

Enhancing IoT Security: Integrating Hyperelliptic Curve Cryptography Scheme for Secure Video Data Transmission

Talluri Jyothi¹, Sarikonda Sindhuja¹, Peram Prashanthi¹

¹Assistant Professor, Department of Computer Science and Engineering

¹Malla Reddy Engineering College and Management Sciences, Medchal, Hyderabad, 501401, Telangana, India

Abstract

In the modern world, digitalization plays an increasingly important part in the applications that people use on a daily basis. The Internet of Things (IoT) is essential to its successful adoption in the future because it enables automation, remote monitoring, and predictive analysis. IoT stands for "internet of things," and it refers to both a device that is connected to the internet as well as a mix of embedded technologies, such as actuators and sensor devices. Additionally, it includes both wired and wireless communication equipment, in addition to actual physical items that are connected to the internet. The Internet of Things is finding widespread application in a wide variety of industries, including smart classrooms, smart banking, smart homes, smart agriculture, smart healthcare applications, and many more. This article discusses the creation of a hybrid steganography-cryptography system for video data transmission in an Internet of Things environment. The goal of this scheme is to effectively secure information that is based on the IoT. Nevertheless, the penetration of attackers is becoming more important as an increasing number of Internet of Things sensor nodes are associated with an unlimited amount of data. In addition, the robustness of the system suffers whenever there is an increase in the number of unauthorized interventions within the network. In the beginning, people believed that RSA cryptosystems could be utilized to ensure security because of the reduced amount of computational work that they required. However, after a certain point is achieved, it will undoubtedly become obsolete because additional adversaries will have entered the system by that point. As the algorithm becomes more out of date, the level of computational complexity somewhat increases. However, the currently used versions of the original RSA and ECC algorithms are plagued by a number of issues because of the linear computing challenges they present. Therefore, the purpose of this work is to focus on the implementation of hyperelliptic curve cryptography (HECC) as an alternate option to the ECC in order to evaluate the dependability of cloud data in order to withstand malicious assault. Along with the text data, it is encrypted using a sophisticated cipher block chaining mechanism that is based on an encryption standard. The LSB approach is then used to generate stego video as the last step. The results of the simulation reveal that the proposed method has reliable performance in comparison to other methods that are currently considered state-of-the-art.

Keywords: Internet of Things, cloud security, cryptography, steganography.

1. Introduction

Video steganography [1] has become a major application for multimedia security in IoT field with respect to fields like smart classroom [2], smart banking [3], smart home [4], smart agriculture, smart healthcare application etc. It can be used to check the authentic user's legitimacy. Some of these techniques use the entire video to embed specific data on content. Use of the entire video to hide information can sometimes lead to a decrease in stego video visual quality [5]. This can be a major disadvantage for the security of video steganography in the real-time application. By the way, the quality of the video viewed by the user is undermined, which is one of the major criteria for videos distributed via the real-time application. The product of optimized stego video could overcome this disadvantage [6]. This optimal solution for video steganography not only provides high payload but

also compatibility with other steganography variables. z. For covered writing, video steganography is used. Every technique of video steganography hides a signal (the secret message) from a cover media, to receive a stego signal (stego video). In compliance with certain restrictions a hidden signal is located in an appropriate region of the cover signal. Such drawbacks include payload, numerical undetectability, imperceptibility, attack robustness, video data decoding, etc [7]. Some of these limitations not only contradictory but also multidisciplinary in nature. If the payload is increased, for instance, it may have a significant impact both on imperceptibility and numerical detestability and vice versa [8]. Also, robustness decreases as steganography attempts to increase both imperceptibility and payload. Some aspects of robustness are also covered by another discipline known as stego-analysis. It is therefore very difficult to find regions closer to the covered or secret signal in the cover media. Optimization is the optimal solution among many feasible solutions that are possible. This optimum solution is achieved by either minimizing the process constraints or maximizing the system efficiency [9]. An optimization mathematical formulation may be said to minimize any cost function $f(x)$, subject to certain conditions or constraints. The literature survey shows the use of rigorous mathematical analysis and calculus in the initial days to solve optimization problems. The strategies used in the next century are minimal length, least square methods, steepest descent methods, etc. While common, these methods have a certain inherent drawback because they are slow and they can only solve simple problems. Since the late 1980s, linear programming and dynamic approaches have started to solve large-scale problems [10].

