https://doi.org/10.48047/AFJBS.6.7.2024.3650-3657

African Journal of Biological Sciences

Journal homepage: http://www.afjbs.com

Review Article Open Access

A New LSB-S Image Steganography Method using Galio field in Elliptic Curve Cryptography

[1]D.V.N. Bharathi, [2]Minnakanti Ajay Babu, [3]Kishore Varma Manthena, [4]Anjaneyulu. B, [5]K. Vijay Kumar

[1]Assistant Professor. Dept. of Electronics and Communication Engineering, SRKR Engineering College (A), Chinnamiram, Andhra Pradesh, India

[2]Assistant Professor, Dept. of Computer Science and Engineering, Sri Mittapalli College of Engineering (A), Tummalapalem, Guntur, Andhra Pradesh, India

[3]Assistant professor, Dept. of Computer Science and Engineering, SRKR Engineering College (A), Chinnamiram, Andhra Pradesh, India

[4]Assistant Professor, Dept. of Computer Science and Engineering, Sri Mittapalli College of Engineering (A), Tummalapalem, Guntur, Andhra Pradesh, India

[5]Associate Professor, Dept. of Computer Science and Engineering, Sri Mittapalli College of Engineering (A), Tummalapalem, Guntur, Andhra Pradesh, India

ABSTRACT: The most significant and fundamental problem in the field of message transmission through networks is secure data communication. Cryptography enables the creation of secure messages for the transportation of secure messages. By transforming the sender's message into a secret format known as cypher text, only the intended receiver will be able to comprehend the secret message's meaning. To hide a message's content and its underlying meanings, utilize steganography and cryptography respectively. The message is first encrypted using the Vernam encryption technique, and then it is integrated (encrypted) in the image using a new image steganography method called Least Significant Bit (LSB) with Shifting (LSB-S). Using a pixel's four LSBs, the LSB-S technique executed a left rotation operation and an XOR operation. The use of encryption and steganography together improves the security of hidden message. Following the suggested method's implementation, it was checked against several parameters and gave positive outcomes. To generate hidden messages for communication, several DNA based encryption or scrambling algorithms have been developed. But, all of the suggested DNA-based encryption algorithms are secure enough to provide better security than what is provided today. In this paper, they present the creation of a new LSB-S image steganography approach based on Galois-field

KEYWORDS: Cryptography, LSB-S, Galio Field, Vernam cipher, Steganography.

I. INTRODUCTION

When transmitting communication between sender and recipient, data communication security is necessary. It must be treated as private by the recipient. The process of achieving message confidentiality is known as cryptography. Encryption is the process of encrypting data or messages in order to protect them from various intruder attacks. Encryption is performed by converting a plaintext message into ciphertext using an encryption technique.

The protection of messages or data while they are being transmitted through networks is what security is all about. However, nowadays, it can be difficult to transfer data or messages in a secure manner. To improve data security and privacy, effective encryption methods are required. Technology advancement has also given rise to greater threats as it aims

to provide sophisticated or robust security for the consumer. Subscribers utilize encryption methods to protect their personal information and communications.

The algorithm's ciphering process offers a way to achieve the security requirement of authentication and confidentiality. The utilization of wireless airwaves opens the door to various network-targeting cyberattacks. The attacks could range from passive eavesdropping to active ones including impersonation, message replay, message modification, and signal jamming. Attackers can access sensitive information and violate security conditions such as data privacy by eavesdropping. Even messages that are already being transmitted over the network can be deleted by an active attacker, and they can even introduce false messages into a route through which they are participating. Availability, integrity, authentication, and non-repudiation are all violated by these attacks. Integrity refers to the method by which the consumer of a communication validates its truthfulness by checking for message modification during transit.

