption and Compression for Secure Storage and Transmission," *2019 International Conference on Computing, Power and Communication Technologies (GUCON)*, New Delhi, India, pp. 371-379, 2019.

[10] Bruno Carpentieri, "Efficient Compression and Encryption for Digital Data Transmission", Security and Communication Networks, vol. 2018, Article ID 9591768, 9 pages, 2018.

[11] Walid El-Shafai, Ahmed K. Mesrega, Hossam Eldin H. Ahmed, Nirmeen A. El-Bahnasawy, Fathi E. Abd El-Samie, “An efficient multimedia compression-encryption scheme using latin squares for securing Internet-of-things networks”, Journal of Information Security and Applications, vVol. 64, 2022.

[12] Ahmed, Mahmood Ali, and Khamees Khalaf Hasan. "Data Compression and Encryption for Remote Sensor Networks Using Different Techniques Methods." JCIT vol.23, no.2: pp.39-49, 2021.

[13] Nasrullah, Jun Sang, Muhammad Azeem Akbar, Bin Cai, Hong Xiang and Haibo Hu, ”Joint Image Compression and Encryption using IWT with SPIHT, Kd-Tree and Chaotic Maps”, Applied Sciences, vol. 8 (10), 1963, 2018.

[14] Ponmani E, Nandhini E, Karthika K, Saravanan Palani, “Secured Transmission of a compressed image by using ECC”, International Journal of Pure and Applied Mathematics, Vol. 119, No. 12, pp. 13387-13396, 2018.

[15] Tsai, C. J., Wang, H. C., & Wu, J. L. “Three Techniques for Enhancing Chaos-Based Joint Compression and Encryption Schemes”. Entropy, 21(1), 40, 2019.

[16] P. Wang, X. He, Y. Zhang, W. Wen, and M. Li, ‘‘A robust and secure image sharing scheme with personal identity information embedded,’’ Comput. Secur., vol. 85, pp. 107–121, Aug. 2019.

[17] Chaudhary, Pratibha & Gupta, Ritu & Singh, Abhilasha & Majumder, Pramathesh & Pandey, Ayushi. “Joint image compression and encryption using a novel column-wise scanning and optimization algorithm”. Procedia Computer Science. vol. 167, pp. 244-253, 2020.

[18] Bergeron, Cyril & Hamidouche, Wassim & Déforges, Olivier. “Crypto-compression of Videos”, pp. 129-171, 2022.

[19] Karthick Panneerselvam, K. Rajalakshmi, V. L. Helen Josephine, Dhivya Rajan, L. Visalatchi, K. Mahesh, Meroda Tesfaye, "Improving the Security of Video Embedding Using the CFP-SPE Method", Journal of Engineering, vol. 2022, Article ID 6903695, 5 pages, 2022.

[20] H. Dweik, and M. Abutaha, "A Survey of Lightweight Image Encryption for IoT", in Lightweight Cryptographic Techniques and Cybersecurity Approaches. London, United Kingdom: IntechOpen, 2022.

[21] Alhayani, Bilal et al. “Optimized video internet of things using elliptic curve cryptography based encryption and decryption”, Computers and Electrical Engineering, vol. 101. Pages: 108022, 2022.

[22] Nagaraj, S., Raju, G. & Rao, K. Image encryption using elliptic curve cryptograhy and matrix. Proc. Comput. Sci. 48, pp.276-281, 2015.

[23] Geetha G, Padmaja Jain , ” Implementation of Matrix based Mapping Method Using Elliptic Curve Cryptography ”, International Journal of Computer Applications Technology and Research Vol. 3, Issue 5, pp. 312-317, 2014.

[24] Piyush Raghav, Amit Dua, “Security and Cryptography in Images and Video Using Elliptic Curve Cryptography (ECC), pages 30, e-Book ISBN 9780429435461, 2018.

[25] Hayat U, Ullah I, Azam NA, Azhar S. A Novel Image Encryption Scheme Based on Elliptic Curves over Finite Rings. Entropy (Basel), 19;24(5):571. 2022.

[26] C.-H. Tsai and P.-C. Su, ‘‘An ECC-based blind signcryption scheme for multiple digital documents,’’ Secur. Commun. Netw., vol. 2017, pp. 1–14, 2017.

[27] G. Suseela, Niharika Kumari and Y. Asnath Victy Phamila, “Secured Image Compression using Wavelet transform”, Vol. 9, Issue: 33, Pages: 1-6, 2016.

[28] Soumya Babu H, Vijayakumar N. and Gopakumar. K, “Discrete Wavelet Transform Based Cryptosystem”, International Journal on Recent and Innovation Trends in Computing and Communication, vol. 10, no. 11, pp. 47-52, 2022.

[29] V.V. Sunil Kumar and M. Indra Sena Reddy, “Image Compression Techniques by using Wavelet Transform”, Vol 2, No.5, Journal of Information Engineering and Applications, 2012.

[30] Ga, H. & Zeng, Wenjuan, “Image compression and encryption based on wavelet transform and chaos”, Computer Optics. vol. 43. pp. 258-263, 2019.

[31] Huynh-Thu, Q., Ghanbari, M. “The accuracy of PSNR in predicting video quality for different video scenes and frame rates”, Telecommun Syst, 49, pp.35-48, 2012.

[32] Setyaningsih, E. and R. Wardoyo, “Review of image compression and encryption techniques”, International Journal Of Advanced Computer Science And Applications, vol. 8, Issue 2, 2017.

[33] Wang, X. & Su, Y. “Color image encryption based on chaotic compressed sensing and two-dimensional fractional Fourier transform”. Sci. Rep. 10, 18556, 2020.

[34] Gao, X. et al. “A new image encryption scheme based on fractional-order hyperchaotic system and multiple image fusion”. Sci. Rep. 11, 15737, 2021.