The major contributions of this paper as follows:

- The input video sequence divided into multiple frames and each frame is encrypted by using the HECC cryptography method.
- The input text is preprocessed and encrypted by using the AES-CBC for further cryptography operation.
- Finally, the encrypted video data and text messages are embedded using the LSB steganography mechanism and generates the stego video sequence.

This paper is summarized follows through as: In Section 2, literature review for cloud data security with the comparison of methodology with defining problem, implication, merits and demerits. Section 3 gives the detailed information about the proposed methodology. Section 4 discusses about the results analysis and finally Section 5, concluded the summarization of whole paper.

2. Literature Survey

Most of the traditional works emphasize the combination of steganography and cryptography to securely transfer data across an unsecured network, and such a secret message communication scheme can be used in business applications across a network to control data theft and peer repudiation. They proposed an image steganography method similar to Jpeg, where the encrypted message is embedded in the quantized DCT coefficients [11], with the exception of the value-1, 0, + 1 of the DCT coefficients. The aim of the proposed technique is to create a process that incorporates the characteristics of steganographic and cryptographic techniques by integrating cryptography and throwing steganography.

By performing cryptographic functionality and also preserving its steganographic nature, the combining model may result in a steganographic image. The procedure first encrypts the secret message using substitution cipher and then uses the modified quantization table to insert the encrypted message into the frequency domain's high frequency coefficients. A replacement cipher is one where each character in the plaintext is replaced by another character in the ciphertext [12]. In this case, before embedding, the cover image is pre-processed. They suggested the pre-processing used in this

procedure. Images are the most common and commonly used steganography carrier medium. To a machine, an object is a set of numbers that in different areas of the image represent different light [13]. This numeric representation is a grid and is referred to as pixels for the individual points [14].

These pixels are the raster data of the image. Data hidden in images benefits from the finite power of the human visual system (HVS) with low sensitivity to changes in patterns and luminance [15]. Most digital steganography methods benefit from the margin between the multimedia carriers' numerical value and visual perception. In other words, the secret messages are embedded in the images by some minor distortions in the non-significant parts that are invisible to the system of human perception. Due to its importance in many applications, the number of digital images on the Internet has increased rapidly. In image steganography, the changes in the stego-image due to data embedding must be visually and statistically negligible in order to make it difficult to detect the steganography method. The most efficient way to hide data in an image is to change the content of the image, i.e. the pixel colors. Although crude, this technique hides a large volume of information within the image. The idea is to incorporate the data into a much larger object so that the changes are undetectable

Steganography techniques for modifying the image cover in the space domain are known as spatial domain techniques involving LSB encoding [16]. In spatial steganography the pixel values for hiding data are directly altered. Least significant bit substitution involves integration of secret data into bits, with a minimum weighting, so that the quality of original pixels is not affected. Either change the value of the pixel with ± 1 or leave it altered which depends on its nature and on the pixel value LSB. LSB based technique is a steganography technique based on the pixels. They have proposed a spatial image hiding scheme that embeds hidden image into true-color pixels. The hidden image can be both a color and a grayscale.

If a color image reduces the size of the data transmitted, the secret image is quantized where the secret image's red, green and blue components are quantified grossly. This proposed method is capable of hiding three hidden image types: the hiding of a secret colour-based image, the hiding of an actual color-based 256 image, and the hiding of a image of a real colour. They further argued that the proposed method allows for hidden embedding capacity and performs better in terms of PSNR and image quality. Most of previous works[17] on steganography images have been designed to hide gray scale images in gray scale host images. There are two disadvantages to this restriction. First, only gray images are used for hiding gray images. The proposed steganography approach was based on the sensitivity of human visual systems to object contrast which hides information within the spatial image domain. In order to measure the degree of flatness and pixel contrast, the method uses a comparison between the adjacent pixels.

3. Proposed Methodology

A steganography application was proposed shown in Figure 1 that uses as a basic technique the LSB to hide a Stego-message or plain text to be sent, which, has been previously encrypted with AES-CBC, to avoid that the text is read in case the existence of the message is detected inside the image, all this making a safe exchange of the key and without altering any of the characteristics of the Stego-image.