Elliptic Curve Cryptography (ECC), a form of public key cryptography, is used to ensure total security. ECC transforms the mathematical issue into the appropriate computer algorithm. To overcome the difficulties presented by the difficult issues in public key cryptography, the cryptosystem requires a highly computational model. The algebraic structure of elliptic curves over infinite fields is the basis on which the ECC is designed. In comparison to RSA, ECC has shorter operand lengths since it is based on discrete log functions of infinite fields.

To ensure message integrity, ECC offers a variety of security features, including key exchange, communication confidentiality through encryption, sender authentication, and digital signatures. The application of security regulations in industry is controlled by a variety of standard units. Elliptic curve-based systems are implemented utilizing significantly less parameters, which improves performance, when considering the recent history of known attacks.

Steganography is a technique for keeping data secret from one another. It combines the science and art of secure communication. Secure data transport over the internet is the main goal of steganography [7]. The data in steganography is encrypted through a variety of file carriers, including picture, audio, video, and text. The cover material in image steganography is an image. The cover media for the text steganography technique is a text file, while the cover media for the video steganography technique is a video file. Different steganography techniques exist to hidden data in photographs, each with its own strengths and weaknesses and degree of complexity.

To communicate data more securely Steganography utilizes cryptography. Before being sent to the opposite end, the message is encrypted using an encryption method and a secret key in cryptography. The receiver then uses a decryption process to recover the original message [8]. In the approach, different algorithms have been presented. One of the most and simple methods used for data hiding is LSB. The message bit is used by the LSB (Least Significant Bit) method [9] to replace the cover file's least significant bit. This method of message steganography is the most widely utilized.

The analysis's next section is structured as follows, with Section II providing a literature review. In Section III demonstrate the view of new LSB-S image steganography method using Galio Field in elliptic curve cryptography, this is followed by a full result analysis in

Section IV, and finally a discussion of the conclusion in Section V.

II. LITERATURE SURVEY

Nicolas Sklavos I, III, I. D. Zaharakis et. al. [1] explained the issues with IoT security and privacy. Current cryptographic concepts, techniques, and implementations, like Elliptic Curve Cryptography (ECC) and the Advanced Encryption Standard (AES), are presented along with their functionality and advantages and disadvantages. It draws attention to the demand for more adaptable cryptography suites.

Centicom et. al. [2] The public key and private key, which are two separate keys used by the algorithm are used for both encryption and decryption operations. These algorithms are mostly used for authentication and integrity protection. They are developed using mathematical abstractions based on computationally challenging number-theoretic problems like integer factorization, discreate logarithmic, etc. preserving the specifications integrity.

I. Hussain et. al. [3] when sensitive data is transferred through an untrusted medium, cryptography becomes important. It becomes extremely useful, especially in a wide range of applications. The key is generated and encrypted using the encryption algorithm. The ability of the Sbox to distort the data determines how strong the encryption is, hence the process of finding new and powerful S-boxes is quite interesting in the world of cryptography.

A.Singh,D. Juneja and A.K.Sharma et. al. [4] If the sender wants to transmit a plaintext message d to the receiver, they will compute cipher text p by encrypting message (d) to produce cipher text (p), and then send cipher text (p) to the receiver. When Receiver N receives the message (p), it will compute the original plaintext message d by decrypting the message p.

Y. Rajkumar, R. Rishi, and S. Batra et. al. [6] presented a different approach based on pixel parity. If the parity is odd, the message is hidden by hiding zero, and if the parity is even, the message is hidden by hiding one. This method's ability to hide data is 98.82 percent. This method is very simple to break using the hit and trail method. Breaking the algorithm only requires one gauss, which is whether the value of a pixel has odd parity or even parity. Extract zero if the parity is odd; otherwise, retrieve one.

S. Parvinder, B. Sudhir and H. R. Sharma et. al. [13] The main disadvantage of the LSB approach is that while the message is hidden in the LSB bit, if the hacker extracts all of the LSB bits, he can read the complete message. A network optimization by Parvinder et al. utilized the sixth and seventh bits to hide the data. Since data is not hidden on LSB, this method eliminates the drawback of LSB. However, the ability to hide data was just a small percentage.

O. Goldreich et. al. [14] In other words, the way keys are exchanged influences the security of symmetric key cryptography to some extent. Public-key cryptography, in which a transmitter and a receiver share a public key but have different private keys, was utilized to get around this difficulty. The keys are connected mathematically. The public key and the private key are used for encryption and decryption, respectively. The mathematical complexity of the link between the public key and private key plays a major role in the security of public-key cryptography.

W.Stalling et. al. [15] The general application of security concepts is explained in significant detail. The concerned about security is generally related to addressing the issues by

selecting a security protocol that exceeds all of the appropriate security requirements. The security protocol satisfies the necessary cryptographic standards for security.

III. LSB-S IMAGE STEGANOGRAPHY METHOD BASED ON GALOIS-FIELD CRYPTOGRAPHY

The proposed work's architecture is described in this section. The secret message's operations are represented in this architecture. The LSB-S image steganography approach, shown in Figure 1, is based on the Galois-Field cryptography architecture.

The analysis attempts to provide a comprehensive security strategy for protecting communication using Elliptic curve cryptography's Galois field technique. With this analysis, they aim to strengthen the analytical approach for communication security. In elliptic curve cryptography, the Galois field is used to conceptualize the analytic model. Plaintext refers to the presentation of a message in a straightforward manner which is simple sufficiently for a new user to understand.

By means of encryption, plain text is changed into cipher text, a format that protects the meaning of the communication from all users except for the user who is an authorized communicating partner. When a user uses a device or application for web-based communication, security is an important concern because the user is susceptible to various types of attacks based on the network's design. Algorithms are applied to solve security problems. The data in this suggested work is encrypted using the Vernam cypher and then it is hidden using the LSB-S approach described in the methodology section. This analysis uses a two-layer framework to hide the message. The first layer uses the Vernam cipher to scramble the data, and the second layer uses the novel LSB-S algorithm to scramble the data received from the first layer, which has the advantages of perceptual degradation and message capacity.

The security of the data is increased by combining the new steganography technique with the current cryptography technique. For the Vernam cipher algorithm, the sender and receiver use the identical one-time pad key. Receiver is aware of the encryption algorithm. The format's cover is chosen with the approval of both the sender and the recipient. The steganography algorithm used by the sender to hide the message is known to the receiver. The hidden's length is known to the receiver.

Consider the grayscale image and binarization is then applied to the image. Binarization is the process of converting any entity's data characteristics into vectors of binary values to improve the performance of classifier algorithms. The grayscale of a picture is converted during binarization from a 0-255 spectrum to 0-1 spectrum. Any gray-scale (multi-tone) image can be converted into a black-and-white image using the binarization technique (two tone image).

To complete the binarization procedure, first determine the grayscale threshold value and determine if a pixel has a specific grey value or not. If the threshold is exceeded and a pixel's grey value is higher, the pixel is turned into white. Similar to this, if a pixel's grey value is lower than the threshold, that pixel is turned into black. The generation of a Session Shared Key (SSK). A session key is a randomly generated encryption and decryption key that is used to protect an image communications session between a user and another computer or two computers. For a designated user, the system will generate a key pair. A private key and a public key are produced.

Since the public and private keys are mathematically connected, any messages encrypted using the public key can be decrypted using the private key. The data has now been assigned to the key pairs. The S-box procedure is then carried out. An S-box (Substitution-box) is a fundamental part of symmetric key algorithms in cryptography that performs substitution. They are commonly implemented in block ciphers to hide the connection between the key and the ciphertext, providing Shannon's property of confusion. In this case, the S-box converts the input bits into the output bits.