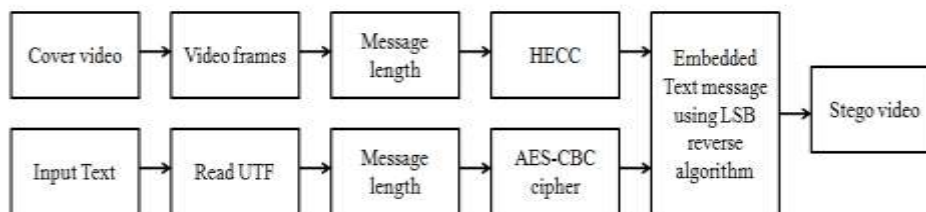


Figure 1: Description of the proposed method.

The combined scheme of mixing and encrypting the information should start with determining the best way to exchange the key by a secure means. Also, a way to delimit the information should be established by packaging the data with a specific character sequence, which indicates the exact position of the encrypted stemming message, as it is an encryption scheme that complies with the philosophy of Feistel networks by applying the reverse process, the message sent will be accessed hidden and encrypted, in a scheme that avoids the detection of hidden information, but if it is detected, it will maintain the integrity and security of the information. It is important to emphasize that the software tool will determine in a semi-automatic way the sizes of the Stego-image concerning the size of the Stego-message be sent, in other words, if the message is short a lower resolution image will be required, but it will always be necessary to fill in the information with a sequence of pseudo-random characters, to avoid the LSB plane of the Stego-image being empty and in this way, the detection tools will show the presence of a message in the Stego-image.

3.1 Hyperelliptic curve cryptography (HECC)

HECC is a public key encryption process based on the Jacobian of elliptical curve hypothesis and is used to create highly efficient, agile and compact cryptographic keys. Due to the development of prime numbers rather than standard forming techniques, rounded cryptography creates a key to the character of elliptic curves. The HECC approach can generate private and public keys, which make information more secure. The general position of the elliptic curve is given below by using genus g is the set of solutions, Jacobian of C is $J(C)$

$$J(C): Y^2 = X^{2g+1} + A_1X^{2g} + \dots + A_{2g}X + A_{2g+1}$$

Base-point generator $G(X) = X^{2g+1} + A_{2g+1}$ is chosen so that G is a very large value n and $n = 0$. HECC's key block is the collections of scalar points that are belonged to region g .

$$\{P_1, P_2, \dots, P_g\} \text{ and } \{Q_1, Q_2, \dots, Q_g\}$$

By adding the scalar points, new collection of g points generated such as $\{R_1, R_2, \dots, R_g\}$. The addition operation is performed by using the two elliptic curves with the precise formulation respectively. Recovery of g , however, understanding points P and Q are complicated or computationally infeasible as Hyper Elliptic Curve Discrete Logarithmic Problem. C is heavily built on real-time applications to solve predicting and resolving energy attacks. However, the ECC is not yet commonly applied cryptographic technique, and its theoretical basis in standard protocols. The HECC supports point multiplication i.e, repeated addition of two points. Numerous ECs are as of now licensed, making distinguishing new ones significantly more overwhelming. A bad random number generator can also lead to successful attacks and there may be underlying loops behind poor curve designs. To solve this proposed algorithm is described as follows;

Table 1: HECC Algorithm

key pair generation of HECC

Input: Domain parameters
Output: private key k and Public key R_g
Step 1: Choose a random integer $k \in [1, r - 1]$. Here r is the smallest possible integer of Divisor R_g
Step 2: Calculate $R_g = k * R_1$
Step 3: Generate the key pair as (R_g, k)
Encryption of HECC
Input: Private key k , Message m and Domain parameters
Output: cipher text (C_1, C_2, \dots, C_g)
Step 4: Consider m as message over hyper elliptic curves Jacobian J using reduced divisor M .
Step 5: Calculate the cipher texts as $C_1 = kR_1, C_g = M + kR_g$
Decryption of HECC
Input: Private key k , cipher text (C_1, C_2, \dots, C_g) and Domain parameters
Output: Message m
Step 6: Perform the successive subtraction operation $M = C_g - kC_1$
Step 7: generate message m from M using successive division