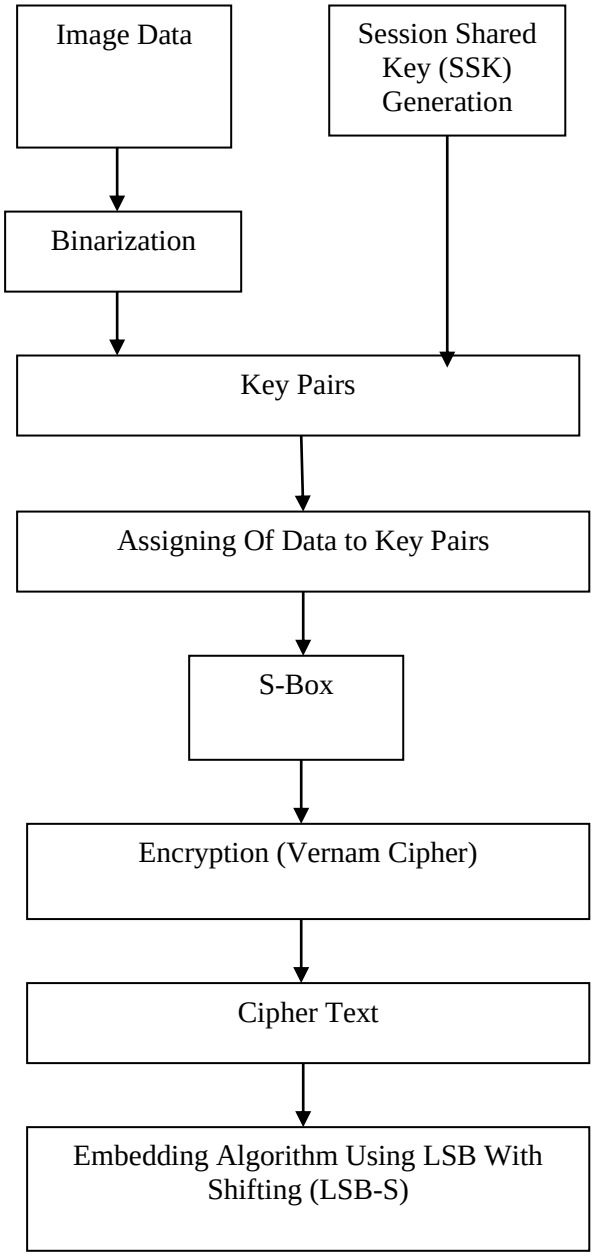

Fig. 1: BLOCK DIAGRAM

The message is then converted to ciphertext using Vernam encoding and stored as bits in M. Here, the encrypted text is retrieved, and the subsequent steps are then carried out.

In a temporary matrix Tl of pixels, extract the four LSB bits, do an I-bit circular left shift over these bits, and then store them once again. Increase 1 in the current place to shift on the subsequent Tl element. 2. Get the LSB of the first element in Tl and perform a perfonn XOR with one of the message bits from the message matrix. Decrease the message's length by one. Store the previous step's result in I at the first pixel's LSB and Shift on the next element of I by increasing 1 in the present location. Till length of M=O, repeat step 3; then stop. Data is encrypted before being finalized.

IV. RESULT ANALYSIS

After carrying out the required work, the algorithm was evaluated and contrasted with other approaches based on PSNR, MSE, and accuracy.

The parameter that allows access to the quality of the Stego image in comparison to the original image is the PSNR (Peak Signal to Noise Ratio). It determines the Stego image's imperceptibility. It calculates and evaluates how similar two images are, or the similarity between the Stego image and the original image, in simple fonn. The quality of the Stego image will be higher if the PSNR value is higher, or, alternatively, the imperceptibility of the hidden message hidden behind an image's pixels will be higher.

$$PSNR = 10\log_{10}\left[\frac{I^2}{MSE}\right] \quad (1)$$

A parameter called Mean Squared Error (MSE) determines the average size of the error between the original image and the Stego image. After being squared, the difference between the values shown in the original image and the Stego image is averaged. Due to the relatively high weight that RMSE gives to significant errors, these errors are often the ones that are utilized. So when there are major errors in the carrier file that are undesirable, RMSE is quite demanding. The lower the value of RMSE, the higher the system quality will be.