3.2. Encryption (AES and CBC)

AES is an encryption standard that is a symmetrical cipher or a finite block cipher (128 bits). It consists of three main rounds: The initial round, the standard round and the final round. The initial round is based on the AddRoundKey transformation, which performs an XOR operation between two matrices, the state matrix (which is the one containing the blocks of the original text) and the key matrix. After this, the standard round starts, this round consists of 4 processes: ByteSub, ShiftRow, MixColumns and AddRoundKey. ByteSub does the substitution of each of the bytes of the resulting array from the previous round, but this substitution depends on these same bytes. Using an inversion operation and a linear transformation that is carried out point by point to the matrix resulting from the initial round. ShiftRows applies shifts to the rows of the state matrix, so the first row is shifted by 0 bytes, the second by 1 byte, and so on. MixColumns performs the function of taking each column and multiplying it by a constant matrix. AES is applied in this way for encryptions up to 128 bits, but when there is a much longer message as in this case the input must be segmented into blocks. For this AES has among its modes of operation one called CBC (Cipher Block Chaining) that allows encrypting messages of greater length, its structure has shown in Figure 2. CBC proposes to segment in blocks of fixed length the information and to the first segment to apply an XOR operation with a random number to the one that is denominated like initialization vector, this initialization vector can be zero although it is not recommended since it would reduce the security level of the algorithm. Having the result of this exercise is encrypted with a key and thus the first encrypted block is obtained. This way, the next block is applied XOR together with the previous ciphertext and is also coded for the following blocks.

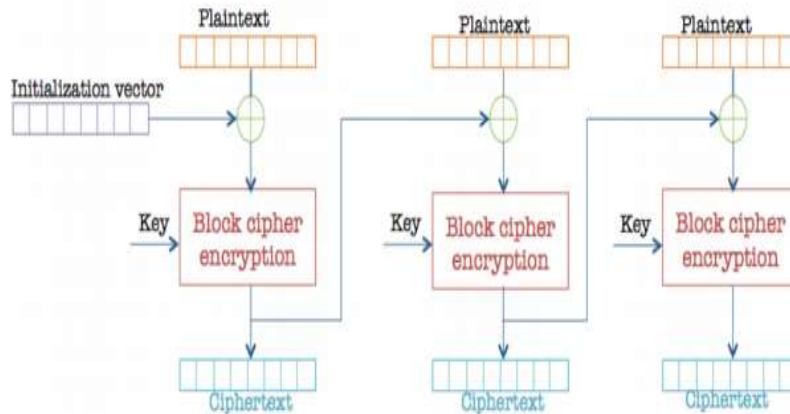


Figure 2: CBC block diagram

3.1. LSB (Least Significant Bit) technique

It is the most basic and therefore most widely used technique, in which plain text is converted into ASCII, this is then fed into a binary string and mixed into the least significant bit of text.

Initially, it is required to have installed the Opencv version 2 libraries, which allows operations with images and vectors, this library has some tools for digital signal and image processing. In this case, the function is defined: bits_generator, this function, is in charge of reading the message (msg) which was already read from a file that stores information in ASCII-UTF8 format, when reading the string of characters msg, the conversion of ASCII to its respective 8-bit value is performed with the command ord that gives the value in the whole format that corresponds to the value of the ASCII table of each of the data of the string of characters read, after this a string of binary numbers is created using a cycle that goes through each 8-bit data and puts it in a binary string with which it is ready to be mixed with each of the pixels of the chosen image to be the Stegoimage, the RGB structure of the imaged is shown in Figure 3. At this point, an algorithm must be made that somehow guarantees that the size of the Stego-message corresponds to the number of pixels that the image has, so to avoid limitations on the size of the message, the size of the image is preserved and the Stegomessage is repeated as many times as necessary, the value of the rows and columns of the image is determined and the message to be mixed is repeated a whole number of times, if at the end the exact size of the message does not match, bits are included in a random pattern to complete each of the pixels in the image. To avoid confusion for the receiver of the message, some delimiters of the message are defined, that the message is repeated more than once in the image serves as a methodology to verify the information.

4. Simulation Results

4.1 Dataset

There are two main factors in the proposed work, first one is data embedding process and second one is data extraction process. The analysis of proposed work is entirely based on these two factors only. The first method is based on the comparison of stego-video quality with original video while the second method is based on comparison of qualitative analysis of extracted secret message with the original secret message. Inserting the secret message into the video means insertion process, this process produces stego video which we can be played on any video player compatible to operating system. This shows that we can perform embedding process without any damage in original video. The extraction process produces message which is same as original message. There is no change in the message. After comparison we found no loss in the quality of video and the presence of secret

message in the video was undetectable. If we calculate the PSNR value for the video frame we get always value greater than 60, if value is more than 50 then it shows good quality of video.