$$MSE=\frac{1}{[R\times C]^2}\sum_{i=1}^{N}\sum_{j=1}^{M}(X_{ij}-Y_{ij})^2 \quad (2)$$

Here, I, stands for the image's highest possible pixel value. For instance, the maximum value for a grayscale image is 255. MSE stands for Mean Square Error. R and C represent the number of Rows and Columns in the cover image. Xij denotes the intensity of the Xijth pixel in the cover image. Yij denotes the intensity of the Yijth pixel in the Stego image.

Accuracy: It is described as being the proportion of correctly identified occurrences to all instances, and it is provided as

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} \times 100 \quad (3)$$

True Positive (TP): TP is the total number of positive predictive instances that are correctly classified and are actually positive.

True Negative (TN): TN is the total number of actually negative predictive instances that are labelled without error.

False Positive (FP): FP is the total amount of positive predictive instances that are classified as error and are not actually positive.

False Negative (FN): FN is the total number of negative predictive instances that are classified as erroneous and are not actually negative.

MATLAB was used to implement the suggested technique. The standard image with the dimensions 256*256 was obtained from the USC-SIPI-ID database for this experiment. These photos have been reduced in size to 256*256 for simplicity. The message size was set to lKB, 2KB, and 4 KB. PSNR, MSE, and accuracy were determined for each cover and Stego picture using the formulas given in equations 1, 2, and 3.

The performance analysis of the new LSB-S picture steganography method, Linguistic approach, and Format Based method is shown in table 1.

Table 1: PERFORMANCE ANALYSIS

Methods	accuracy	PSNR	MSE
Linguistic	89	58.3514	1.1522
Format Based	85	55.6380	1.8633
LSB-S	96	62.2465	0.0695

The above table shows that the PSR, MSE and accuracy values of the suggested new LSB-S image steganography method using Galio Field in elliptic curve cryptography has achevied a good results.

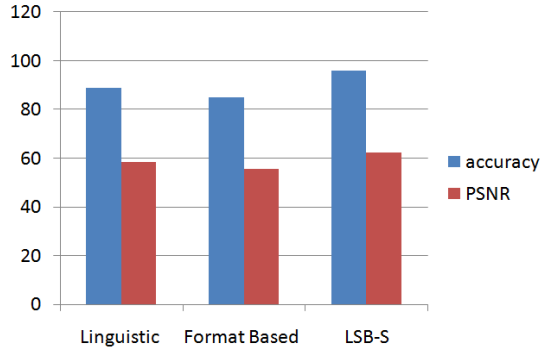

Fig. 2: ACCURACY AND PSNR PERFORMANCE COMPARISON BETWEEN METHODS

Therefore the LSB-S has better accuracy and PSNR than the Linguistic and Format Based methods.

In this comparision the above graph shows that LSB-S has lower MSE than the Linguistic and Format Based methods.

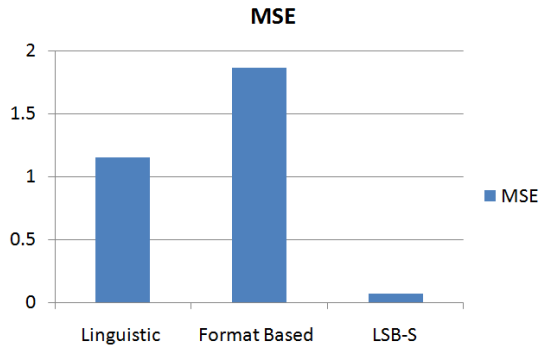

Fig. 3: MSE PERFORMANCE COMPARISON BETWEEN METHODS

Hence, presented a new LSB-S image steganography method using Galio Field in elliptic curve cryptography effectively has the high hiding capacity.

V. CONCLUSION

This analysis suggested a new data hiding strategy that overcomes the limitations of existing methods. This approach suggests an LSB-S image steganography approach based on an elliptic curve encryption mechanism, which is widely utilized in the field of encryption. Arithmetic operations on Galois fields are significant in communications because they are utilized in error correcting codes and encryption. An algorithm is utilized to encrypt the image in this approach, and then a novel method (LSB-S) is implemented to hide the ciphertext in the grey image. This method outperforms the existing one in that it gets around its limitations. Since every pixel in the proposed method is capable of holding a data bit, the data hiding capacity is 100%. An attacker will not get the message if he takes all of the LSB bits. Significant advances in privacy, authenticity, integrity, and non-repudiation have been achieved by utilizing a new LSB-S image steganography approach in elliptic curve encryption that use the Galio Field. The experimental result shows that the suggested new LSB-S image steganography method using Galio Field in elliptic curve cryptography has obtained good results in terms of PSNR, MSE and accuracy.

VI. REFERENCES

[1] Nicolas Sklavos I, III, I. D. Zaharakis,"Cryptography and Security in Internet of Things (IoTs) : Models, Schemes and Implementations", in2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS)

[2] "Centicom", Link: www.certicom.com Retrived, 23rd August, 2015

[3] I. Hussain, et al., "A projective general linear group based algorithm for the construction of substitution box for block ciphers," Neural Computig. Appliction, Vol. 22, no. 6, pp. 1085–1093, Feb. 2012.

[4] A.Singh,D. Juneja and A.K.Sharma,"Elliptical Curve Cryptography Based Security Engine for Multiagent System Operating in Semantic Cyberspace",International Journal of Reserach and REviews in Computer Science (IJRRCS), Vol.2,no.2,pp.283-290, 2011

[5] B. Sudhir, R. Rahul, and Y. Rajkurnar "Insertion of message in 6th, 7th and 8th bit of pixel values and its retrieval in case intruder changes the least significant bit of image pixels" International Joumal of Security and Its Applications, Vol. 4, No. 3, July, 2010

[6] Y. Rajkumar, R. Rishi, and S. Batra, "A New Steganography Method for Gray Level Images using Parity Checker," Int. J. Comput. Appl., vol. II, no. II, pp. 18-24,2010.

[7] K. Macrakis, "Confessing Secrets: Secret Communication and the Origins of Modern Science," Intell. Nat!. Secur., vol. 25, no. 2, pp. 183- 197,2010.
[8] I. V. S. Manoj, "Cryptography and Steganography," Int. J. Comput. Appl., vol. I, no. 12, pp. 63-68, 2010.
[9]A. C. A, 1. Condell, K. Curran, and P. M. Kevitt, "Digital image steganography-: Survey and analysis of current methods," Signal Processing, vol. 90, no. 3, pp. 727-752,2010.
[10] C. H. Yang and S. J. Wang, "Transforming LSB substitution for imagebased steganography in matching algoritInns," J. Inf. Sci. Eng., vol. 26, no. 4,pp. 1199-1212,2010.
[11] B. Sudhir, R. Rahul, and Y. Rajkurnar "Insertion of message in 6th, 7th and 8th bit of pixel values and its retrieval in case intruder changes the least significant bit of image pixels" International Joumal of Security and Its Applications, Vol. 4, No. 3, July, 2010
[12] A. Ahnohammad, "Steganography-Based Secret and Reliable Communications: Improving Steganographic Capacity and Imperceptibility by," 2010.
[13] S. Parvinder, B. Sudhir and H. R. Sharma, "Evaluating the Performance of Message Hidden in First and Second Bit Plane, W SEAS Transaction on Information Science and Technology, Vol. 2, No. 89, PP 1220- 1222, Aug. 2005
[14] O. Goldreich, “Basic applications,” in Foundations of Cryptography, vol. 2, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 2004, pp. 375–376.
[15] W.Stalling “cryptography and network security principles and practice 4th edition princetice Hall.