4.2 Performance evaluation

The criteria to calculate the performance of the Steganography system is based on Robustness, Capacity and Security. Robustness: Means the ability to withstand or overcome adverse conditions. It describes the quality of the system. The performance of the system is measured in terms of (PSNR) Peak-Signal-to-Noise-Ratio. The quality comparison measurement of original video with stego video is known as Peak-Signal-to-Noise-Ratio. PSNR is measured in terms of decibels (dB). The high value of PSNR means the better video quality.

$$PSNR = 20 \log_{10} (MAX / \sqrt{MSE})$$

Where MAX= Maximum Possible Pixel Value of an image. Generally it is 255. The distortion between original video with stego video is measured in terms of Mean Square Error (MSE).
















Frame No.	Original frame	Stego frames			
		Scaling Factor			
		4	6	8	16
1		 PSNR 44.9055	 PSNR 41.5133	 PSNR 39.0782	 PSNR 33.2044
28		 PSNR 44.6255	 PSNR 41.4487	 PSNR 39.0139	 PSNR 33.0446
50		 PSNR 44.7747	 PSNR 41.3680	 PSNR 39.0632	 PSNR 33.0486

Figure 3: Some results after implementing the Steganography

Table 2: Performance comparison

Video Steg Models	PSNR	MSE	Encryption Time (s)	Decryption Time (s)
DWT+ HomomorphicEnc [16]	32.43	2.55	2143	1973
DCT+ HomomorphicEnc [18]	37.75	2.46	2324	1935
Proposed	73.2185	0.1798	1673	1747

From table 2, it is observed that the proposed method shows the high video quality as its PSNR is increased with reduced MSE. As well as the proposed method consumes the low time for both Stego-

Encryption and Stego-Decryption operations. From the table, it is observed that the performance of proposed method is improved compared to the DWT+ HomomorphicEnc [16], and DCT+ HomomorphicEnc [18].

4.3 Robustness Measures

The robustness of the system is measured according the Normalized Correlation (NC). NC is defined in the following equation.

$$NC = \frac{\sum_{i=1}^x \sum_{j=1}^y w(i,j)w'(i,j)}{\sqrt{\sum_{i=1}^x \sum_{j=1}^y w(i,j)^2}}$$

Where, w refers to the original secret image and w ' refer to recovered secret image. Figure 5 shows original and extracted secret image without any attack.

Several attacks are implemented on the stego frames for checking performance of the suggested scheme. Table 3 illustrates NC values for the extracted secret image after attacking the stego frame with several attacks.

Table 3: NC values after subjecting several attacks on the stego frame

Type of attack	Proposed	DWT+ HomomorphicEnc
No attack	1	0.9984
salt & pepper	0.9984	0.9829
Gaussian (mean = 0, variance = 0.0001)	0.9829	0.9692
Speckle (variance = 0.0002)	0.9984	0.9610
Cropping (50*50)	0.9807	0.9510
Compression	1	0.9984
Brightness (+35)	0.9610	0.9772

From the Table 3, it is observed that against several attacks the proposed method gives the robust performance compared to state of art approaches.

Conclusion

A Joint steganography-cryptography method was implemented using standard video processing and cryptography libraries that hide a flat text file in UTF-8 format of any size and such information when hidden and combined with the LSB technique, does not generate significant changes in the output image, mixed with the text and also after passing it through the AES-CBC block cipher algorithm, which shows us that the input and output image after the cipher process have a high entropy so if the output image is encrypted with a tool to verify the existence of a hidden message it could go unnoticed. The use of the LSB method is appropriate for the task of hiding information securely, but the secure sending of data is only guaranteed when using a standard cryptographic technique such as AES-CBC, which ensures that the secret is not violated if it is tried to break it. The sequential mixing of the key with the information by the CBC method guarantees a high complexity of the encryption algorithm and that it is not simply broken by any computational methods. By mixing two computer security techniques such as steganography and cryptography using a symmetrical block cipher, a double layer of security is given to the information by a method called mixed, named by some authors, which makes the sending of information safe and safeguards the secrecy of the data sent. This is the first work of the research group SIE (Embedded Computer Security) and it opens the door for

further work on the subject of steganography combined with classical cryptography since when measuring encryption times concerning the amount of information that needed to be hidden, it is noted that some of the processing times are excessive, so it is required to modify parts of the algorithm, verify if the algorithm and all the libraries can be run from the PC video card used and not from the CPU as it was currently run, another possible change or improvement would be to use cards with embedded Linux with dedicated use of video card for information processing or as an alternative solution, you can speed up the processing of the image using FPGA devices.

References

- [1]. C. H. Wang and S. L. Lin, "Why are People Willing to Pay for Cloud Storage Service?", In IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS), 2016, pp.1-6.
- [2]. I. G. N. A. Jayarana, A. A. K. A Cahyawan, and G. M. A. Sasmita, "Dynamic Mobile Token for Web Security using MD5 and One Time Password Method", International Journal of Computer Applications, Vol.55, No.2, 2012, pp.1-6.
- [3]. R. J. Mstafa and K. M. Elleithy, "A Highly Secure Video Steganography using Hamming Code (7,4)", In System, Applications and Technology Conference (LISAT), 2014, pp.1-.
- [4]. C. Abbas, et al. "Digital image steganography: Survey and analysis of current methods", Signal processing, Vol.90, No.3, 2010, pp.727-752.
- [5]. M. Bashardoost, G. B. Sulong, and P. Gerami, "Enhanced LSB image Steganography method by using knight Tour algorithm, Vigenere Encryption and LZW compression", IJCSI International Journal of Computer Science Issues, Vol.10, No.2, 2013, pp.221-227.
- [6]. R. Mritha, "Stego machine-video steganography using modified LSB algorithm", World Academy of Science, Engineering and Technology. Vol.74, 2011, pp.502-505.
- [7]. A. Swathi, and S. Jilani, "Video Steganography by LSB Substitution Using Different Polynomial Equations", International Journal Of Computational Engineering Research, Vol.2, No.5, 2012, pp.1620-1623.
- [8]. Lou, D., Wu, N., Wang, C., Lin, Z., Tsai, C.S., 2010. A novel adaptive steganography based local complexity and human vision sensitivity. Journal of Systems and Software 83(7), 1236-1248.
- [9]. Chang, C., Kiew, T.d., 2010. A reversible data hiding scheme using complementary embedding strategy. Information Sciences 180(16), 3045-3058.
- [10]. Samira Bouchama, Latifa Hamami, and Hassina Aliane : H.264/AVC Data Hiding Based on Intra Prediction Models for Realtime Applications. In: Proceedings of the World Congress on Engineering and Computer Science .Vol. 1. WCECS2012, USA.
- [11]. Sajedi, H., Jamzad, M., 2010. BSS: boosted steganography scheme with cover image pre processing. Expert Systems with Applications 37(12), 7703-7710.
- [12]. Yun Cao, Xianfeng Zhao, Denqquo Feng, Rennong Sheng. Video steganography with Perturbed Motion Estimation . DOI 10.1007/978-3-642-24178-9_14 .pp 193-207
- [13]. Seyyed Mohammad Reza Farschi. H. Farschi. A novel chaotic approach for information hiding in image. DOI 10.1007/s 1071-012-0367-5.
- [14]. Johnson, Neil F., and Sushil Jajodia. "Exploring steganography: Seeing the unseen." Computer 31.2 (1998): 26-34.
- [15]. Kumar, Arvind, and Km Pooja. "Steganography-A data hiding technique." International Journal of Computer Applications 9.7 (2010): 19-23.
- [16]. Mishra, Rina, Atish Mishra, and Praveen Bhanodiya. "An edge based image steganography with compression and encryption." 2015 International Conference on Computer, Communication and Control (IC4). IEEE, 2015.

- [17]. Burney, Micaela L. The History of Steganography and the Threat Posed to the United States and the Rest of the International Community. Diss. Utica College, 2018.
- [18]. Hashim, Mohammed Mahdi, et al. "Anextensive analysis and conduct comparative based on statistical attach of LSB substitution and LSB matching." International Journal of Engineering & Technology 7.4 (2018): 4008-4023.